MastDP: Matching Based Double Auction Mechanism for Spectrum Trading with Differential Privacy

Feng Hu*, Bing Chen*, Jingyi Wang†, Ming Li‡, Pan Li§, Miao Pan¶
*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
†Department of Computer Science, San Francisco State University, San Francisco, USA
‡Department of Computer Science and Engineering, University of Texas at Arlington, USA
§Department of Electrical Engineering and Computer Science, Case Western Reserve University, USA
¶Department of Electrical and Computer Engineering, University of Houston, Houston, USA
{huf, cb_china}@nuaa.edu.cn, Jingyiwang@sfsu.edu, ming.li@uta.edu, lipan@case.edu, mpan2@uh.edu

***Abstract*—The auction mechanism is deemed to be an effective method to address the problem of spectrum scarcity. Numerous spectrum auction mechanisms can alleviate spectrum shortage under the consideration of truthfulness, social welfare maximization and spectrum reusability, while the privacy preservation and preferences of primary/secondary users have not been fully discussed. In this paper, we propose a matching based double auction mechanism for spectrum trading with differential privacy (MastDP) to protect the privacy of buyers/sellers from the untrustworthy auctioneer, other buyers/sellers and other potential parties. Each participant adds distributed differential private noise following $Geom(\alpha)$ distribution to his bid value and encrypts the noisy bid value. The auctioneer can decrypt only the sum of all uploaded noisy bid values and determines the clearing price by using its private key. Based on the clearing price, the matching theory is adopted to maximize the winning participants' revenue while fully considering their preferences and spectrum reuse. Simulation results show that MastDP achieves satisfactory performance in terms of economic properties' privacy preservation and spectrum trading efficiency.**

***Index Terms*—Cognitive radio network, double auction mechanism, matching theory, differential privacy.**

I. Introduction

With the increase of multimedia services, the demand for bandwidth and data rate is increasing [1]. However, in the past few decades, the vast majority of available frequency bands have been exhausted by radio regulatory agencies in various countries. *How to efficiently use limited spectrum resources has drawn significant attention in both industry and academia.* The cognitive radio (CR) technology has been identified as a promising solution for the spectrum scarcity because of its ability to dynamically utilize spectrum resources. Owing to the fairness and allocation efficiency, auction theory has been widely applied to solve the spectrum trading in cognitive radio networks (CRN) [2], [3]. To ensure the performance of spectrum auctions and maximize the benefits of auction participants, strategy-proofness is an important index to evaluate the performance of auction mechanism [4]. However, different from the way that an item can only be sold to one buyer in the traditional auction, spectrum has the reusability in time, space and frequency domain. Moreover, the heterogeneity of spectrum resources make the interference relationship among different buyers in different frequencies different, while the current researches on spectrum reuse [5]–[7] assume that the interference relationship of buyers in all spectrum resources is the same. Obviously, this assumption is rarely valid when the frequency of the auctioned spectrum is quite different.

Double auction is widely used in spectrum trading, while existing truthful double auction designs [8], [9], first form a super buyer by grouping buyers who bid the same channel for each seller and select a group bid for each super buyer. After grouping, the double auction was transformed into multiple single seller-buyer McAfee auctions. It may cause the auction untruthful, since buyers can manipulate their bids to reduce their shares in the group bid while the group also wins the auction. On the other hand, existing spectrum auction mechanism requires each bidder to report its true valuation, while once the bidder's true valuation is reported, the other bidders can infer the bidder's private valuation based on the outcome of the auction. Yet, most existing spectrum auction mechanisms do not consider the privacy-preserving auction or merely concentrate on the bidding privacy in single-sided auctions [10]–[12]. Moreover, how to design a privacy-preserving double auction mechanism is rarely investigated.

In order to address the above mentioned challenges, in this paper, we proposed MastDP, a **M**atching based double **A**uction mechanism for **S**pectrum **T**rading with **D**ifferentially **P**rivacy. We first consider the market of spectrum trading as a double auction, in which there are multiple sellers, multiple buyers, and a single third-party auctioneer. Then, we exploit the distributed differential privacy mechanism to guarantee participants' bid privacy. The main contribution of this work are as follows:

- MastDP integrates the differential privacy mechanism with double auction to protect bidders' privacy without high computational and communication overheads, and achieves ϵ-differential privacy.

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

- We present a many to many spectrum matching approach to achieve winning participants allocation in MastDP considering participants' preferences and spectrum reuse.
- We theoretically prove that the proposed MastDP is individual rationality and incentive compatible.
- We implement the proposed MastDP and extensively compare its performance with existing mechanisms. The simulation results show that MastDP can achieve better performance on both spectrum trading efficiency and bid privacy preservation.

The rest of paper is organized as follows. We present the system model and some related solution concepts in Section II. In Section III and Section IV, we present design details of our proposed double auction mechanism and theoretically prove its properties. Section V reports our performance evaluation results. Finally, we draw a conclusion in VI.

II. Preliminaries and System Model

A. System Model

We consider a double auction market that consists of M Primary users (PUs) who are the spectrum owners and sellers, N Secondary users (SUs) who are spectrum buyers, and an auctioneer who performs the running of double auction mechanism periodically.

We suppose that there is a set of sellers, denoted by $\mathcal{S} = \{s_1, s_2, s_i, ..., s_m\}, (1 \leq i \leq m)$. Moreover each seller s_i has one channel, denoted by l_i, in addition, a channel can be allocated to multiple buyers, if these buyers can communicate simultaneously. We use $\mathcal{V}^s = (v_1^s, v_2^s, v_i^s, ..., v_m^s)$ and $\mathcal{B}^s = (b_1^s, b_2^s, b_i^s, ..., b_m^s)$ to represent seller s_i's true valuation profile and bid profile for the channel. Similarly, there is a set of buyers, denoted by $\mathcal{R} = \{r_1, r_2, r_j, ..., r_n\}, (1 \leq j \leq n)$. We use $\mathcal{V}^r = \left(v_1^r, v_2^r, v_j^r, ..., v_n^r\right)$ and $\mathcal{B}^r = \left(b_1^r, b_2^r, b_j^r, ..., b_n^r\right)$ to denote the buyer r_j's true valuation profile and bid profile for the sellers' channels. The auctioneer sets the price to determine the set of winning sellers who do not interfere with each other and the set of winning buyers, thereby maximizing the total revenue. The outcome of an auction includes an allocation matrix, denoted by $\mathcal{A} = (a_{j,i})$, and a payment profile $\mathcal{P}\left(p_1, p_2, p_j, ..., p_n\right)$, where $a_{j,i}$ means buyer j successfully obtain the channel i,

$$a_{j,i} = \begin{cases} 1, & \text{the channel } i \text{ is allocated to buyer } j; \\ 0, & \text{otherwise.} \end{cases}$$

As each seller and buyer are considered selfish and individual rationality in double auction, after the auction, the utility of all sellers are the payment they receive minus their true valuation for all sold channel:

$$u_s = \sum_{i \in m} \sum_{j \in n} p_j a_{j,i} - \sum_{i \in m} v_i^s.$$

Similarly, the utility of buyers are the true valuation for the sold channel minus their total payment:

$$u_r = \sum_{j \in n} v_j^r - \sum_{i \in m} \sum_{j \in n} p_j a_{j,i}.$$

Analogously, the conflict relationship among multiple SUs over the same band can be defined by the interference range. We note that spectrum is heterogeneous, so different frequencies have different transmission range, different coverage, and interference range.

Buyer's and Seller's Preference*:* For the buyer r_j, he prefers to buy a channel to maximize his data transmission rate. We use $\succ_{r_j}$ denote the preference list of buyer r_j. For instance, $s_1 \succ_{r_j} s_2 \succ_{r_j} s_3$ indicates that seller s_1 is the largest favorite of r_j while r_j's least favorite is seller s_3. Since the buyer's transmission rate is closely related to the capacity of the channel [13], the preference relationship of r_j over two given sellers s_i and s_i' can be expressed as

$$s_i \succ_{r_j} s_i' \Leftrightarrow c_i >_{r_j} c_i'. \qquad (1)$$

On the other hand, a seller s_i prefers to sell his channel to maximize his revenue, since the bid price of each buyer is different, the preference relationship of s_i over two given buyer sets g_{r_j} and g_{r_j}' can be constructed as

$$g_{r_j} \succ_{s_i} g_{r_j}' \Leftrightarrow b_{g_{r_j}} >_{s_i} b_{g_{r_j}}'. \qquad (2)$$

B. Solution Concepts

1) Privacy Preservation: Differential privacy is a new model of cyber security that can protect personal data far better than traditional methods. It ensures that the probability of a statistical query will produce a given result is (nearly) the same whether it's conducted on the first or second database.

Definition 1 (ϵ-differential Privacy [14])**.** *A randomized mechanism $\mathcal{M}$ gives ϵ-differential privacy if for all data sets $\mathbf{D}_1$ and $\mathbf{D}_2$ differing on a single user, and all $S \subseteq$ Range $(\mathcal{M})$,*

$$\mathbf{Pr}\left[\mathcal{M}\left(\mathbf{D}_1 \in \mathcal{S}\right)\right] \leq \exp\left(\epsilon\right) \times \mathbf{Pr}\left[\mathcal{M}\left(\mathbf{D}_2 \in \mathcal{S}\right)\right],$$

where $\epsilon > 0$ is a small constant.

Definition 2 (Laplace Mechanism [14])**.** *Given a function $f : \mathcal{D} \to \mathcal{R}^d$ over a dataset $\mathbf{D}$, mechanism $\mathcal{M}$ provides the ϵ-differential privacy if it follow*

$$\mathcal{M}\left(D\right) = f\left(D\right) + Lap\left(\Delta f / \epsilon\right),$$

where the noise $Lap\left(\Delta f/\epsilon\right)$ is drawn from a Laplace distribution with mean zero and scale $\Delta f/e$.

Definition 3 (l_1-sensitivity)**.** *Let $\boldsymbol{f} : \mathcal{D} \to \mathcal{R}^d$ be a deterministic function. The l_1-sensitivity of $\boldsymbol{f}$ is:*

$$\Delta f = \max_{x, y \in \mathcal{R}^d} \left\| \boldsymbol{f}\left(x\right) - \boldsymbol{f}\left(y\right) \right\|_1$$

We use l_1-sensitivity to represent the largest difference between the values of $\boldsymbol{f}$ of any two neighboring datasets.

2) Matching Theory: Matching theory is a promising approach to provide low complexity and tractable solutions for the combinatorial problem of matching players from two distinct sets, while considering the preference of each player.

Definition 4 (Pairwise Block)**.** *Given a matching result μ, there is a pair (r_x, s_y) that is said to be a blocking pair if the following conditions are satisfied:*

(i) *r_x is unassigned or prefers s_y to his allocated channel, and*

(ii) *s_y is under subscribed or prefers r_x to his worst allocated buyer.*

Definition 5 (Pairwise Stable)**.** *A matching μ is pairwise stable if it is individual rationality and there is no pairwise block of μ.*

III. Auction Design of MastDP

A. Distributed Differential Private Participant Bidding

Most of the previous studies assumed that the auctioneer was trustworthy, while an untrustworthy auctioneer would manipulate the auction based on the participant's bid. In order to prevent the frauds of the auctioneer, we make the auctioneer merely obtain the sum of the bid values uploaded by all the participants, and can not learn any part of the information, as well as employ encryption technology to ensure that multiple ciphertexts from participants can only be decrypted by the auctioneer to protect bid values from other buyers/sellers and other potential parties.

1) Adding Geometric Noise: The previous studies implemented differential privacy protection by adding random noise that obeys the Laplace distribution. However, if such noise is added to each participant, the auctioneer may not only accumulate too much noise, but excessive noise may cause huge errors to the true bid values. Similar to [15], we attempt to reduce the noise added by each participant, while the sum of the noise accumulated in the auctioneer is large enough to protect the privacy. Each seller/buyer adds a noise e_i^s or e_j^r following geometrically distribution $Geom\left(\alpha\right)$ to their bid values. Let $\tilde{b_i^s}$ denote additive noise e_i^s to seller s_i's bid value b_i^s, i.e. $\tilde{b_i^s} = b_i^s + e_i^s$. Analogously, $\tilde{b_j^r} = b_j^r + e_j^r$ denote additive noise e_j^r to buyer r_j's bid value b_j^r.

2) Encrypting Bid Values: Let $\mathcal{G}$ denote a cyclic group of prime order p, in which the Decisional Diffie-Hellman Problem is hard to solve. Let $\mathcal{H} : \mathcal{Z} \to \mathcal{G}$ denote a hash function. First of all, the auctioneer chooses a random generator $g \in \mathcal{G}$ and $m + 1$ random secret keys $sk_0, sk_1, \cdot\cdot\cdot, sk_m \in \mathcal{Z}_p$, as well as $sk_0 = -(sk_1 + sk_2 + \cdots + sk_m)$. The public parameter is g. Each seller s_i obtains the private key sk_i and the auctioneer obtains the private key sk_0. Similarly, the auctioneer chooses $n+1$ random secrets $sl_0, sl_1, \cdots, sl_n \in \mathcal{Z}_p$ for spectrum buyers. Then each seller s_i encrypts his noise-added bid value b_i^s with the private key sk_i as:

$$c_s \leftarrow \boldsymbol{g}^{\tilde{b_i^s}} \cdot \mathcal{H}\left(k\right)^{sk_i},$$

Meanwhile, each buyer r_j encrypts his noise-added bid value b_j^r with the private key sl_j as:

$$c_r \leftarrow \boldsymbol{g}^{\tilde{b_j^r}} \cdot \mathcal{H}\left(k\right)^{sl_j}.$$

Finally, all buyers and sellers submit their encrypted bid values to the auctioneer.

B. Distributed Differential Private Clearing Price Determination

1) Decrypting Bid Values: The auctioneer obtains the sum of decrypted sellers' bid values by summing up these encrypted values and its own secret key sk_0,

$$A_s \leftarrow \mathcal{H}\left(k\right)^{sk_0} \prod_{i=1}^{m} c_s,$$

where,

$$A_s = \mathcal{H}\left(k\right)^{sk_0} \cdot \prod_{i=1}^{m} c_s = \mathcal{H}\left(k\right)^{\sum_{i=0}^{m} sk_i} \cdot \boldsymbol{g}^{\sum_{i=1}^{m} \tilde{b_i^s}}.$$

Since the sk_i sum to zero, $\mathcal{H}\left(k\right)^{\sum_{i=0}^{m} sk_i} = 1$.

$$A_s = \boldsymbol{g}^{\sum_{i=1}^{m} \tilde{b_i^s}}.$$

Consequently, the auctioneer can obtain the sellers' bid sum $\sum_{i=1}^{m} \tilde{b_i^s}$ by computing the discrete log of A_s base $\boldsymbol{g}$, i.e,

$$\sum_{i=1}^{m} \tilde{b_i^s} = \log_{\boldsymbol{g}} A_s.$$

Analogously, the auctioneer obtains the decrypted buyer's bid sum by summing up these encrypted values and its own secret key sl_0.

2) Determining Clearing Price: The clearing price for each participant can be calculated by dividing the bid value by the total number of all sellers and buyers,

$$P_c = \frac{\sum_{i=1}^{m} \tilde{b}_i^s + \sum_{j=1}^{n} \tilde{b}_j^r}{m+n},\ 1 \leq i \leq m, 1 \leq j \leq n. \quad (3)$$

According to the clearing price P_c, the winner candidates can be selected: all the sellers who bid values less than P_c can sell and all buyers who bid values larger than P_c can purchase. Therefore, the final trade price from all winning buyers b_j^{win} to the winning spectrum sellers s_i^{win} is the sum of the clearing price.

C. Winner Allocation with Preferences

After differential private bid values submission and clearing price determination, winning sellers' spectrum can be allocated to winning buyers considering their preference by exploiting matching theory.

1) Generating Conflict Graph and Maximal Independent Set: Due to the spectrum reusability, multiple non-interfering winning buyers can be allocated for one spectrum to maximize seller's revenue. We use conflict graph $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$ to describe the interference relationship of seller among winning buyers. In graph $\boldsymbol{G}$, each vertex and edge denote all buyers bid for the spectrum seller and the interference relationship of them, respectively. An edge connecting two buyers indicates they interfere with each other when transmitting via the same spectrum. Consequently, which buyers can be allocated to one seller at the same time is transformed into finding maximal independent set on the conflict graph.

2) Spectrum Matching with Evolving Preferences: We achieve a stable and non-interference spectrum matching for winning participants by using many to many matching algorithm. We let $\varPhi\left(i,j\right)$ denotes the procedure of spectrum matching as follows:

$$\varPhi\left(i,j\right)=\begin{cases}\mathcal{F}_{s_i}\left(\mu\left(s_i^{win}\right),PL\left(s_i^{win}\right)\right), & \forall 1\leq i\leq m\\ \mathcal{F}_{r_j}\left(\mu\left(r_j^{win}\right),PL\left(r_j^{win}\right)\right), & \forall 1\leq j\leq n\end{cases} \tag{4}$$

The target of our spectrum matching on spectrum seller is to search the optimal set of winning buyers to maximize its revenue, given sellers' preference lists. Note that we set the clearing price to the final payment price for each winning buyer, thus winning sellers obtain a uniform price from each buyer. We perform the procedure of spectrum matching $\varPhi\left(i,j\right)$ to choose the buyer with the largest preference for all winning seller in the first round, and iterative execute the $\varPhi\left(i,j\right)$ for the remaining winning buyers who start to proposed to sellers following the order of preference list while they do not allocated yet, given the evolved conflict graph eliminating vertices of already matched buyers and corresponding edges that no longer exist from the second round until the current round when there are no winning buyers/sellers to be matched.

3) Rematching with Participants Exchanging: After all sellers have completed the above matching process, buyer r_j^{win*} will try to be matched to seller s_i^{win*} when buyer r_j^{win*} is more inclined to the current matching s_i^{win}, i.e. $s_i^{win*}\succ_{r_j^{win*}} s_i^{win}$. Then, the seller s_i^{win*} verifies whether accepting buyer r_j^{win*} and buyers who don not interfere with r_j^{win*} will gain more revenue than the current matching. If the revenue can be increased, the buyer r_j^{win*} is exchanged from the current matching result to the seller s_i^{win*}, and the buyers who conflicts with this buyer will be removed.

IV. Theoretical Analysis

Theorem 1 (Individual Rationality)**.** *The matching result of the proposed MastDP algorithm is individual rationality.*

Proof: It can be easily proved that we select winning participants with a uniform clearing price, thus on the one hand each buyer prefers the current set of matched spectrum sellers who can maximize their communication rate to any subset of these sellers in the final matching. On the other hand, each seller prefers the current set of matched buyers who can maximize their revenue to any subset of these buyers. Therefore, the matching result of the proposed MastDP algorithm is individual rationality. ■

Theorem 2 (Pairwise Stability)**.** *The matching result of the proposed MastDP algorithm is pairwise stability.*

Proof: We have already proved that the algorithm is individual rationality. According to Definition 5, to prove that the matching result of the proposed MastDP algorithm is pairwise stability, we just need to prove that there is no pairwise block in the result of the MastDP algorithm. We suppose that the final matching result exists blocking pairs, i.e., for winning buyers, $\exists r_x,\exists s_y,\ r_x\notin\mu\left(s_y\right)$, $r_x\in\mathcal{F}_{r_x}\left(\mu\left(s_y\right)\cup r_x,PL\left(s_y\right)\right)$, and for winning sellers, $s_y\notin\mu\left(r_x\right)$, $s_y\in\mathcal{F}_{s_y}\left(\mu\left(r_x\right)\cup s_y,PL\left(r_x\right)\right)$. Thus it is obviously true that $\mu\left(r_x\right)\neq\mathcal{F}_{s_y}\left(\mu\left(r_x\right)\cup s_y,PL\left(r_x\right)\right)$, and $\mu\left(s_y\right)\neq\mathcal{F}_{r_x}\left(\mu\left(s_y\right)\cup r_x,PL\left(s_y\right)\right)$. This means that winning buyer r_x prefers to be allocated to another seller rather than its current matching result, besides winning seller s_y prefers to accept another seller rather than its current matching result for more revenue. Since the pairwise blocks will be rematched, we can derive that $\mu\left(r_x\right)=\mathcal{F}_{s_y}\left(\mu\left(r_x\right)\cup s_y,PL\left(r_x\right)\right)$ and $\mu\left(s_y\right)=\mathcal{F}_{r_x}\left(\mu\left(s_y\right)\cup r_x,PL\left(s_y\right)\right)$. Therefore the matching result of the proposed algorithm is pairwise stability. ■

Theorem 3 (Truthfulness)**.** *MastDP is truthful for buyers and sellers.*

Proof: We should prove that any participant can not achieve a better utility through misreporting the true valuation for one spectrum. We first focus on the buyers and distinguish the following four cases:

1) We consider the scenario where the buyer does not selected as a winning buyer when he bids truthfully and untruthfully. In this case, the same zero utility indicates that the buyer's untruthful bidding can not achieve higher utility.
2) We consider the scenario where the buyer was selected as a winning buyer only when he bids truthfully. It happens when r_j bids lower than his true value, $b_j^r<v_j^r$. In this case, the buyer r_j does not selected as a winning buyer after the clearing price determination since his bid is too low, and thereby his utility becomes 0. Each winning buyer's bid price b_j^r is higher than the clearing price P_c, leading to a non-negative utility. Consequently, the buyer's untruthful bidding can not achieve higher utility.
3) We consider the scenario where the buyer was selected as a winning buyer only when he bids untruthfully. It happens when r_j bids higher than his true value, $b_j^r>v_j^r$. In this case, winning buyer's true value v_j^r is lower than the clearing price P_c, resulting in negative utility. Consequently, the buyer's untruthful bidding can not achieve higher utility.
4) We consider the scenario where the buyer was selected as a winning buyer when he bids truthfully and untruthfully. In this case, the buyer is charged the same clearing price when he bids truthfully and untruthfully. Consequently, the buyer's untruthful bidding can not achieve higher utility.

Therefore, buyer r_x can not achieve higher utility by misreporting his true valuation. Similarly, we can obtain the same conclusion for sellers. In summary, MastDP is truthful for buyers and sellers. ■

Theorem 4 (ϵ-differential Privacy)**.** *The proposed MastDP algorithm satisfies ϵ-differential privacy.*

Proof: Let $\epsilon>0$ be the privacy parameter, and let e_1, e_2,..., e_{m+n} be random variables independently sampled from geometric distribution $Geom\left(\exp\left(\epsilon/\Delta f\right)\right)$. Let the randomized function $\mathbf{sum}$ such that $\mathbf{sum}\left(\tilde{b}\right) = \sum_{l=1}^{m+n}\left(b_l + e_l\right)$. We consider two neighboring bid values b' and b'' differing in only one bid, and use $\mathbf{Pr}\left(\mathbf{sum}\left(\tilde{b}'\right) = z\right)$ and $\mathbf{Pr}\left(\mathbf{sum}\left(\tilde{b}''\right) = z\right)$ to denote the probability density function at some arbitrary point $z \in \mathcal{S} \cap \mathcal{R}$. We have

$$\begin{aligned}
&\frac{\mathbf{Pr}\left(\mathbf{sum}\left(\tilde{b}'\right) = z\right)}{\mathbf{Pr}\left(\mathbf{sum}\left(\tilde{b}''\right) = z\right)} \\
&= \prod_{l=1}^{m+n}\left(\frac{\frac{\alpha-1}{\alpha+1}\cdot\alpha^{-\left|\mathbf{sum}\left(\tilde{b}'\right)_l - z_l\right|}}{\frac{\alpha-1}{\alpha+1}\cdot\alpha^{-\left|\mathbf{sum}\left(\tilde{b}''\right)_l - z_l\right|}}\right) \\
&\leq \prod_{l=1}^{m+n}\exp\left(\frac{\epsilon\left|\mathbf{sum}\left(\tilde{b}''\right)_l - \mathbf{sum}\left(\tilde{b}'\right)_l\right|}{\Delta f}\right) \\
&= \exp\left(\frac{\epsilon\left\|\mathbf{sum}\left(\tilde{b}''\right) - \mathbf{sum}\left(\tilde{b}'\right)\right\|_1}{\Delta f}\right) \\
&\leq \exp\left(\epsilon\right)
\end{aligned}$$

Therefore, MastDP algorithm satisfies ϵ-differential privacy. ■

Theorem 5 (Computational Complexity)**.** *The computational complexity of proposed MastDP algorithm is $O\left(KM^2N^2X\right)$, in which K and X are the secret key size and the computational complexity of greedy algorithm, respectively.*

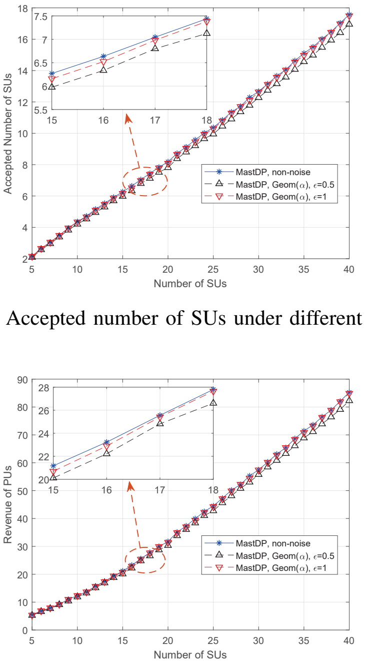
Proof: The complexity of the proposed MastDP algorithm for M PUs and N SUs consists of three parts: 1) the complexity of the M PUs and N SUs encrypting their bid values while the auctioneer decrypting these bid values using distributed differential privacy scheme, 2) the complexity of finding maximal independent sets for PUs with their preference, and 3) the complexity of matching between PUs and SUs. First, the complexity of distributed differential privacy scheme comes from the secret key size and the number of PUs and SUs, which is $O\left(KMN\right)$, in which K is the secret key size. Then as the complexity of greedy algorithm adopted for finding maximal independent set, we set it to $O\left(X\right)$. Finally, the complexity of matching is determined by the total number of PUs and SUs, which is $O\left(MN\right)$ [16], [17]. Therefore, the overall complexity of MastDP algorithm is $O\left(KM^2N^2X\right)$. ■

V. Simulation Results

We evaluate the performance of MastDP on spectrum trading efficiency and the performance on bid privacy preservation. Furthermore, we also compare it with two existing mechanisms: Grouping and Random. In Grouping algorithm, the auctioneer groups participants and sorts them based on the group's bid price, while Random refers to the randomly allocation algorithm that does not consider preference of participants.

A. Simulation Setup

We consider a double auction that a set of PUs offer spectrum to numbers of SUs, where the number of SUs varies from 5 to 40 with a step of 5, and the number of PUs is set to be 10. We randomly deploy PUs and SUs in a 1000x1000 m^2 area, and set the distance between SU's transmitter and receiver is $20m$, in addition the distance between any two SUs is not less than $50m$ to avoid overlapping, while the distances between PU and SU are randomly from 20m to 80m. We assume that each PU's request and each buyer's demand are uniformly distributed over $(0, 1]$, while the bids of them are randomly picked over $(1, 10]$. All the results are averaged over 2000 runs.



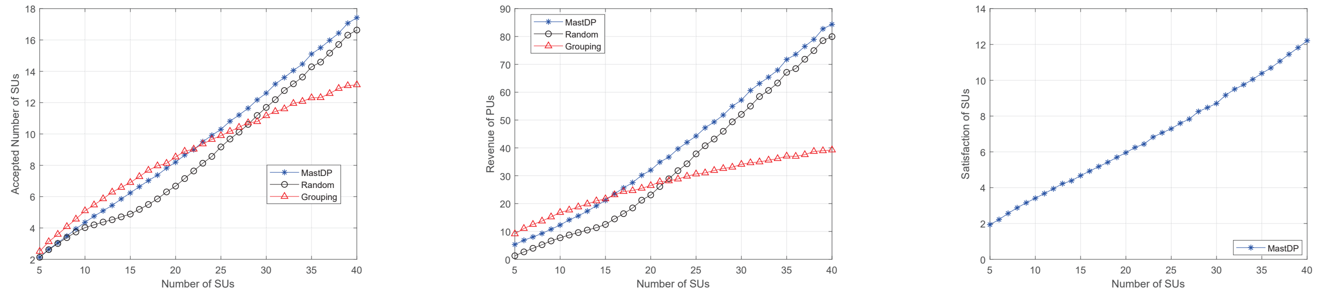
(a) Accepted number of SUs under different ϵ.

(b) Revenue of PUs under different ϵ.

Fig. 2. Performance on bid privacy preservation under different differential privacy levels, ϵ.

B. Performance on Spectrum Trading Efficiency

Figure 1(a) demonstrates the comparison results among MastDP, Grouping and Random on accepted number of SUs. From the figure we can see that as the number of SUs increases, the accepted number of SUs in MastDP is more than that of Grouping and Random, and in the linearity increasing trend. Since the revenue depends on both the clear price and the number of accepted SUs, as shown in Figure 1(b), MastDP with more accepted participants gains higher revenue. Afterward, we evaluate the performance of the matching algorithm in MastDP by a metric of SUs' satisfaction, which is the number of SUs whose first preference are satisfied. Figure 1(c) illustrates that the satisfaction of SUs almost linearly increases with the increase of SUs. Since the Grouping and Random do not consider participant satisfaction, we can draw a conclude that MastDP can not only obtain better performance, but also improve SUs' incentive to participate in the spectrum double auction.



(a) Accepted number of SUs.

(b) Revenue of PUs.

(c) Satisfaction of SUs.

Fig. 1. Performance on spectrum trading efficiency comparison of MastDP, Grouping and Random.

C. Performance on Bid Privacy Preservation

Figure 2(a) and Figure 2(b) illustrate the accepted number of SUs and revenue of PUs under different differential privacy levels, respectively. We can notice that the performance of that accepted number of SUs and revenue of PUs after adding noise are slightly worse than the performance without considering privacy preservation. In addition, he performance when ϵ is 1 is closer. The reason is that ϵ indicates privacy level in difference privacy. When ϵ is small, it means a higher level of difference privacy, which causes participants to add more noise to their submitted data.

VI. Conclusions

In this paper, we have proposed MastDP, a differential privacy and matching algorithm combined double auction mechanism for spectrum trading that can achieves both spectrum trading efficiency and differential privacy preservation for individual's sensitive information. Focusing on protecting participants' bid information from the frauds of the auctioneer, other buyers/sellers and other potential parties, we present a distributed differential privacy mechanism by adding $Geom(\alpha)$ noise to individual's bid value, leading to the sum of all noisy bid values obtained by the auctioneer satisfies the ϵ-differential privacy protection, as well as utilize the cryptography technology to enable the uploaded bid values from all participants to be decrypted merely by the auctioneer. Then we design a matching based approach to allocate winning buyers to spectrum sellers with considering participants' preferences while maintaining spectrum reuse to maximize the revenue of spectrum sellers. The simulation results confirm that MastDP is able to realize economic properties privacy and spectrum trading efficiency.

Acknowledgment

This work was supported in part by the National Key Research and Development Program of China, under Grant 2017YFB0802303, in part by the National Natural Science Foundation of China, under Grant 61672283, in part by the U.S. National Science Foundation, under Grant US CNS-1350230 (CAREER), CNS-1646607, CNS-1702850, and CNS-1801925.

References

[1] E. Hossain and M. Hasan, "5G cellular: key enabling technologies and research challenges," *IEEE Instrumentation Measurement Magazine*, vol. 18, no. 3, pp. 11–21, Jun. 2015.

[2] X. Wang, Y. Ji, H. Zhou, Z. Liu, Y. Gu, and J. Li, "A privacy preserving truthful spectrum auction scheme using homomorphic encryption," in *Proceedings IEEE GLOBECOM*, Dec. 2015, pp. 1–6.

[3] M. Li, P. Li, L. Guo, and X. Huang, "PPER: Privacy-preserving economic-robust spectrum auction in wireless networks," in *Proceedings IEEE INFOCOM*, Apr. 2015, pp. 909–917.

[4] 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*, vol. 29, no. 4, pp. 866–876, Apr. 2011.

[5] M. Al-Ayyoub and H. Gupta, "Truthful spectrum auctions with approximate revenue," in *Proceedings IEEE INFOCOM*, Apr. 2011, pp. 2813–2821.

[6] R. Zhu and K. G. Shin, "Differentially private and strategy-proof spectrum auction with approximate revenue maximization," in *Proceedings IEEE INFOCOM*, Apr. 2015, pp. 918–926.

[7] C. Wu, Z. Wei, F. Wu, and G. Chen, "Diary: A differentially private and approximately revenue maximizing auction mechanism for secondary spectrum markets," in *Proceedings IEEE GLOBECOM*, Dec. 2014, pp. 625–630.

[8] X. Zhou and H. Zheng, "Trust: A general framework for truthful double spectrum auctions," in *Proceedings IEEE INFOCOM*, Apr. 2009, pp. 999–1007.

[9] Z. Zheng, Y. Gui, F. Wu, and G. Chen, "Star: Strategy-proof double auctions for multi-cloud, multi-tenant bandwidth reservation," *IEEE Transactions on Computers*, vol. 64, no. 7, pp. 2071–2083, Jul. 2015.

[10] R. Zhu, Z. Li, F. Wu, K. Shin, and G. Chen, "Differentially private spectrum auction with approximate revenue maximization," in *Proceedings of MobiHoc*, 2014, pp. 185–194.

[11] A. Ghosh and A. Roth, "Selling Privacy at Auction," *arXiv e-prints*, Nov. 2010.

[12] H. Zhai, S. Chen, and D. An, "Expo: Exponential-based privacy preserving online auction for electric vehicles demand response in microgrid," in *Proceedings of International Conference on Semantics, Knowledge and Grids (SKG)*, Aug. 2017, pp. 126–131.

[13] J. Wang, W. Ding, Y. Guo, C. Zhang, M. Pan, and J. Song, "M^3-step: Matching-based multi-radio multi-channel spectrum trading with evolving preferences," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 11, pp. 3014–3024, Nov 2016.

[14] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proceedings IEEE FOCS*, Oct 2007, pp. 94–103.

[15] E. Shi, H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proceedings NDSS*, Feb. 2011.

[16] D. Gale and L. S. Shapley, "College admissions and the stability of marriage," *The American Mathematical Monthly*, vol. 69, no. 1, pp. 9–15, 1962.

[17] D. F. Manlove *et al.*, "Algorithmics of matching under preferences," *Bulletin of EATCS*, vol. 1, no. 112, 2014.