PPS: Privacy-Preserving Strategyproof Social-Efficient Spectrum Auction Mechanisms

He Huang, *Member, IEEE,* Xiang-Yang Li, *Senior Member, IEEE,* Yu-e Sun, Hongli Xu, *Member, IEEE,* and Liusheng Huang *Member, IEEE*

Abstract—Many spectrum auction mechanisms have been proposed for spectrum allocation problem, and unfortunately, few of them protect the bid privacy of bidders and achieve good social efficiency. In this paper, we propose PPS, a Privacy Preserving Strategyproof spectrum auction framework. We design two schemes based on PPS separately for 1) the Single-Unit Auction model (SUA), where only single channel will be sold in the spectrum market; and 2) the Multi-Unit Auction model (MUA), where the primary user subleases multi-unit channels to the secondary users and each of the secondary users wants to access multi-unit channels either. Since the social efficiency maximization problem is NP-hard in both auction models, we present allocation mechanisms with approximation factors of $(1+\epsilon)$ and 32 separately for SUA and MUA, and further judiciously design strategyproof auction mechanisms with privacy preserving based on them. Our extensive evaluations show that our mechanisms achieve good social efficiency and with low computation and communication overhead.

Index Terms—Spectrum auction, Approximation algorithm, Privacy preserving, Social efficiency, Strategyproof.

1 Introduction

The ever-increasing demand for limited radio spectrum resource poses a great challenge in spectrum allocation and usage [32]. Recent years, auction has been widely regarded as a preeminent way to tackle such a challenge because of its fairness and efficiency [19]. In general, bidders in spectrum auctions are the secondary users, while the auctioneer is a primary user in the single-sided spectrum auctions.

In recent years, many strategyproof auction mechanisms, in which bidding the true valuation is the dominant strategy of bidders, have been proposed for solving spectrum allocation issue. Unfortunately, the auctioneer is not always trustworthy. Once the true valuations of bidders are revealed to a corrupt auctioneer, he may abuse such information to improve his own advantage. Besides, the true valuation may divulge the profit of bidders, which is also a commercial secret for each bidder. Therefore, bid privacy preservation should be considered in spectrum auction design.

Allocating channels to the buyers who **value** them most will improve the *social efficiency*. However, it is not trivial to design a strategyproof spectrum auction mechanism with maximum social efficiency, due to its NP-hardness. There have been many studies devoted to maximizing the social efficiency while ensuring strategyproofness in spectrum auction mechanism design [8], [10], [32], [38], [40]. Only a few of these auction mechanisms address performance guarantee on social efficiency, *e.g.* [8] proposes a strategyproof combinatorial spectrum auction mechanism with an approximation factor of $\sqrt{m}$ and [12] designs a set of $1-1/e$ approximation spectrum auction mechanisms with spatial and temporal reuse. However, none of them provides any guarantee on bid privacy preservation. To tackle this, [13] and [26] study the problem of designing privacy-preserving or secure spectrum auction mechanisms with untrustworthy auctioneer. Unfortunately, neither of them provides any performance guarantee.

To maximize the social efficiency of spectrum auctions, we need to compute various bid sums of conflict-free bidders, and make decisions based on these bid sums. However, it is hard for the auctioneer or the bidders to compute these bid sums with privacy preserving since the auctioneer does not know any bidder's true bid value. Furthermore, since the computation burden for the auctioneer which relies on the bid values of bidders is too heavy, we cannot get a secure auction mechanism through simply combining the existing social-efficient auction mechanisms and some bid privacy preserving solutions directly. Thus, the task of designing a privacy preserving strategyproof spectrum auction mechanism with performance guarantee is highly challenging. We need to design some new mechanisms to provide good performance guarantee and protect the true bid values of bidders.

In this paper, we consider the issue of designing strategyproof spectrum auction mechanism which maximizes the social efficiency while protecting the bid privacy of bidders. We propose a Privacy Preserving Strategyproof spectrum auction framework (PPS). Under PPS, we mainly study two models:

- The Single-Unit Auction model (SUA)
- The Multi-Unit Auction model (MUA)

- H. Huang is with the School of Computer Science and Technology, Soochow University, Suzhou, Jiangsu, 215006.
E-mail: huangh@suda.edu.cn
- X.-Y. Li is with the Department of Computer Science, Illinois Institute of Technology, and Tsinghua National Laboratory for Information Science and Technology (TNLIST), Tsinghua University, E-mail: xli@cs.iit.edu.
- Y. Sun is with the School of Urban Rail Transportation, Soochow University, Suzhou, Jiangsu, 215006, E-mail: sunye12@suda.edu.cn.
- H. Xu, L. Huang are with the School of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui, 230027, E-mail: {xuhongli, lshuang}@ustc.edu.cn.

In the SUA model, the auction mechanism design only focuses on single channel trading. Multi-unit channels trading is supported in the case of MUA model. Since the maximization of social efficiency problem in both SUA and MUA are NP-hard, we design allocation mechanisms with approximation factors of $(1 + \epsilon)$ and 32 separately for the SUA and the MUA. We show that the proposed approximation allocation mechanisms are bid-monotone, and further design strategyproof auction mechanisms based on them, which are denoted as PPS-SUA and PPS-MUA respectively. As the PPS-MUA only ensures the worst case performance, we further propose an improved mechanism, denoted by PPS-EMUA, to improve the social efficiency of PPS-MUA. We also show that PPS-EMUA is strategyproof and privacy-preserving.

It is not a trivial job to protect privacy of the true bid values of bidders in the auction mechanisms as auction relies on these bid values to make decision on allocation and payment computation. To address this challenge, we will first introduce an *agent*, which is a semi-trusted third party (such as FCC), different from auctioneer. The agent, together with the auctioneer, will execute the auction in PPS. In our design, bidders apply *Paillier's homomorphic encryption* to encrypt the bids so agent can perform computation on the ciphertexts, agent then sends the results by adding random numbers and shuffling bidder IDs to auctioneer for making allocation decision, which provides privacy protection without affecting the correctness of the allocation. We will prove that neither the agent nor the auctioneer can infer any true bid value about the bidders without collusion. To the best of our knowledge, PPS is the first privacy preserving spectrum auction scheme that maximizes the social efficiency. Note that we did not focus on protecting the location privacy of bidders in our mechanisms, as previous schemes (*e.g.*, [22]) can be integrated into our mechanisms.

The remainder of paper is organized as follows. In Section 2, we formulate the spectrum auction and present the framework of PPS. Section 3 proposes a strategyproof spectrum auction mechanism for solving the single-unit auction model. Section 4 further extends the auction model with consideration of multiple-items trading model. Extensive simulation results are evaluated in Section 5. Section 6 discusses the related literatures and Section 7 concludes the paper.

2 Problem Formulation and Preliminaries

In this section, we first formulate our spectrum auction model, and state the design targets of our work. Then, we overview the cryptographic tools used in this paper. At last, we will introduce the PPS, which is a privacy preserving spectrum auction framework.

2.1 Spectrum Auction Model

We model the procedure of secure spectrum allocation as a sealed-bid auction, in which there is an *auctioneer* (*a.k.a.* primary user), a set of *bidders* (*a.k.a.* secondary users) and an *agent*. In each round of the auction, the auctioneer subleases the access right of m channels to n bidders. The bidders first encrypt their bids by using the *encryption key* of a homomorphic encryption scheme (*e.g.*, Paillier's scheme) for the auctioneer, and submit the encrypted bids to the *agent* (not the auctioneer). Here, $E(m)$ denotes the homomorphic encryption of message m. Then, the auctioneer and the agent allocate the channels to the bidders via communicating with each other. We assume that the agent is a *semi-trusted party*, and will not collude with the auctioneer.

We use $\mathcal{C} = \{c_1, ..., c_m\}$ to denote the set of channels, and $\mathcal{B} = \{1, ..., n\}$ to denote the set of bidders. Each bidder $i \in \mathcal{B}$ is described as $i = \{L_i, N_i, b_i, v_i, p_i\}$, where L_i is the geographical location of i, N_i is the number of channels that bidder i wants to buy, b_i, v_i and p_i separately denote the bid value, true valuation and payment of i for all the channels that he wants to buy. We assume that the interference radii of all channels are the same, which are equal to $\frac{1}{2}$ unit. Then, two bidders i and j conflict with each other if the distance between L_i and L_j is smaller than 1 unit. Bidders can share one channel iff they are conflict free with each other.

In this paper, we study two spectrum auction models. The first one is that there is only one channel in the spectrum market, then $m = 1$ and $N_i = 1$ for each bidder. We call this model the *Single-Unit Auction model* (SUA). The second one is the *Multi-Unit Auction model* (MUA) which supports multiple channels trading in the market. In MUA, each bidder wants to access $N_i \geq 1$ channels rather than part of them.

2.2 Design Targets

Our work is to design social efficient strategyproof spectrum auction mechanisms with bid privacy preservation. Firstly, we will allocate channels to the bidders who value them most to maximize the social efficiency. However, the optimal channel allocation problem in SUA and MUA are all NP-hard. Thus, we will design approximation mechanisms instead. Secondly, our auction mechanisms should be strategyproof, which means bidding truthfully is the *dominant strategy* for any bidders. To achieve this, it is sufficient to show that our allocation mechanism is *bid-monotone*, and always charges each winner its *critical value* [25]. We say an allocation mechanism is bid-monotone if bidder i wins the auction by bidding b_i, he will always win by bidding $b'_i > b_i$. And the critical value of each bidder i in a bid-monotone allocation mechanism is the minimum bid that bidder i will win in the auction. The third objective is to protect the privacy of the bid values of bidders. To achieve privacy protection, we will apply homomorphic encryption to encrypt the bid values using the public key of auctioneer, and agent will perform the most of the computation and send the intermediate results to the auctioneer. We will show that both the auctioneer and the agent cannot get any information about the true bid values of bidders as long as they will not collude with each other.

2.3 Cryptographic Primitives

In this part, we will introduce the cryptographic tools used in this paper: Paillier's cryptosystem and homomorphic encryption.

Paillier's cryptosystem: An entity first randomly chooses two large prime numbers h_1 and h_2. Then, he computes $h = h_1 h_2$, $H = h + 1$, and publishes $EK = (h, H)$ as his public key (encryption key). Next, he computes $\lambda = (h_1 - 1)(h_2 - 1)$ and $\mu = (\lambda \ mod \ h^2)^{-1} \ mod \ h$, and sets $DK = (\lambda, \mu)$ as his private key(decryption key).

An encrypter selects a random integer $r' \in \mathbb{Z}_h$ and encrypts the message msg by using EK and r':

$$E(\mathsf{msg}, r') = g^{\mathsf{msg}} {r'}^h \ mod \ h^2,$$

where $E(\mathsf{msg}, r')$ is the ciphertext of msg.

The holder of $DK = (\lambda, \mu)$ can decrypt the ciphertext $E(\mathsf{msg}, r')$, and recover the message by computing the following:

$$\mathsf{msg} = L(E(\mathsf{msg}, r')^{\lambda} \ mod \ h^2)\mu \ mod \ h,$$

where $L(a) = (a - 1)/h \ mod \ h$.

Homomorphic Encryption (HE): Homomorphic encryption is a form of encryption which allows addition and multiplication to be carried out on ciphertext, and obtain a correct encrypted result.

The Paillier's cryptosystem satisfies the following homomorphic operation:

$$E(\mathsf{msg}_1, r'_1)E(\mathsf{msg}_2, r'_2) = E(\mathsf{msg}_1 + \mathsf{msg}_2, r'_1 r'_2) \ mod \ h^2$$

$$E(\mathsf{msg}_1, {r'}_1)^{\mathsf{msg}_2} = E(\mathsf{msg}_1 \mathsf{msg}_2, {r'}_1^{\mathsf{msg}_2}) \ mod \ h^2.$$

Note that the random integer r' dose not contribute to decryption or other homomorphic operation, hence we use $E(\mathsf{msg})$ instead of $E(\mathsf{msg}, r')$ in the remaining paper.

Indistinguishability under chosen-plaintext attack (IND-CPA): Ciphertext indistinguishability plays an important role in cryptosystems. Intuitively, if a cryptosystem possesses the property of indistinguishability, then an adversary will not be able to distinguish from a pair of ciphertexts via the messages they encrypt. Commonly, the property of indistinguishability under chosen plaintext attack (IND-CPA) is defined by the following game:

1) A adversary is given a public key, which it may use to perform a polynomially bounded number of encryptions or other operations.
2) The adversary generates two equal-length messages msg_1 and msg_2, and transmits them to a challenge oracle along with the public key.
3) The challenge oracle selects one of the messages uniformly at random, encrypts the message under the public key, and returns the resulting ciphertext to the adversary.

We say an underlying cryptosystem is IND-CPA if the probabilistic polynomial time-bounded adversary cannot determine which of the two messages was chosen by the oracle, with probability significantly greater than $\frac{1}{2}$ (the success rate of random guessing).

2.4 A Spectrum Auction Framework with Privacy Preserving

The process of our spectrum auction mechanisms consists of three steps: bidding, allocation and payment calculation. To protect the bid values of bidders, we design a strategyproof spectrum auction framework with privacy preserving, namely PPS, which is shown in Algorithm 1.

Algorithm 1 PPS: Privacy Preserving Strategyproof Spectrum Auction Framework

```
Each bidder $i$ submits $E(b_i)$, $N_i$ and $L_i$ to the agent, where $b_i$ is encrypted by using the encryption key of the auctioneer;
The agent and the auctioneer run a bid-monotone allocation mechanism while protecting the bid privacy of bidders.
The agent and the auctioneer compute a critical value for each winner with bid privacy preserving.
```

3 A Single-unit Scheme

In this section, we will present a strategyproof spectrum auction mechanism for SUA, denoted by PPS-SUA, which maximizes the social efficiency and preserves the bid privacy.

3.1 Initialization and Bidding

Before running the auction, the auctioneer generates an encryption key EK and a decryption key DK of Paillier's cryptosystem. Then, he announces EK as the public key, and keeps DK in private. Each bidder i encrypts his bid b_i by using EK, and sends $(E(b_i), L_i)$ to the agent. In the sending procedure, each bidder keeps his encrypted bidding price as a secret to the auctioneer.

3.2 Allocation Mechanism with Privacy Preserving

After receiving the encrypted bids from bidders, the auctioneer and the agent allocate channels to bidders via communicating with each other. The goal of our allocation mechanism is to maximize the social efficiency, which is equal to finding a group of conflict-free bidders with highest bid sum. Define the bid value of each bidder as his weight. Our optimal allocation problem can be easily reduced to the *maximum weighted independent set* (MWIS) problem, which is a well-known NP-hard problem. To tackle this NP-hardness, we propose a polynomial time approximation scheme (PTAS) based on *shifting strategy* [14], [23], which provides an approximation factor of $(1 + \epsilon)$. For completeness of presentation, we first review this PTAS method.

In the PTAS, we first select a positive integer k, then, the plane is subdivided into several grids of size at $k * k$ by a collection of vertical lines $x = i \cdot k + r$ and horizontal lines $y = j \cdot k + s$, where $0 \leq r, s \leq k - 1$. We call such a subdivision as *(r, s)-shifting*. Here we assume that the conflict radius of each bidder is $\frac{1}{2}$, then each bidder can be viewed as a *unit disk*. Fig. 1 gives an instance of a grid subdivided by (r, s)-shifting, where $k = 4$. We will throw away all the disks which

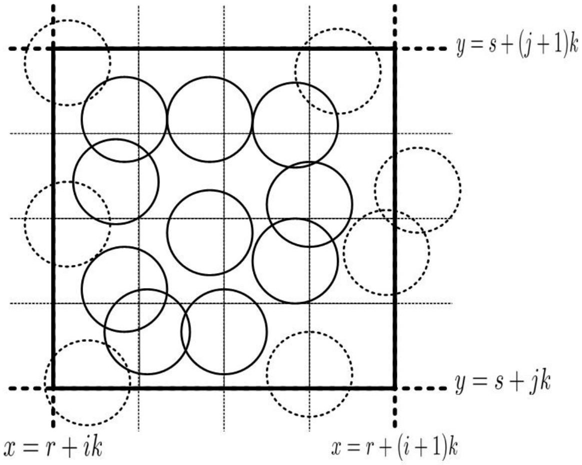


Fig. 1: A grid subdivided by (r,s)-shifting ($k = 4$).

intersect with some special lines $X \equiv r \mod k$ and $Y \equiv s \mod k$ in (r,s)-shifting, and solve the sub-instances of disks contained in each grid individually. Here, a grid is a square defined by $\{(x,y) \mid r+ik \le x \le r+(i+1)k, s+jk \le y \le s+(j+1)k\}$ for some integers i and j. Let the optimal solution of (r,s)-shifting be the union sets of all the optimal solution of the subdivided grids, and $w(OPT(r,s))$ be the weight of the optimal solution of (r,s)-shifting. It can be proven that there is at least one (r,s)-shifting, $0 \le r,s \le k-1$, with

$$w(OPT(r,s)) \ge (1-\frac{1}{k})^2 w(OPT(\mathcal{B})), \qquad (1)$$

where $OPT(\mathcal{B})$ is the maximum weighted independent set of all the bidders, and $w(OPT(\mathcal{B}))$ is the weight of $OPT(\mathcal{B})$. For any given integer $k \ge 1$, there are k^2 kinds of different shiftings in total. We will choose the optimal solution of (r,s)-shifting's that with the highest weight as our final approximation solution. Thus, we have a PTAS for optimal channel allocation problem, *i.e.* setting $k = \frac{1+\epsilon+\sqrt{1+\epsilon}}{\epsilon}$.

Based on this PTAS we then present our channel allocation mechanism with privacy preserving. Observe that the bidders submit their bids to agent encrypted using the auctioneer's public key. Following the PTAS protocol, we need to compute a maximum weighted independent set for each grid in the (r,s)-shifting, *i.e.*, compare the weights of all independent sets. Clearly, the auctioneer should not access the encrypted bid of any bidder as he has the decryption key. In our protocol, the agent will compute $E(\sum_{i\in S} b_i)$ for each of the maximal independent set contained in a grid, which can be done easily as $E(b_i)$ is computed from homomorphic encryption. For any given grid $g^{r,s}_j$ of the (r,s)-shifting, let $\mathcal{D} = \{d^{r,s}_{1,j}, \cdots, d^{r,s}_{z,j}\}$ be the set of *maximal independent sets* of bidders in $g^{r,s}_j$. We use $OPT(g^{r,s}_j)$ to denote the optimal solution in the grid $g^{r,s}_j$. Clearly $\mathcal{D}$ has cardinality of at most $O(k^2)$ and can be enumerated in time $O(n^{O(k^2)})$. In Algorithm 2, we present our method for finding the $OPT(g^{r,s}_j)$ for each subdivided grid $g^{r,s}_j$ with privacy preserving. To hide the true values of $w(d^{r,s}_{i,j})$ (which may break privacy) from the auctioneer, the agent will mask them by using two random values δ_1 and δ_2 as $\delta_1 + \delta_2 \cdot w(d^{r,s}_{i,j})$. Note that the range $[1, 2^{\gamma_1}]$ and $[1, 2^{\gamma_2}]$ for δ_1 and δ_2 are chosen based on the consideration of the correctness of modular operations: $\delta_1 + \delta_2 \cdot w(d^{r,s}_{i,j})$ should be smaller than the modulo used in Paillier's system.

Assume that the number of grids that subdivided by (r,s)-shifting is $N_{r,s}$, then the optimal solution of (r,s)-shifting is

$$OPT(r,s) = \bigcup\nolimits_{j\le N_{r,s}} d^{r,s}_{\sigma(1),j}. \qquad (2)$$

By sending the intermediate results to the auctioneer, the auctioneer can compare and find which independent set will be chosen for each subgrid. Observe that both the auctioneer and the agent will not know the bid values in the independent set. By using the optimal solution of each grid, the agent can calculate the encrypted value $E(w(OPT(r,s)))$, and allocate channels to bidders without leaking the true bid values of bidders. The allocation will be sent to the auctioneer. The details are described in Algorithm 3.

Algorithm 2 Computing the optimal solution for grid $g^{r,s}_j$

```
1: The agent randomly picks two integers $\delta_1 \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta_2 \in \mathbb{Z}_{2^{\gamma_2}}$, computes and sends $\{E(\delta_1 + \delta_2 w(d^{r,s}_{i,j}))\}_{1\le i\le z}$ to the auctioneer, where
      $E(\delta_1 + \delta_2 w(d^{r,s}_{i,j})) = E(\delta_1)(\prod_{l\in d^{r,s}_{i,j}} E(b_l))^{\delta_2}.$
2: The auctioneer decrypts $\{E(\delta_1 + \delta_2 w(d^{r,s}_{i,j}))\}_{0\le i\le z}$, and sorts them in non-increasing order. Assume
      $w(d^{r,s}_{\sigma(1),j}) \ge w(d^{r,s}_{\sigma(2),j}) \ge ... \ge w(d^{r,s}_{\sigma(z),j}),$
   where $d^{r,s}_{\sigma(i),j}$ is the maximum independent set with rank $i$ in the sorted list.
3: The auctioneer sends $\{\sigma(i)\}_{1\le i\le z}$ to the agent.
4: The agent chooses $d^{r,s}_{\sigma(1),j}$ as the optimal solution of grid $g^{r,s}_j$.
```

Algorithm 3 PTAS with bid privacy preserving

```
1: The agent randomly picks two integers $\delta_3 \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta_4 \in \mathbb{Z}_{2^{\gamma_2}}$, computes and sends $E(\delta_3 + \delta_4 w(OPT(r,s)))$ for any $1 \le r,s \le k$ to the auctioneer, where
      $E(\delta_3+\delta_4 w(OPT(r,s))) = E(\delta_3)(\prod_{j\le N_{r,s}} E(w(d^{r,s}_{\sigma(1),j})))^{\delta_4}.$
2: The auctioneer decrypts and sorts the weights of the optimal solution of different shiftings in non-increasing order.
      $w(OPT(\sigma_1(1),\sigma_2(1))) \ge ... \ge w(OPT(\sigma_1(k^2),\sigma_2(k^2))),$
   where $OPT(\sigma_1(i),\sigma_2(i))$ is the optimal solution of $(\sigma_1(i),\sigma_2(i))$-shifting with rank $i$ in the sorted list.
3: The auctioneer sends $\{(\sigma_1(i),\sigma_2(i))\}_{1\le i\le k^2}$ to the agent.
4: The agent chooses $OPT(\sigma_1(1),\sigma_2(1)))$ as the final solution, and sends the allocation result to the auctioneer.
```

Lemma 1: Our allocation mechanism for SUA is bid-monotone.

Proof: Without loss of generality, we assume that the bidder i wins by bidding b_i in grid $g_j^{r,s}$. Then, $\sigma_1(1) = r$, $\sigma_2(1) = s$ and bidder i in $d_{\sigma(1),j}^{r,s}$. It is not hard to get that the bidder i is still in $d_{\sigma(1),j}^{r,s}$ when he increases his bid to $b_i' > b_i$. Furthermore, the increased weight of other shiftings is no more than (r, s)-shifting when i increases his bid, which indicates that $\sigma_1(1) = r$ and $\sigma_2(1) = s$ still hold. Thus, we can conclude that i will always win by bidding $b_i' > b_i$. □

3.3 Payment Calculation with Privacy Preserving

We have proved that our allocation mechanism is bid-monotone, which indicates that there exists a critical value for each bidder. The bidder i will win the auction by bidding a price which is higher than its critical value, otherwise, bidder i will lose in the auction. To ensure the strategyproofness of our auction mechanism, we will compute the critical value for each winner as the final payment in the following.

Without loss of generality, we also assume that the bidder i wins by bidding b_i in grid $g_j^{r,s}$. We further assume that $d_{l(i),j}^{r,s}$ is the maximum independent set with highest weight which does not include bidder i, and $OPT(\sigma_1(f(i)), \sigma_2(f(i)))$ is the optimal solution of $(\sigma_1(f(i)), \sigma_2(f(i)))$-shifting which has the highest weight and does not include the bidder i. We will calculate the critical value of the winner i based on the following considerations.

- The minimum bid price, denoted as p_i^1, ensures bidder i win in grid $g_j^{r,s}$. Then, we can get that
$$p_i^1 = w(d_{l(i),j}^{r,s}) - w(d_{\sigma(1),j}^{r,s}) + b_i.$$
- The minimum bid of bidder i which makes $OPT(r, s)$ always with the highest weight among all the optimal solutions of shiftings including bidder i. We use p_i^2 (p_i^2 exists *iff* $f(i) > 2$) to denote this minimum bid, and set $p_i^{2,q} = w(OPT(\sigma_1(q), \sigma_2(q))) - w(d_{\sigma(1),j}^{\sigma_1(q),\sigma_2(q)}) + w(d_{l(i),j}^{\sigma_1(q),\sigma_2(q)}) - w(OPT(r, s)) + b_i$, then
$$p_i^2 = \max\{p_i^{2,1}, ..., p_i^{2,f(i)-2}\}.$$
- The minimum bid of bidder i that ensures $w(OPT(r, s)) \geq w(OPT(\sigma_1(f(i)), \sigma_2(f(i))))$, which is denoted by p_i^3. Then, we can get that
$$p_i^3 = w(OPT(\sigma_1(f(i)), \sigma_2(f(i)))) - w(OPT(r, s)) + b_i.$$

In conclusion, the critical value of bidder i is $p_i = \max\{p_i^1, p_i^2, p_i^3, 0\}$. Since the agent knows the order of all the maximum independent sets of each grid and the order of all the optimal solution of shiftings, he can compute the encrypted value of p_i^1, p_i^2 and p_i^3 by homomorphic operations, respectively. Then, our payment calculation mechanism with privacy preserving is depicted as follows:

1) The agent computes $E(p_i^1)$, $E(p_i^{2,1})$, $\cdots$, $E(p_i^{2,f(i)-2})$, $E(p_i^3)$, and sends the results to the auctioneer.
2) The auctioneer decrypts the ciphertexts and sets the payment of winner i as
$$p_i = \max\{p_i^1, p_i^{2,1}, ..., p_i^{2,f(i)-2}, p_i^3, 0\}. \qquad (3)$$

It is easy to prove the following theorems.

Theorem 2: PPS-SUA charges each winner its critical value and is strategyproof.

Theorem 3: The computation and communication cost of PPS-SUA are all $O(n^{k^2+1})$.

3.4 Privacy analysis of PPS-SUA

Theorem 4: PPS-SUA is bid privacy-preserving.

Proof: To confirm the bid privacy, we consider the view of agent and auctioneer, respectively.

During our auction mechanism for SUA, the agent can obtain nothing but the encrypted bids and the sorting results of the weight of each grid and each shifting. Based on the IND-CPA security of homomorphic cryptosystem, the agent cannot learn more information about the bid of any bidder.

The auctioneer holds the decryption key. Nevertheless, he has no direct access to the encrypted bids. While computing the optimal allocation and critical value of winner i, the auctioneer can receive the encrypted weight of maximal independent sets in each grid, weight of the optimal solution of each shifting, and $\{p_i^1, p_i^{2,1}, ..., p_i^{2,f(i)-2}, p_i^3\}$. From the weight of solutions in the grids or shiftings, the auctioneer cannot infer any bid, since they are encrypted by the agent and the auctioneer has no idea about which bidders are in these solutions, except the winning shifting. Consider $\{p_i^1, p_i^{2,1}, ..., p_i^{2,f(i)-2}, p_i^3\}$, auctioneer can construct the equation of them. However, the bid value of bidder i can still be well preserved, as auctioneer does not know any value of the variables in these equations. □

4 A MULTI-UNIT SCHEME

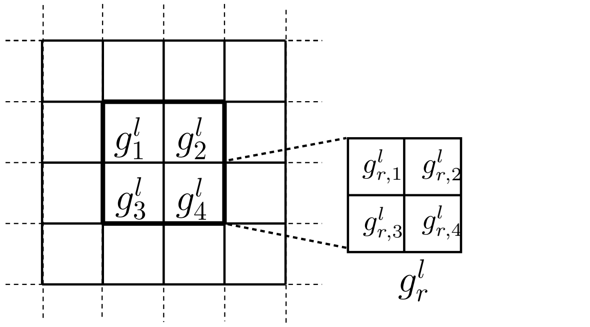
In this section, we propose a strategyproof auction mechanism for MUA, namely PPS-MUA, which protects the bid privacy of bidders and provides an approximation factor of 32. Then, we further design an extended version of PPS-MUA, namely PPS-EMUA, to improve the average performance of PPS-MUA, while keeping other properties unchanged. Although PPS-EMUA outperforms PPS-MUA, thoroughly introducing PPS-MUA can help us to better understand the mechanism of PPS-EMUA, and to better analyze the key properties of PPS-EMUA. Thus, we will introduce PPS-MUA first in the following.

4.1 Initialization and Bidding

The initialization and bidding procedure in MUA is similar as that in SUA, which can be referred in section 3.1. At last, each bidder i encrypts his bid b_i by using the encryption key of the auctioneer, and only sends $(E(b_i), N_i, L_i)$ to the agent.

4.2 Allocation Mechanism with Privacy Preserving

We have proved that the allocation problem which maximizes the social efficiency in SUA is an NP-hard problem. Since SUA is a special case of MUA, the optimal allocation issue



(a) l-th grid at size $2*2$ (b) g^l_r grid at size $1*1$

Fig. 2: An example of the subdivided grids

in MUA is also NP-hard. Thus, we will introduce a simple allocation mechanism which approximates the social efficiency. We first subdivide the plane into grids at size $2*2$, and use the symbol g^l to denote the l-th $2*2$ grid. It is obvious that there are four $1*1$ grids in each g^l. These four $1*1$ grids can be categorized into four types as shown in Fig. 2(a). Let g^l_r be the $1*1$ grid in g^l with type r, g_r be the set of $1*1$ grids with type r. We also assume that the conflict radius of each bidder is $\frac{1}{2}$ and regard each bidder as a unit disk. Obviously, each bidder located in g^l_r cannot conflict with the bidders located in $g^{l'}_r$ when $l \neq l'$. Let $OPT(g^l_r)$ be the optimal solution of allocation problem in g^l_r, $OPT(g_r)$ be the optimal solution of the allocation problem in g_r, then

$$OPT(g_r) = \bigcup\nolimits_l OPT(g^l_r). \tag{4}$$

Note that we cannot get the optimal solution in each grid g^l_r. To tackle this, we further subdivide each $1*1$ grid g^l_r into four $\frac{1}{2}*\frac{1}{2}$ sub-grids as shown in Fig. 2(b), which are denoted by $g^l_{r,1}$, $g^l_{r,2}$, $g^l_{r,3}$ and $g^l_{r,4}$, separately. Notice that all the bidders located in the same sub-grid $g^l_{r,s}$ conflict with each other. Thus, one channel can only be sold to one bidder in $g^l_{r,s}$.

The optimal allocation problem in each sub-grid $g^l_{r,s}$ can be reduced to a *knapsack problem* (KP), where the bid value of bidders is the value of items in KP, the number of channels in the market and channel demand of each bidder is the total volume of the knapsack and the volume of each item respectively. Although the KP is an NP-hard problem, there exists a PTAS [20], and a greedy allocation mechanism with approximation factor of 2 (the details can be referred to lines 3-5 in Algorithm 4). It is hard to design a privacy preserving version of the PTAS based on dynamic programming, thus, we design our allocation mechanism for MUA based on the greedy allocation mechanism in each sub-grid $g^l_{r,s}$. Assume that $APP(\mathcal{B})$, $APP(g_r)$, $APP(g^l_r)$ and $APP(g^l_{r,s})$ are the approximation solution of the allocation problem in the whole plane, g_r, g^l_r and $g^l_{r,s}$, separately. We choose the $APP(g^l_{r,s})$ with biggest weight as the solution of grid g^l_r and the $APP(g_r)$ with the biggest weight as our final solution $APP(\mathcal{B})$ (the details is depicted in Algorithm 4).

Theorem 5: Our auction mechanism for MUA has an approximation factor of 32.

Proof: Assume that $OPT(\mathcal{B})$ is the optimal solution of our original allocation problem, and $OPT_r(\mathcal{B}) = \{i|i \in OPT(\mathcal{B})$ and i is allocated in $g_r\}$. Then, we can get that

$$\begin{aligned} w(OPT(\mathcal{B})) &= \sum_{1\le r\le 4} w(OPT_r(\mathcal{B})) \\ &\le \sum_{1\le r\le 4} w(OPT(g_r)) \\ &\le 4\max\{w(OPT(g_r))\}_{1\le r\le 4}, \end{aligned} \tag{5}$$

where $w(\cdot)$ is an operation to compute the weight of solutions. For each grid g^l_r, we can get that

$$\begin{aligned} w(OPT(g^l_r)) &\le \sum_{1\le s\le 4} w(OPT(g^l_{r,s})) \\ &\le 4\max\{w(OPT(g^l_{r,s}))\}_{1\le s\le 4}. \end{aligned} \tag{6}$$

Since we sort bidders in non-increasing order according to their per-unit bidding prices, so user i has the i-th largest value in $\frac{b_i}{N_i}$ and $\sum_{i=0}^{k} N_i > m$, $\sum_{i=0}^{k} b_i > w(OPT(g^l_{r,s}))$. Our approximation allocation mechanism sets $APP(g^l_{r,s}) = \{1, 2, ..., k-1\}$ if $\sum_{i=0}^{k-1} b_i \ge b_k$; otherwise, we set $APP(g^l_{r,s}) = \{k\}$. Thus,

$$OPT(g^l_{r,s}) \le 2APP(g^l_{r,s}). \tag{7}$$

Because we choose the $APP(g^l_{r,s})$ with biggest weight as $APP(g^l_r)$, we can further get that

$$\begin{aligned} OPT(g^l_r) &\le 4\max(OPT(g^l_{r,s}))_{1\le s\le 4} \\ &\le 8APP(g^l_r). \end{aligned} \tag{8}$$

In a similar way, we can get that

$$\begin{aligned} OPT(\mathcal{B}) &\le 4\max(OPT(g_r))_{1\le r\le 4} \\ &\le 32APP(\mathcal{B}). \end{aligned} \tag{9}$$

□

In the following, we will show the privacy preserving version of our channel allocation mechanism for MUA in Algorithm 5. To protect the bid privacy of bidders, the agent confuses the ID of bidders by using a permutation $\pi : \mathbb{Z}_n \to \mathbb{Z}_n$, and masks the encrypted bids by using two random values $\delta^l_{r,1} \in \mathbb{Z}_{2^{\gamma_1}}$ and $\delta^l_{r,2} \in \mathbb{Z}_{2^{\gamma_1}}$ as $E(\delta^l_{r,1} b_i + \delta^l_{r,2})$ after receiving the encrypted bids. Following by our channel allocation mechanism for MUA, we need to sort the bidders which are allocated in each sub-grid $g^l_{r,s}$ by their bidding prices and find the critical bidder $\sigma(k)$ in the sorted bidder list to decide which bidders should win in $g^l_{r,s}$. This can be easily done by the auctioneer as he has the decryption key. Meanwhile, the auctioneer cannot access any true bid values

Algorithm 4 Channel allocation mechanism for MUA

```
for each sub-grid $g^l_{r,s}$ do
    if The number of channels that all the bidders located in $g^l_{r,s}$ want to buy is larger than $m$ then
        Sorting the bidders that located in $g^l_{r,s}$ in non-increasing order according to their per-unit bid values $\frac{b_i}{N_i}$, where $\sigma(i)$ is the bidder with $i$-th per-unit bid value in the sorted list;
        Find the critical bidder $\sigma(k)$ in the sorted bidder list, which satisfies:
            $$\sum_{i=1}^{k-1} N_{\sigma(i)} \le m < \sum_{i=1}^{k} N_{\sigma(i)};$$
        Set $APP(g^l_{r,s}) = \{\sigma(1), \sigma(2), ..., \sigma(k-1)\}$ if $\sum_{i=1}^{k-1} b_{\sigma(i)} \ge b_{\sigma(k)}$; otherwise, set $APP(g^l_{r,s}) = \{\sigma(k)\}$;
    else
        Set $APP(g^l_{r,s})$ is all the bidders that located in $g^l_{r,s}$;
for each grid $g^l_r$ do
    Set $s' = \arg\max_s \{w(APP(g^l_{r,s})) | 1 \le s \le 4\}$, where $w(\cdot)$ is an operation to compute the weight of solutions.
    Set $APP(g^l_r) = APP(g^l_{r,s'})$;
for $r = 1$ to $4$ do
    Set $APP(g_r) = \bigcup_l APP(g^l_r)$;
Set $r' = \arg\max_r \{w(APP(g_r)) | 1 \le r \le 4\}$;
Return $APP((B)) = APP(g_{r'})$ as the final solution;
```

or the bid order of bidders as the ID and encrypted bid of bidders are permutated or masked by random values. Then, the agent can compute the encrypted bid sums $E(w(APP(g^l_{r,s})))$ for each sub-grid $g^l_{r,s}$ and $E(w(APP(g_r)))$. To hide the true values of $w(APP(g^l_{r,s}))$ and $E(w(APP(g_r)))$ from the auctioneer, the agent masks these encrypted bid sums by random integers either. Then, the agent can decide which buyers should win the auction via communicating with the auctioneer with bid privacy preserving.

Lemma 6: Our allocation mechanism for MUA is bid-monotone.

Proof: Assume bidder i is located in grid $g^l_{r,s}$ and wins the auction by bidding b_i, then he must be in the solutions $APP(g^l_{r,s}), APP(g^l_r)$ and $APP(\mathcal{B})$ at the same time. Thus, we will check if the bidder i still belongs to these solutions when he bids $b'_i > b_i$ in the following.

First, we consider the solution $APP(g^l_{r,s})$. Obviously, the rank of bidder i will not decrease when bidder i increases his bidding value. Thus, b'_i is always larger than the sum bid of the top $k-1$ bidders when $i = \sigma(k)$, which means i will remain in $APP(g^l_{r,s})$ in this case. In another case, all the bidders with top $(k-1)$ per-unit bid remains unchanged when i bids $b'_i > b_i$, and thus their sum bid is still larger than the k-th bid. Thus, i will always win the auction when he increases his bid.

Then, we consider the solutions $APP(g^l_r)$ and $APP(\mathcal{B})$. When i bids $b'_i > b_i$, the $w(APP(g^l_{r,s}))$ will increase, and $w(APP(g^l_{r,s'}))$ will keep unchanged if $s' \neq s$. Thus, $APP(g^l_{r,s})$ still has the highest weight and will be selected as $APP(g^l_r)$. Similarly, $APP(g_r)$ will be selected as the final allocation $APP(\mathcal{B})$ either.

Bidder i will always win by bidding $b'_i > b_i$ if he wins by bidding b_i, *i.e.*, our allocation mechanism is bid-monotone. □

Algorithm 5 Channel allocation mechanism for MUA with bid privacy

```
for each sub-grid $g^l_{r,s}$ do
    if The number of channels that all the bidders located in $g^l_{r,s}$ want to buy is larger than $m$ then
        The agent randomly chooses two integers $\delta^l_{r,1} \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta^l_{r,2} \in \mathbb{Z}_{2^{\gamma_2}}$, computes and sends $(\pi(i), E(\delta^l_{r,1} b_i + \delta^l_{r,2}), N_i)$ to the auctioneer if $i$ is located in $g^l_{r,s}$.
        The auctioneer decrypts and sorts the per-unit bids of bidders in non-increasing order;
        The auctioneer finds the critical bidder $\sigma(k)$ in the sorted bidder list, and sends $(\{\sigma(i)\}_{i<k}, \sigma(k))$ to the agent;
        The agent computes and sends $E(\delta^l_{r,1} \sum_{i=1}^{k-1} b_{\sigma(i)} + \delta^l_{r,2}))$ to the auctioneer;
        The auctioneer sends $\{\sigma(i)\}_{i<k}$ to the agent if $\sum_{i=1}^{k-1} b_{\sigma(i)} \ge b_{\sigma(k)}$; otherwise, he sends $\sigma(k)$;
        The agent sets $APP(g^l_{r,s})$ includes all the bidders that the auctioneer sent to him;
    else
        The agent sets $APP(g^l_{r,s})$ as all the bidders located in $g^l_{r,s}$;
for each grid $g^l_r$ do
    The agent chooses two integers $\delta^l_{r,3} \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta^l_{r,4} \in \mathbb{Z}_{2^{\gamma_2}}$, computes $\{(s, E(\delta^l_{r,3} w(APP(g^l_{r,s})) + \delta^l_{r,4})\}_{1 \le s \le 4}$ and sends them to the auctioneer.
    The auctioneer decrypts the ciphertexts and finds $s' = \arg\max_s \{w(APP(g^l_{r,s})) | 1 \le s \le 4\}$. Then, he sends $s'$ to the agent.
    The agent sets $APP(g^l_r) = APP(g^l_{r,s'})$;
for $r = 1$ to $4$ do
    The agent sets $APP(g_r) = \bigcup_l APP(g^l_r)$;
The agent chooses two integers $\delta^l_1 \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta^l_2 \in \mathbb{Z}_{2^{\gamma_2}}$, computes $\{(r, E(\delta^l_1 w(APP(g_r)) + \delta^l_2)\}_{1 \le r \le 4}$ and sends them to the auctioneer.
The auctioneer decrypts the ciphertexts and finds $r' = \arg\max_r \{w(APP(g_r)) | 1 \le r \le 4\}$. Then, he sends $r'$ to the agent;
The agent sets $APP(\mathcal{B}) = APP(g_{r'})$, and sends $APP(\mathcal{B})$ to the auctioneer as the final solution;
```

4.3 Payment Calculation with Privacy Preserving

After allocating channels to the bidders in our allocation mechanism, we need to compute a critical value for each winner as their payment. We now consider the procedure of payment calculation for a winner i which is located in grid $g^l_{r,s}$.

Since the bidder i wins the auction, we can conclude that:

1) $i \in APP(g^l_{r,s})$;

2) $APP(g_r^l) = APP(g_{r,s}^l)$;
3) $APP(\mathcal{B}) = APP(g_r)$.

We first consider the minimum bid value of bidder i, denoted by p_i^1, with which the bidder i will be put in $APP(g_{r,s}^l)$. In the case that all the bidders located in $g_{r,s}^l$ win the auction, we set $p_i^1 = 0$; otherwise, we assume that $i = \sigma(j)$ in the sorted bidder list of $g_{r,s}^l$ when i bids b_i, then the process of p_i^1 computation is shown in Algorithm 6.

Under the assumption that $APP(g_{r,s}^l)$ keeps unchanged, we suppose p_i^2 is the minimum bid value of bidder i that makes $APP(g_r^l) = APP(g_{r,s}^l)$, p_i^3 is the minimum bid value of bidder i that makes $APP(\mathcal{B}) = APP(g_r)$. Then, we have

$$p_i^2 = \max\{w(APP(g_{r,s'}^l))|s' \neq s\} - w(APP(g_{r,s}^l)) + b_i. \tag{10}$$

$$p_i^3 = \max\{w(APP(g_{r'}))|r' \neq r\} - w(APP(g_r)) + b_i. \tag{11}$$

The critical value of bidder i is $p_i = \max(p_i^1, p_i^2, p_i^3)$. Next we will show that we can compute the critical value for each winner without leaking the true bid value of bidders.

Algorithm 6 p_i^1 computation for winner i in MUA

```
1: Set $j = j + 1$;
2: Set $b_i' = \frac{b_{\sigma(j)} N_i}{N_{\sigma(j)}}$;
3: Run lines $3 \sim 5$ of Algorithm 4 to check if bidder $i$ will win by bidding $b_i'$;
4: if $i$ wins by bidding $b_i'$ then
5:     Repeat steps $1 \sim 3$ until $i$ lose the auction;
6: if $i$ is the $k$-th bidder when he bids $b_i'$ then
7:     Set $p_i^1 = \max(\sum_{q=1}^{k-1} b_{\sigma'(q)}, b_i')$, where $\sigma'(q)$ is the bidder with $q$-th per-unit bid when $i$ bids $b_i'$;
8: else
9:     Set $p_i^1 = \max(b_{\sigma'(k)} + b_i - \sum_{q=1}^{k-1} b_{\sigma'(q)}, b_i')$;
```

Since the agent can compute $E(\delta_{r,1}^l b_i' N_{\sigma(j)} + \delta_{r,2}^l N_{\sigma(j)})$ which is equal to $E(\delta_{r,1}^l b_{\sigma(j)} N_i + \delta_{r,2}^l N_{\sigma(j)})$, the auctioneer can decrypt and compute the value of $\delta_{r,1}^l b_i' + \delta_{r,2}^l$. Thus, the auctioneer and agent can check if bidder i will win the auction by bidding b_i' as they did in lines $3 \sim 7$ of Algorithm 5. Further, the agent can get $\max\{w(APP(g_{r,s'}^l))|s' \neq s\}$ and $\max\{w(APP(g_{r'}))|r' \neq r\}$ via communicating with the auctioneer. Thus, the agent can choose two integers $\delta_1 \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta_2 \in \mathbb{Z}_{2^{\gamma_2}}$ and compute the ciphertexts of $\delta_1 p_i^1 + \delta_2$, $\delta_1 p_i^2 + \delta_2$ and $\delta_1 p_i^3 + \delta_2$ through homomorphic operations, and sends them to the auctioneer. Then, the auctioneer decrypts these ciphertexts, sets $\delta_1 p_i + \delta_2 = \max(\delta_1 p_i^1 + \delta_2, \delta_1 p_i^2 + \delta_2, \delta_1 p_i^3 + \delta_2)$ and sends $\delta_1 p_i + \delta_2$ to the agent. After computing the payment p_i of each winner i, the agent sends them to the auctioneer.

From above analysis, we can conclude that:

Theorem 7: We charge each winner its critical value in PPS-MUA. PPS-MUA is strategyproofness.

4.4 Extended Auction Mechanism for MUA

We have designed a simple allocation mechanism for MUA, which provides an approximation factor of 32. However, PPS-MUA only chooses the solution of a $\frac{1}{2} * \frac{1}{2}$ sub-grid as the final solution of a $2 * 2$ grid, while dropping all the other bidders that located in other 15 sub-grids. Although the allocation in this way provides a guarantee for the worst case performance, the average performance may be relatively low. To address this issue, we extend our allocation mechanism by supplementing the solution with other bidders as shown in Algorithm 7.

Algorithm 7 Extended Allocation Mechanism PPS-EMUA

```
1: Run Algorithm 4 to allocate channels to bidders;
2: Sort all the bidders who lose in Algorithm 4 in non-increasing order according to their bid values.
3: for each loser $i$ in the sorted list do
4:     if we can allocate channels to $i$ without interfering with the existing winners then
5:         Set $i$ wins and allocate channels to him;
```

Lemma 8: The allocation mechanism PPS-EMUA presented in Algorithm 7 is bid-monotone.

Proof: Since we have proved that if the winner i increases his bid in Algorithm 4, he will always win the auction. Here, we only need to concentrate on the winners that lose in Algorithm 4, but will win in the extended version. Suppose such a winner i increases his bid to b_i' which satisfies $b_i' > b_i$, there are two possible cases: 1) i wins in Algorithm 4 and 2) i remains lose in Algorithm 4. In the case that i loses in Algorithm 4, the final allocation of Algorithm 4 is the same as the allocation when i bids b_i. Thus, there is no new bidder whose bidding price is higher than i in the sorted loser list of Algorithm 7 after the bidder i increasing his bid. In addition to i wins by bidding b_i, we can conclude that the bidder i will also win the auction when he increases his bid. □

As this new allocation mechanism is bid-monotone, there exists a critical value for each winner. We use p_i' here to denote the minimum bid value of bidder i with which i will win in Algorithm 4, and p_i'' to denote the minimum bid value of winner i with which i will win in the sorted loser list. According to Algorithm 7, p_i' is the critical value of bidder i in Algorithm 4, and p_i'' should be smaller than p_i'.

For each winner i, his critical value can be computed as follows:

- If i wins in line 1 of Algorithm 7 and will lose as long as he bids $b_i' < p_i'$, his critical value is equal to p_i';
- Otherwise, his critical value is equal to p_i''. Suppose $f(i)$ is the first bidder in the sorted loser list who loses the auction but will win as long as the bidder i's bidding price is smaller than his, then $p_i'' = b_{f(i)}$ if $f(i)$ exits and $p_i'' = 0$ otherwise.

As the extended allocation mechanism is bid-monotone and we always charge each winner its critical value, we have

Theorem 9: PPS-EMUA is strategyproof and social efficient.

In the following, we will show that PPS-EMUA can be performed with privacy preserving. Algorithm 8 shows the allocation mechanism of PPS-EMUA with bid privacy.

The procedure of payment calculation has four steps: 1) We can obtain p_i' for each winner who wins in line 1 of Algorithm

Algorithm 8 PPS-EMUA: Privacy-Preserving Allocation Mechanism

```
The auctioneer and the agent run Algorithm 5;
The agent randomly chooses two integers $\delta_1 \in \mathbb{Z}_{2^{\gamma_1}}$, $\delta_2 \in \mathbb{Z}_{2^{\gamma_2}}$, computes and sends $(\pi(i), E(\delta_1 b_i + \delta_2))$ if bidder $i$ loses in Algorithm 5, and $\{\pi(i), N_i, L_i\}_{i \in \mathcal{B}}$ to the auctioneer;
The auctioneer decrypts the encrypted bids, and run lines $2 \sim 5$ of Algorithm 7;
```

7 and protect the true bid value of bidders by using the method we have introduced previously. 2) The auctioneer and agent can check if bidder i will lose as long as his bid is smaller than p'_i by running Algorithm 8 and assuming i loses in line 1 of Algorithm 7. 3) In the case that i may win when he bids smaller than p'_i, the auctioneer sets $p''_i = 0$ if $f(i)$ does not exist, and sets $p''_i = \delta_1 b_{f(i)} + \delta_2$ if $f(i)$ exists. The auctioneer sends $\delta_1 p'_i + \delta_2$ in the case that p'_i is the critical value of bidder i, and $\delta_1 p''_i + \delta_2$ in other case. 4) With the encrypted critical value, the agent can compute the payment of winner i. After obtaining all the payment of winners, the agent will send them to the auctioneer.

Theorem 10: The computation and communication cost are all $O(n^2)$ for PPS-MUA and PPS-EMUA.

4.5 Privacy Analysis

Theorem 11: PPS-MUA and PPS-EMUA are privacy-preserving for each bidder.

Proof: Here we only prove it for PPS-EMUA as PPS-MUA is a procedure of PPS-EMUA. We first consider the agent. Except the encrypted bids, the agent can only obtain some orders, such as the bidding price of the bidders in each sub-grid, during our auction mechanism of PPS-EMUA. In the process of payment calculation, the agent can get nothing but the auction outcomes and some new orders. Based on the IND-CPA security of homomorphic cryptosystem, the agent cannot learn more information about the bid of any bidder.

Although the auctioneer holds the decryption key, he has no direct access to the encrypted bids. While computing the allocation in each sub-grid $g^l_{r,s}$, the auctioneer can built $|g^l_{r,s}| + 1$ functions that with $|g^l_{r,s}|$ bids and two random numbers, where $|g^l_{r,s}|$ is the number of bidders that located in $g^l_{r,s}$. Since the number of variables is larger than the number of functions, the auctioneer cannot decrypt any true bid value of bidders. In the other parts of our auction mechanism, the auctioneer only receives the weight of solutions. Since the auctioneer has no idea about which bidders are in these solutions, he can also get nothing from them. □

5 Performance Evaluations

5.1 Simulation Setup

In our simulations, the number of bidders varies from 50 to 300, and all the bidders are randomly distributed in a square area. The bidding price of each bidder is uniformly generated in $[0, 100]$. We use a 1024-bit length Pailliers homomorphic encryption system in the simulation. Thus, we choose $\gamma_1 = 1007$ and $\gamma_2 = 1022$ to ensure the correctness of modular operations. For Multi-Unit Auction (MUA), we assume the channel demand of each bidder is randomly generated from 1 to 4, and there are 4 or 8 available channels in spectrum market.

We mainly study the social efficiency ratio, computation overhead and the communication overhead in our simulations. We define the social efficiency ratio is the ratio between the social efficiency of our approximation mechanism and the optimal one. Since agent and auctioneer are two central party in this paper, we evaluate the computation overhead of them in our design by recording the required processing time, and evaluate the communication overhead through calculating the size of essential information transferred in the auction. All the simulations are performed over 100 runs and the result is the averaged value.

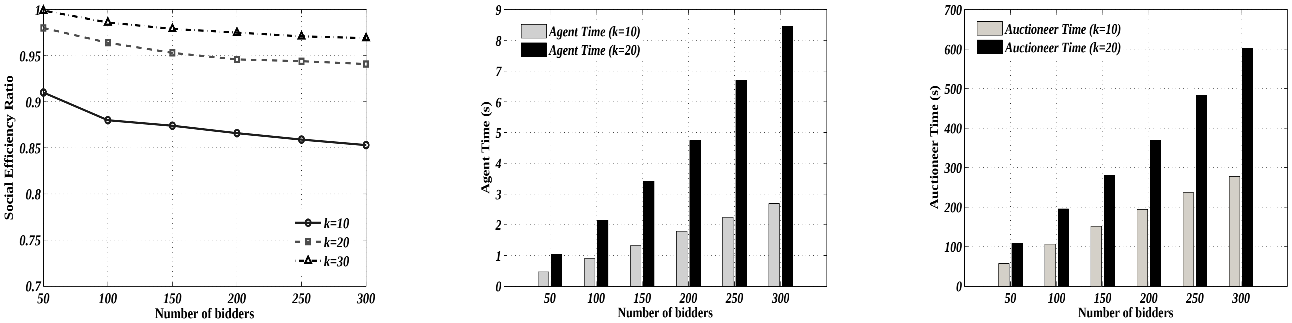
5.2 Performance of the PPS

In this section, we mainly focus on the performance of social efficiency ratio, auction computation overhead, and communication overhead under different simulation settings.

We first study the *social efficiency ratio* of our mechanisms under SUA model and MUA model respectively. From Fig. 3(a) and Fig. 4(a), obviously, the social efficiency ratio decreases when the number of bidders increases. This is because the increasing number of bidders will incur a more fierce degree of competition. Therefore, the social efficiency ratio decreases slightly with the increasing number of bidders in both auction models. Fig. 3(a) also shows that the social efficiency ratio increases when k increases, where k is the size of a subdivided grid. From the theoretical analysis, we can learn that when k increases, less unit-disk defined by bidders' requests are thrown away by using the shifting method. Thus, the social efficiency ratio increases with the increase of parameter k. Of course, the performances of our proposed PPS-SUA is always better than the theoretical bound in performance analysis. Specifically, Fig. 4(a) examines the social efficiency ratio achieved by PPS-MUA and extended version of PPS-MUA (*a.k.a PPS-EMUA*). We can observe that the ratio of PPS-EMUA performs much better than PPS-MUA when the available channels in spectrum market is fixed to 4. We can also observe that the PPS-EMUA greatly improves the performance in Fig. 4(a). This is because the PPS-EMUA adopts a greedy-like allocation mechanism to allocate channels to the potential bidders who lose in PPS-MUA.

Then we study the computation overhead of the proposed mechanisms that were depicted in Fig. 3(b) and Fig. 4(b). It is obvious that the computation overhead of the agent change greatly as the number of bidders and k in PPS-SUA. We can also find that the computation overhead of the agent is increased with the number of bidders, and affected by the changing of the number of channels slightly in Fig. 4(b).

Similar to the agent computation overhead, Fig. 3(c) and Fig. 4(c) plot computation overhead of the auctioneer. We find that the cost time of auctioneer is much larger than that of the agent, this is because that the decryption operation cost much

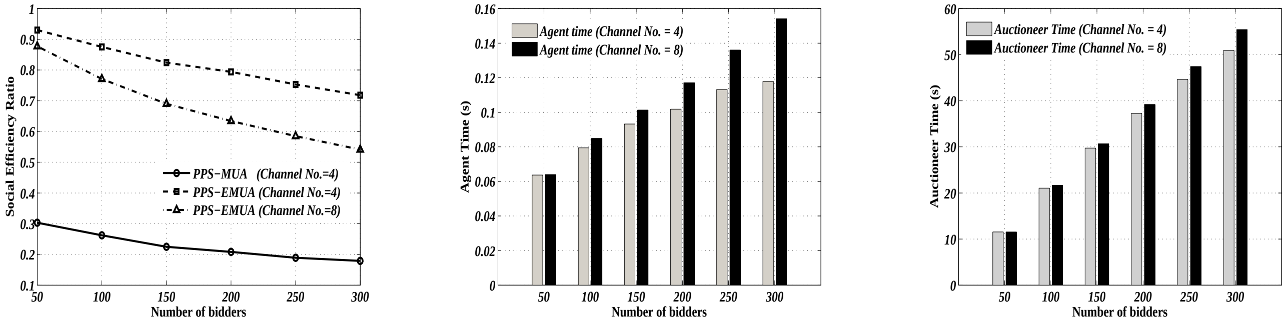


(a) The Performance of Social Efficiency Ratio under SUA model

(b) The Computation Overhead of the agent

(c) The Computation Overhead of the Auctioneer

Fig. 3: The performance of PPS under SUA model. Here all the bidders are uniformly distributed in a 100 × 100 square area.



(a) The PPS-MUA and PPS-EMUA Performance of Social Efficiency Ratio under MUA model

(b) The Computation Overhead of the Agent

(c) The Computation Overhead of the Auctioneer

Fig. 4: The performance of PPS under MUA model. Here all the bidders are uniformly distributed in a 100 × 100 square area, and the channel demand of each bidder is randomly generated from 1 to 4.

TABLE 1: Communication Overhead under SUA model (KB)

k	Number of bidders					
	50	100	150	200	250	300
k=10	124	233	333	428	521	611
k=20	231	416	601	799	1026	1273
k=30	327	603	926	1312	1779	2619

more time than the homomorphic operations and auctioneer is responsible for all the decryption operations.

Table 1 and Table 2 show the overall communication overhead induced under SUA and MUA respectively. We can easily get that the communication overhead is increased with the increment of number of bidders and k in Table 1. In Table 2, the total number of channels also plays an important role in the cost of communication overhead. Anyway, the overheads of the proposed PPS mechanism are appropriate to be applied in real auction systems.

6 Literature Reviews

6.1 Spectrum Auction

Auctions have been widely used in the scope of dynamic spectrum allocation. Large amount of studies are proposed aiming at designing economical robust spectrum auction mechanisms (*e.g.* [2], [7], [8], [10], [12], [28]–[30], [32], [34], [37]–[41]). One line of work on spectrum auction is based on studying auction with spectrum spatial reuse, *e.g.* [11], [15], [29], [30], [31], [38] and *etc.* The basic idea is that the spectrum can be reused by s set of conflict-free winning buyers. However, a number of recent studies have shown that the spectrum utilization varies dramatically, both in the spatial and temporal domains [36]. The above studies do not consider the temporal demands from buyers, where each buyer may only require a channel within a certain period of time and different buyers may have different time periods. Thus, another line is based on spectrum temporal reuse, *e.g.* [8], [28]. These studies ignore spatial reuse by assuming that the conflict graph amongst buyers geometry locations is a completed graph for each channel.

Each of these approaches has its own optimization goal. For instance, [8], [10], [32], [38], [40] focus on maximizing the social efficiency while ensuring strategyproofness in an auction design, and [2], [15] aim at achieving the optimal revenue for the primary user. Moreover, most above auction mechanisms were designed to achieve strategyproofness, without considering performance guarantee.

In [7], [28], [33], [34], the authors consider the strategyproof online spectrum auction or allocation design. Wu *et al.* [30] and Xu *et al.* [32], [34] proposed spectrum auction mechanisms for multi-channel wireless networks. Wang *et al.* [29] and Zhou *et al.* [39] solve the spectrum allocation in a double auction framework. Unfortunately, none of the above studies addresses the privacy preserving issue in the auction

TABLE 2: Communication Overhead under MUA model (KB)

Channel Number	Number of bidders					
	50	100	150	200	250	300
4	33.5	61.9	87.5	110.8	132.2	153.0
8	34.2	63.7	90.7	117.2	140.6	164.1
12	34.4	63.8	91.1	116.7	142.0	165.1

design.

6.2 Privacy Preserving Spectrum Auction

Privacy preserving, one of the critical human factors, has gained increasing attentions recently. Many privacy preserving mechanisms have been proposed in mechanism design [5], [16], [18], [21], [27]. Recent years, many research efforts begin to focus on privacy preserving study in auction design, *e.g.* [3], [4], [24]. Brandt *et al.* [3] studied unconditional full privacy in the sealed-bid auctions. Naor *et al.* [24] proposed an architecture for auction mechanism design with the goal of preserving the privacy of the inputs of the participants while maintaining communication and computational efficiency. However, these methods cannot be directly applied in spectrum auction design due to various reasons (such as spectrum spatial reuse, computationally complexity).

Huang *et al.* [13] first proposed a strategyproof spectrum auction with consideration of privacy preserving, and Pan *et al.* [26] provided a secure spectrum auction to prevent the frauds of the insincere auctioneer. Unfortunately, none of the existing solutions with privacy preserving provides any performance guarantee, such as maximizing the social efficiency which is often NP-hard. Designing a strategyproof auction mechanism with provable performance guarantee is a harder problem, particularly if we want to support privacy preservation. Our mechanisms rely on privacy preserving comparison and polynomial evaluations [17], which is extensively studied topic in secure multi-party computation [1], [6], [9], [35].

7 Conclusion

In this paper, we focused on designing strategyproof auction mechanisms which maximize the social efficiency without leaking any true bid value of bidders, and proposed a framework of PPS for solving this issue. We designed privacy-preserving strategyproof auction mechanisms with approximation factors of $(1+\epsilon)$ and 32 separately for SUA and MUA. Our evaluation results demonstrated that both PPS-SUA and PPS-EMUA achieve good performance on social efficiency, while inducing only a small amount of computation and communication overhead. A future work is to design robust privacy-preserving strategyproof auction mechanisms without inexplicitly requiring the location of bidders. Another future work is to design privacy-preserving auction mechanisms by removing the dependency of third-party agent.

Acknowledgement

Yu-e Sun is the corresponding author. The research of authors is partially supported by NSF CNS-0832120, NSF CNS-1035894, NSF ECCS-1247944, NSF ECCS-1343306, National Natural Science Foundation of China under Grant No. 61170216, No. 61228202, No. 61303206, No. 61202028, No. 61373164. Specialized Research Fund for the Doctoral Program of Higher Education (SRFDP) under Grant No. 20123201120010. 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 (NSF, and NSFC).

References

[1] G. Aggarwal, N. Mishra, and B. Pinkas. Secure computation of the k*th*-ranked element. In *Advances in Cryptology-EUROCRYPT 2004*, pages 40–55, 2004.

[2] M. Al-Ayyoub and H. Gupta. Truthful spectrum auctions with approximate revenue. In *IEEE INFOCOM*, pages 2813–2821, 2011.

[3] F. Brandt and T. Sandholm. On the existence of unconditionally privacy-preserving auction protocols. *ACM Transactions on Information and System Security (TISSEC)*, 11(2):6, 2008.

[4] C. Cachin. Efficient private bidding and auctions with an oblivious third party. In *ACM CCS*, pages 120–127, 1999.

[5] I. Damgård, M. Geisler, and M. Krøigaard. Efficient and secure comparison for on-line auctions. In *Proceedings of the Springer Information Security and Privacy*, pages 416–430, 2007.

[6] I. Damgård, M. Geisler, and M. Krøigaard. Homomorphic encryption and secure comparison. *International Journal of Applied Cryptography*, 1(1):22–31, 2008.

[7] L. Deek, X. Zhou, K. Almeroth, and H. Zheng. To preempt or not: Tackling bid and time-based cheating in online spectrum auctions. In *IEEE INFOCOM*, pages 2219–2227, 2011.

[8] M. Dong, G. Sun, X. Wang, and Q. Zhang. Combinatorial auction with time-frequency flexibility in cognitive radio networks. In *IEEE INFOCOM*, pages 2282–2290, 2012.

[9] W. Du and M. J. Atallah. Secure multi-party computation problems and their applications: a review and open problems. In *Proceedings of the 2001 workshop on New security paradigms*, pages 13–22, 2001.

[10] A. Gopinathan and Z. Li. Strategyproof wireless spectrum auctions with interference. In *IEEE GLOBECOM*, pages 1–5, 2010.

[11] A. Gopinathan, Z. Li, and C. Wu. Strategyproof auctions for balancing social welfare and fairness in secondary spectrum markets. In *Proceedings of the INFOCOM 2011*, pages 2813–2821, 2011.

[12] 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 *ACM MOBIHOC*, pages 237–240, 2013.

[13] Q. Huang, Y. Tao, and F. Wu. SPRING: A strategy-proof and privacy preserving spectrum auction mechanism. In *IEEE INFOCOM*, pages 851–859, 2013.

[14] H. Hunt III, M. Marathe, V. Radhakrishnan, S. Ravi, D. Rosenkrantz, and R. Stearns. Nc-approximation schemes for np-and pspace-hard problems for geometric graphs. *Journal of Algorithms*, 26(2):238–274, 1998.

[15] J. Jia, Q. Zhang, Q. Zhang, and M. Liu. Revenue generation for truthful spectrum auction in dynamic spectrum access. In *ACM MOBIHOC*, pages 3–12, 2009.

[16] T. Jung and X.-Y. Li. Collusion-tolerable privacy-preserving sum and product calculation without secure channel. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2014.

[17] T. Jung, X.-Y. Li, and S. Tang. Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation. In *IEEE INFOCOM*, pages 2634–2642, 2013.

[18] T. Jung, X.-Y. Li, Zhiguo Wan, and Meng Wan. Privacy preserving cloud data access with multi-authorities. In *IEEE INFOCOM*, pages 2625–2633, 2013.

[19] V. Krishna. *Auction theory*. Academic press, 2009.

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

[21] Q. Li and G. Cao. Providing privacy-aware incentives for mobile sensing. In *IEEE Percom*, pages 76–84, 2013.

[22] X.-Y. Li and T. Jung. Search me if you can: Privacy-preserving location query service. In *IEEE INFOCOM*, pages 2760–2768, 2013.

[23] X.-Y. Li and Y. Wang. Simple approximation algorithms and ptass for various problems in wireless ad hoc networks. *Journal of Parallel and Distributed Computing*, 66(4):515–530, 2006.

[24] M. Naor, B. Pinkas, and R. Sumner. Privacy preserving auctions and mechanism design. In *ACM conference on Electronic commerce*, pages 129–139, 1999.

[25] N. Nisan, T. Roughgarden, E. Tardos, and V. Vazirani. *Algorithmic game theory*. Cambridge University Press, 2007.

[26] M. Pan, J. Sun, and Y. Fang. Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem. *IEEE Journal on Selected Areas in Communications*, 29(4):866–876, 2011.

[27] X. Sui and C. Boutilier. Efficiency and privacy tradeoffs in mechanism design. In *IEEE AAAI*, pages 738–744, 2011.

[28] 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 *IEEE DYSPAN*, pages 1–10, 2010.

[29] W. Wang, B. Li, and B. Liang. District: Embracing local markets in truthful spectrum double auctions. In *IEEE SECON*, pages 521–529, 2011.

[30] F. Wu and N. Vaidya. SMALL: A strategy-proof mechanism for radio spectrum allocation. In *IEEE INFOCOM*, pages 3020–3028, 2011.

[31] H. Xu, J. Jin, and B. Li. A secondary market for spectrum. In *IEEE INFOCOM*, pages 1–5, 2010.

[32] P. Xu, X.Y. Li, and S. Tang. Efficient and strategyproof spectrum allocations in multichannel wireless networks. *IEEE Transactions on Computers*, 60(4):580–593, 2011.

[33] P. Xu, S.G. Wang, and X.Y. Li. SALSA: Strategyproof online spectrum admissions for wireless networks. *IEEE Transactions on Computers*, 59(12):1691–1702, 2010.

[34] P. Xu, X. Xu, S. Tang, and X.-Y. Li. Truthful online spectrum allocation and auction in multi-channel wireless networks. In *IEEE INFOCOM*, pages 26–30, 2011.

[35] Andrew Chi-Chih Yao. Protocols for secure computations. In *FOCS*, pages 160–164, 1982.

[36] S. Yin, D. Chen, Q. Zhang, M. Liu, and S. Li. Mining spectrum usage data: a large-scale spectrum measurement study. *IEEE Transactions on Mobile Computing*, 11(6):1033–1046, 2012.

[37] Z. Zheng, F. Wu, and G. Chen. SMASHER: Strategy-proof combinatorial auction mechanisms for heterogeneous channel redistribution. In *ACM MOBIHOC*, pages 305–308, 2013.

[38] X. Zhou, S. Gandhi, S. Suri, and H. Zheng. ebay in the sky: strategy-proof wireless spectrum auctions. In *ACM Mobicom*, pages 2–13, 2008.

[39] X. Zhou and H. Zheng. TRUST: A general framework for truthful double spectrum auctions. In *IEEE INFOCOM*, pages 999–1007, 2009.

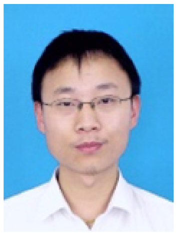
[40] Y. Zhu, B. Li, and Z. Li. Truthful spectrum auction design for secondary networks. In *IEEE INFOCOM*, pages 873–881, 2012.

[41] Y. Zhu, B. Li, and Z. Li. Core-selecting combinatorial auction design for secondary spectrum markets. In *IEEE INFOCOM*, pages 1986–1994, 2013.

He Huang Dr. He Huang is an associate professor in the School of Computer Science and Technology at Soochow University, P.R. China. He received his Ph.D. degree in Department of Computer Science and Technology 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 Dr. Xiang-Yang Li is a professor at the Illinois Institute of Technology. He holds EMC-Endowed Visiting Chair Professorship at Tsinghua University. He currently is distinguished visiting professor at Xi'An JiaoTong University and University of Science and Technology of China. He is a recipient of China NSF Outstanding Overseas Young Researcher (B). Dr. Li received MS (2000) and PhD (2001) degree at Department of Computer Science from University of Illinois at Urbana-Champaign, a Bachelor degree at Department of Computer Science and a Bachelor degree at Department of Business Management from Tsinghua University, P.R. China, both in 1995. His research interests include mobile computing, cyber physical systems, wireless networks, security and privacy, and algorithms. He published a monograph ”Wireless Ad Hoc and Sensor Networks: Theory and Applications”. Dr. Li is an editor of several journals, including IEEE Transaction on Parallel and Distributed Systems, IEEE Transaction on Mobile Computing. He has served many international conferences in various capacities. He is a senior member of IEEE and a member of ACM.

Yu-e Sun Dr. Yu-e Sun is a Lecturer of Urban Rail Transportation Department, Soochow University, P.R. China. She received her Ph.D. degree in Shenyang Institute of Computing Technology from Chinese Academy of Science. Her current research interests 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.



Hongli Xu Hongli Xu received his Ph. D degree in Computer Science from the University of Science and Technology of China in 2007. Currently, he is a post-doctor in the School of Computer Science and Technology at the University of Science and Technology of China. His main research interest is wireless sensor networks, wireless mesh network and cooperative communications.

Liusheng Huang Liusheng Huang received the M.Sc. degree in computer science from University of Science and Technology of China, Hefei, P.R. China, in 1988. He is currently a Professor and Ph.D. Supervisor with the School of Computer Science and Technology, University of Science and Technology of China. He has published six books and more than 200 papers. His research interests are in the areas of wireless networks, information security, distributed computing, VANET, and algorithms.