PPER: Privacy-Preserving Economic-Robust Spectrum Auction in Wireless Networks

Ming Li*, Pan Li†, Linke Guo‡ and Xiaoxia Huang§
*Department of Computer Science and Engineering, University of Nevada, Reno, NV 89557
†Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS 39762
‡Department of Electrical and Computer Engineering, Binghamton University, State University of New York, NY 13902
§Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China
Email: mingli@unr.edu, li@ece.msstate.edu, lguo@binghamton.edu, xx.huang@siat.ac.cn

***Abstract*—Many truthful spectrum auction schemes have been recently proposed to to ensure that the dominant strategy for bidders is to bid truthfully and thus protect the auctioneer's benefits. However, most of them assume the auctioneer is trustful and do not protect users' interests. An auctioneer can manipulate the winner's charging price if it knows users' bids. Thus, it is critical to protect bids from the auctioneer in an auction. With this goal, we develop a Privacy-Preserving Economic-Robust spectrum auction scheme, namely PPER. Not only does it well protect users' bid privacy, but also guarantees economic-robustness which is another important auction property. Besides, only transmitters but not receivers are considered in most previous spectrum auctions, resulting in many unexpected collisions during transmissions. In this work, we consider interference constraints from transmissions instead of transmitters in spectrum allocation. Extensive privacy analysis and simulation results show the effectiveness and efficiency of our scheme.**

I. Introduction

The recent exploding growth and popularity of wireless devices and services have exacerbated the spectrum scarcity in wireless networks. Recent studies show that the spectrum scarcity is largely attributed to inefficient spectrum utilization due to the current static spectrum policies, by which spectrums are exclusively used by their licensed holders, and cannot be accessed by other users even if they are not in use. To enhance spectrum utilization, dynamic real-time secondary spectrum auction markets are proposed lately [1], [2], where secondary users (SUs) can compete with each other for the idle spectrums from primary spectrum providers (PSPs), while PSPs receive financial rewards by leasing their idle spectrums.

Many truthful spectrum auction schemes have been proposed to facilitate spectrum allocation in wireless networks [1]–[9]. Although these schemes ensure that the dominant strategy for each bidder is to bid truthfully, and thus protect the auctioneer's revenue, the bidders' benefits are not guaranteed. For example, a misbehaving auctioneer in VCG auction can employ shill bidders to manipulate the charging price to the winners so as to increase its revenue, if it knows bids [10]. In order to prevent the auctioneer from impairing bidders' benefits by taking advantage of their bid information, it is necessary to protect bid privacy from the auctioneer in spectrum auctions. Besides, in addition to truthfulness (also called incentive compatibility (IC) or strategy-proof), individual rationality (IR) and budget balance (BB) are two other important properties of economic-robustness. An auction is proved to be vulnerable to market manipulation and produces poor outcomes if it is not economic-robust [11]. However, it is non-trivial to achieve bid privacy and economic-robustness in spectrum auction simultaneously, as bid information is fundamental in spectrum allocation and pricing, which determine whether an auction is economic-robust. Only a couple of works have attempted to address privacy issues in spectrum auctions. Pan *et al.* [10] propose a privacy-preserving spectrum auction scheme THEMIS by employing Paillier encryption. However, THEMIS fails to protect winners' bids at the end of an auction. A scheme SPRING [12] is developed based on k-anonymity technique, which allows the auctioneer to correctly guess a bid with a probability of $1/k$. Huang *et al*. [13] propose a privacy-preserving truthful spectrum auction scheme to achieve good social welfare based on homomorphic encryption. Notice that all these works [10], [12], [13] assume a trusted third-party to assist in auctions.

We also notice that there have been some works studying privacy-preserving auctions such as [14]–[16]. However, these schemes still reveal the full or part of bids at the end of an auction for pricing purpose. Due to dynamics of secondary spectrum markets, spectrum allocation is not fixed by an one-time auction. The auctioneer can still utilize the bids revealed in previous auctions to manipulate outcomes of the subsequential auctions. Therefore, to protect bid privacy is more challenging compared that in traditional auctions. Besides, the spectrum reusability in wireless networks further differentiates spectrum auctions from traditional auctions. Although the existing works [1]–[8] have extensively discussed this issue in spectrum auctions, besides their lack of bid privacy protection, they do not take receivers into consideration in spectrum allocation. Consequently, many winning SUs may not be able to successfully deliver their traffics due to unexpected interferences at receivers caused by other winning SUs.

In this paper, we consider an auction market where a PSP, who acts as an auctioneer, leases its unused licensed spectrums to a group of SUs. If two SUs, including a secondary transmitter (ST) and its corresponding secondary receiver (SR), have data to transmit between them, they form a secondary transmission pairs and compete in the market. To address the concerns raised above, we then develop a Privacy-Preserving Economic-Robust scheme (PPER) for spectrum auction in wireless networks.

We first propose a basic spectrum auction framework, which consists of two procedures: spectrum allocation and pricing. In the spectrum allocation procedure, the auctioneer finds out the top L bidder groups (BGs) with the highest group bids if it has L spectrums available. Each BG is a set of STs who can simultaneously transmit to their SRs on the same spectrum without interfering each other. For this purpose, the auctioneer formulates and computes L binary integer programming (BIP) optimization problem, taking the interference among transmission pairs (instead of among STs) into consideration. In the pricing procedure, the auctioneer determines the clearing price for each winning ST. The spectrum allocation and pricing are designed to ensure the economic-robustness of the spectrum auction framework.

Noticing that the auctioneer can easily know STs' bids in spectrum allocation procedure, we then develop a privacy-preserving BIP algorithm which protects STs' bid privacy and still allows the auctioneer to optimally solve the BIP problems. There are some existing works discussing privacy protection in solving linear programming (LP) problems. Some of them [17]–[19] transform an LP problem by multiplying both constraints and the objective function with random matrixes or random vectors. In these works, the objective function or the constraint belongs to one party, while in our BIP problem the coefficients of the objective function, i.e., bids, belong to different STs, making our case much more complicated. Another line of research applies partition approaches [20]–[22]. Such schemes only protect the constraint privacy without considering the privacy in objective functions. In this study, we propose to optimally solve the BIP problem under the Branch and Bound (B&B) [23] framework, by which the original problem can be divided into multiple LP subproblems. Then, following the idea of [18] we develop a revised simplex method based privacy-preserving LP algorithm to solve those subproblems. Different from [18], in which only two parties are involved, our algorithm allows multiple parties, including the auctioneer and all STs, to jointly solve the LP problem with their private information well protected. More importantly, the proposed privacy-preserving LP algorithm is not limited in addressing privacy-preserving spectrum auctions but other more general problems.

II. Problem Formulation

A. System Model

We consider an auction market shown in Fig. 1, where a PSP, who acts as an auctioneer, leases a set of unused licensed spectrums $\mathcal{L} = \{1, 2, ..., l, ..., L\}$ to a group of SUs $\overline{\mathcal{N}}$. If two SUs, including an ST and its 1-hop SR, have data to transmit between them, they form a secondary transmission pairs. We assume that there are more transmission pairs than the available spectrums in the system. Thus, to deliver their traffics, all the STs $\mathcal{N} = \{1, 2, ...n, ..., N\} \subseteq \overline{\mathcal{N}}$ are supposed to submit their bids and compete for spectrums. The winning STs pay for the obtained spectrums, on which they can transmit data to their SRs. In a spectrum auction, a spectrum can be leased to several transmission pairs if they can transmit simultaneously without interfering with each other. An ST can also obtain multiple spectrums to transmit to its SR like that in [7], [9], [10].

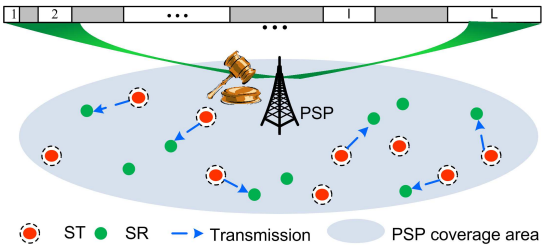


Fig. 1. The architecture of the spectrum auction market.

In order to participate in spectrum auctions, all STs and SRs submit their location to the PSP[1], who can determine the topology of the entire network. Given the network topology, the PSP constructs a conflict graph denoted by $G(V, E)$, where V is the vertex set and E is the edge set. In particular, each vertex corresponds to a secondary transmission pair denoted by (i, r_i), where i and r_i denote an ST and its receiver, respectively. Two vertices in V are connected with an undirected edge if the corresponding transmission pairs interfere with each other on the same spectrum, i.e., if the SR in one transmission pair is within the interference range of the ST in the other transmission pair given that they are using the same band, or these two transmission pairs have at least one node in common (i.e., $r_i = r_j$, or $r_i = j$, or $i = r_j$ for $i \neq j$). In this conflict graph, an independent set (IS) is a set in which each element is a transmission pair, and all the elements (or transmissions) can be carried out successfully at the same time. If adding any more transmission pairs into an IS results in a non-independent one, this IS is defined as a maximal independent set (MIS).

We denote ST i's real valuation and bid price for a spectrum by v_i and c_i, respectively. In an auction, STs submit their bids c_i's in a sealed manner, so that no one has access to any information about others' bids. After the auctioneer receives all the bids, it divides the bidders into different bidder groups (BGs), each of which is a set of STs of all the transmission pairs in one MIS. We denote the set of all the BGs by $\mathcal{G}$. The auctioneer considers each BG as a virtual bidder with its group bid being the sum of all STs' bids in that group, and determines the winning BGs denoted by $\mathcal{G}_W$. We denote each winning BG in $\mathcal{G}_W$ by $\mathcal{G}_{W,t}$ $(1 \leq t \leq |\mathcal{G}_W|)$, and the set of indexes (j's) of the winning BGs containing ST i by H_i, respectively. We also denote the clearing price for ST i in a winning BG containing i, say $\mathcal{G}_{W,t}$ $(t \in H_i)$, by p_i^t.

B. Objective of Auction Design

The design of auction schemes heavily depends on the desired properties. In this work, we aim to design an auction scheme guaranteeing bid privacy and economic-robustness.

We assume that all STs are strategic in the sense that they may manipulate their bids to obtain favorable outcomes. In

[1]The location information and other control messages can be transmitted over a dedicated channel called cognitive pilot channel (CPC) or common control channel as in IEEE 802.22 [24], [25].

order to achieve economic-robustness, we propose to achieve three of the most important economic requirements: Incentive Compatibility (IC), Individual Rationality (IR), and Budget Balance (BB), which are defined as follows:

- **Incentive Compatibility (IC)**: The utility function of ST i ($i \in \mathcal{N}$), is a function of all the bids:

$$u_i(c_i, \mathbf{c_{-i}}) = \begin{cases} \sum_{j \in H_i}(v_i - p_i^t), \text{ if } i \text{ wins} \\ \text{with bid } c_i, \\ 0, \text{ otherwise.} \end{cases} \quad (1)$$

  where $\mathbf{c_{-i}}$ denotes the vector of bids from other STs. Thus, an auction is IC if for any ST i ($i \in \mathcal{N}$) with any $c_i \neq v_i$ while others' bids are fixed, we have

$$u_i(c_i, \mathbf{c_{-i}}) \leq u_i(v_i, \mathbf{c_{-i}}). \quad (2)$$

- **Individual Rationality (IR)**: An auction is IR, if bidder i ($i \in \mathcal{N}$) gets non-negative utility in the auction, i.e., $u_i(c_i, \mathbf{c_{-i}}) \geq 0$.
- **Budget Balanced (BB)**: To make the auction self-sustained without any external subsidies, the generated revenue of the auctioneer, i.e., the PSP, is required to be non-negative.

As we mentioned earlier, to prevent the auctioneer from impairing bidders' benefits by taking advantage of their bids, one effective approach is to hide these information from the auctioneer. Besides, due to dynamics of secondary spectrum markets, spectrum allocation is not fixed by an one-time auction. The auctioneer can utilize the bids revealed in previous auctions for the purpose of pricing to infer future bids and manipulate the subsequential auction outcomes. Therefore, bid information should be protected in the entire auction, including item allocation and pricing procedures.

C. Interference Model

In this work, we employ the protocol model [26], [27] to characterize interference relationships among transmissions. Specifically, the data transmission between an ST and an SR is successful only if the received power spectral density at the SR exceeds a threshold P_T. Meanwhile, we assume interference becomes non-negligible only if it produces a power spectral density over a threshold of P_I ($P_I \leq P_T$) at the SR. We denote SU i's transmission and interference range by R_T^i and R_I^i, respectively. R_T^i and R_I^i can be derived from P_T and P_I.

D. Revised Simplex Method

In this paper, we apply the revised simplex method [28] to develop a privacy-preserving LP algorithm for two purposes. First, as a variant of George Dantzig's simplex method [29], the revised simplex method is a computationally efficient approach to solve LP problems. The second and more important reason is that the unique structure of the revised simplex method can be explored to securely solve LP problems.

The revised simplex method is conducted over the following augmented form of an LP problem

$$\begin{aligned} \textbf{Maximize:} \quad & \mathbf{c}^\top \mathbf{x} \\ \textbf{s.t.} \quad & \mathbf{A}\mathbf{x} = \mathbf{b}, \quad \mathbf{x} \geq \mathbf{0} \end{aligned}$$

where $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{c} \in \mathbb{R}^{n \times 1}$, $\mathbf{b} \in \mathbb{R}^{m \times 1}$, and $\mathbf{x} \in \mathbb{R}^{n \times 1}$. It is assumed that the constraint matrix $\mathbf{A}$ has full row rank and the problem is feasible, i.e., there is at least one $\mathbf{x} \geq \mathbf{0}$ such that $\mathbf{A}\mathbf{x} = \mathbf{b}$. If an LP problem has redundant constraints, it can be transformed to the above augmented form through preprocessing.

Following some well-known results in the theory of linear programming [30], the above LP problem can be rewritten as

$$\begin{aligned} \textbf{Maximize:} \quad & \mathbf{c}_B^\top \mathbf{x}_B + \mathbf{c}_N^\top \mathbf{x}_N \\ \textbf{s.t.} \quad & \mathbf{B}\mathbf{x}_B + \mathbf{N}\mathbf{x}_N = \mathbf{b}, \quad \mathbf{x} \geq \mathbf{0} \end{aligned} \quad (3)$$

where $\mathbf{B} \in \mathbb{R}^{m \times m}$ is a submatrix of $\mathbf{A}$, formed by $\mathbf{A}$'s m arbitrary linearly independent columns, and $\mathbf{N} \in \mathbb{R}^{m \times (n-m)}$ is formed by $\mathbf{A}$'s remaining columns. $\mathbf{x}_B$ and $\mathbf{x}_N$ are called basic variables and non-basic variables, respectively. $\mathbf{c}_B$ and $\mathbf{c}_N$ are their corresponding coefficients. A basic solution to an LP problem corresponds to assigning null values to non-basic variables. Besides, the optimal solution of an LP problem comes from one of its basic solutions. Thus, the general idea of the revised simplex method is to search among an LP problem's basic solutions, by replacing one of current basic variables with one non-basic variable with the most negative reduced cost in each iteration, until the reduced costs of all non-basic variables are non-negative.

Formally, the iteration of the revised simplex method can be specified as follows:

1) The basic solution to (3) is given by $\mathbf{x}_B = \mathbf{B}^{-1}\mathbf{b}$ and $\mathbf{x}_N = \mathbf{0}$.
2) For each non-basic variable, calculate

$$z_j - c_j = \mathbf{c}_B^\top \mathbf{B}^{-1}\mathbf{N}_j - c_j, \quad (4)$$

   where $\mathbf{N}_j$ is the j-th column of $\mathbf{N}$. Let $k = \underset{j}{\operatorname{argmin}}\{z_j - c_j\}$. If $z_k - c_k \geq 0$, then stop; the current solution is optimal, with the optimal result of $\mathbf{c}_B^\top \mathbf{x}_B$. Otherwise, continue to step 3).
3) Calculate $\boldsymbol{\eta}_k = \mathbf{B}^{-1}\mathbf{N}_k$ and $\boldsymbol{\xi} = \mathbf{B}^{-1}\mathbf{b}$, and determine the index of the variable $x_l \in \mathbf{x}_B$ leaving the basic variables as follows:

$$l = \underset{i}{\operatorname{argmin}}\left(\frac{\xi_i}{\eta_{ik}} : \eta_{ik} > 0\right). \quad (5)$$

   Update $\mathbf{B}$ by replacing $\mathbf{B}_l$ with $\boldsymbol{\eta}_k$, $\mathbf{N}$ by replacing $\mathbf{N}_k$ with $\mathbf{B}_l$, and go to step 1).

Notice that if we obtain $\eta_{ik} \leq 0$ in any iteration step, the optimal solution of the above LP problem is unbounded; otherwise $\mathbf{B}^{-1}$ always exists [30].

III. A Basic Economic-Robust Spectrum Auction Framework

In this section, we describe a basic economic-robust spectrum auction framework which does not discuss users' privacy protection. In general, the auction framework consists of two procedures: spectrum allocation and pricing. In what follows, we detail the design of these two procedures, respectively.

A. Spectrum Allocation

Recall that a BG is a set of STs of all the transmission pairs in one MIS. In our auction framework, we assume that each BG only obtains one spectrum from the auction. In order to maximize auction efficiency, i.e., the sum of valuations from all winning bidders [31], the auctioneer needs to find out L winning BGs with the highest group bids in IC spectrum auctions. In particular, these top-L BGs are determined in a monotonic manner, i.e., the BG with the highest group bid is found in the first iteration and excluded from the auction, then the BG with the second highest group bid in the second iteration, and so on and so forth until the top L BGs are found.

We denote by x_i a variable, which is equal to 1 if ST i can transmit to r_i and equal to 0 otherwise. We first consider a constraint due to potential interference among transmission pairs. If ST i is transmitting data to r_i, any other STs that will interfere with r_i's reception should not transmit. To model this constraint, we denote by $\mathcal{O}(r_i)$ the set of STs that can interfere with r_i's reception, i.e., $\mathcal{O}(r_i) = \{o | d(o, r_i) \leq R_I^o, o \in \mathcal{N}\}$, where R_I^o is the interference range of ST o. Therefore, we have

$$x_i + x_p \leq 1, \qquad \forall p \in \mathcal{O}(r_i). \tag{6}$$

Note that if another transmission pair (j, r_j) has at least one node in common with (i, r_i), i.e., if $r_j = r_i$, or $j = r_i$, or $i = r_j$, these two transmission pairs cannot transmit simultaneously either. Define $d(i, i) = 0$ for $i \in \overline{\mathcal{N}}$. Since we have $d(j, r_i) \leq R_T^j \leq R_I^j$ and $d(i, r_j) \leq R_T^i \leq R_I^i$, these scenarios are included in (6) for ST i and ST j.

Moreover, recall that we need to find out the t-th highest group bid in the t-th iteration. In other words, the BG found in the t-th ($2 \leq t \leq L$) iteration should be different from the previously found $t-1$ BGs. Denoting by $\mathcal{G}_{W,t}$ the winning BG found in the t-th iteration, we have

$$\sum_{i \notin \mathcal{G}_{W,\tau}} x_i \geq 1, \quad \forall 1 \leq \tau \leq t-1. \tag{7}$$

This constraint means that the newly found BG should contain at least one different ST from any of the previously found $t-1$ BGs.

Consequently, the spectrum allocation of finding the BG with the t-th ($1 \leq t \leq L$) highest group bid in the t-th iteration can be formulated as

$$\begin{aligned} \textbf{Maximize:} \quad & C_t = \sum_{i \in \mathcal{N}} c_i \cdot x_i \\ \textbf{s.t.} \quad & (6) \text{ when } t = 1 \\ & (6) - (7) \text{ when } 2 \leq t \leq L+1 \\ & x_i \in \{0, 1\} \end{aligned}$$

where x_i's are the optimization variables. The formulated spectrum allocation problem is a BIP problem, which we call the t-th original optimization problem (t-OOP). Assume that there are M constraints in (6). According to the description above, there are $t-1$ constraints in (7) for the t-th iteration.

B. Pricing

In the pricing procedure, we follow the similar idea of VCG auction pricing [31]. Recall that H_i represent the set of indices of winning BGs containing ST i. The clearing price for i is

$$p_i = \sum_{t \in H_i} p_i^t = \sum_{t \in H_i} \big(C_{t,-\mathbf{i}} - (C_t - c_i)\big). \tag{8}$$

where $C_{t,-\mathbf{i}}$ stands for the t-th highest group bid when ST i is excluded from the t-th iteration and $C_t - c_i$ is the sum of bids from the t-th highest group bid except c_i. Clearly, the clearing price for winning ST i is irrelevant to its bid. Based on the proposed spectrum allocation and pricing procedure, we are able to prove this spectrum auction framework is economic-robust. We leave its discussion and proof in Section V.

IV. Privacy-Preserving Economic-Robust Spectrum Auction

In this section, we propose a privacy-preserving spectrum auction scheme based on the economic-robust spectrum auction framework described in Section III. Our objective is to protect STs' bid privacy, i.e., c_i's ($i \in \mathcal{N}$), from other entities, while allowing the auctioneer to determine spectrum allocation and pricing correctly. Thus, the problem becomes how the auctioneer can optimally solve t-OOP without knowing c_i's.

As t-OOP is a BIP problem, we utilize the branch and bound (B&B) algorithm [23] to decompose it into multiple relaxed LP problems. Thus, we first propose a privacy-preserving LP algorithm for such LP problems. Then, the privacy-preserving BIP algorithm to solve t-OOP will be ready to be developed.

A. Privacy-Preserving LP Algorithm

We first rewrite t-OOP in a more general form[2]

$$\begin{aligned} \textbf{Maximize:} \quad & C_t = \mathbf{c}^\top \mathbf{x} \\ \textbf{s.t.} \quad & \boldsymbol{\alpha}\mathbf{x} \leq \boldsymbol{\beta} \\ & x_i \in \{0, 1\} \end{aligned}$$

where $\boldsymbol{\alpha}$ is the constraint matrix of size $(M+t-1) \times |\mathcal{N}|$. Then we apply the B&B algorithm to decompose this BIP problem. In each branching step, an arbitrary variable is picked from the unexplored variables to branch on, i.e., setting its value to either 0 or 1. By further taking linear relaxation on binary constraints, we obtain the following two LP problems

$$K_0(K_1) \quad \textbf{Maximize:} \quad C_t' = \sum_{i \in \mathcal{N}_u} c_i x_i + \sum_{i \in \mathcal{N}_e} c_i \overline{x_i} + c_k x_k \tag{9}$$

$$\begin{aligned} \textbf{s.t.} \quad & \sum_{i \in \mathcal{N}_u} \alpha_{mi} x_i \leq \beta_m - \sum_{i \in \mathcal{N}_e} \alpha_{mi} \overline{x_i} - \alpha_{mk} x_k \\ & (\forall 1 \leq m \leq M + t - 1) \\ & 0 \leq x_i \leq 1 \quad (\forall i \in \mathcal{N}_u) \\ & x_k = 0 \quad (\text{or } x_k = 1) \end{aligned}$$

where x_k is the branching variable, $\mathcal{N}_e$ is the explored variable set with fixed values $\overline{x_i}$'s, and $\mathcal{N}_u = \mathcal{N}/(\mathcal{N}_e \cup \{x_k\})$ is the

[2]The problem when $t = 1$ can be transformed similarly. We focus on the general case where $2 \leq t \leq L$ in the following analysis.

unexplored variable set. Without loss of generality, we now discuss how the auctioneer obtains the optimum solution of the above LP problem, $K_0(K_1)$, without the knowledge of c_i's.

The proposed privacy-preserving LP algorithm is developed based on the revised simplex method which enables the LP problem to be solved in a distributed way. Both STs and the auctioneer compute locally and exchange their intermediate results, based on which a new round of computation is conducted, until the optimal solution is found by the auctioneer. During the computation, c_i is kept at ST i locally. Since the revised simplex method can only be applied to an LP problem with equality constraints, we first transform (9) into its augmented form by introducing non-negative slack variables $\mathbf{s}$ to replace inequalities with equalities in its constraints

$$\begin{aligned} \textbf{Maximize:} \quad & C'_t = \mathbf{c'}^{\top}\mathbf{x'} + \mathbf{0}^{\top}\mathbf{s} + Q_0 \\ \textbf{s.t.} \quad & \mathbf{A}\mathbf{x'} + \mathbf{I}\mathbf{s} = \mathbf{b} \\ & \mathbf{x'}, \mathbf{s} \geq \mathbf{0}, \end{aligned} \tag{10}$$

where $\mathbf{c'} = \{c_i | i \in \mathcal{N}_u\}$, $\mathbf{x'} = \{x_i | i \in \mathcal{N}_u\}$, and Q_0 denotes the fixed value of $\sum_{i \in \mathcal{N}_e} c_i \overline{x_i} + c_k x_k$. $\mathbf{I}$ is an identity matrix of size $M + t - 1 + |\mathcal{N}_u|$.

Algorithm 1 gives details of our privacy-preserving LP algorithm in solving (10) based on the revised simplex method introduced in Section II-D. Initially, we set $\mathbf{B} = \mathbf{I}$, $\mathbf{N} = \mathbf{A}$, $\mathbf{c}_B = \mathbf{0}$, $\mathbf{c}_N = \mathbf{c'}$, $\mathbf{x}_B = \mathbf{s}$, $\mathbf{x}_N = \mathbf{x'}$, and $\mathcal{I} = \emptyset$, among which $\mathbf{B}$, $\mathbf{N}$, $\mathbf{x}_B$, and $\mathbf{x}_N$ are known to all entities, while $c_i \in \mathbf{c'}$ is kept by ST i itself. The "for" loop from line 1 to line 15 captures the spirit of the privacy-preserving aspect. For each non-basic variable, if $i \in \mathcal{N}$, after obtaining the encrypted z_i, the auctioneer engages with ST i in comparing z_i and c_i via secure comparison without the knowledge of either z_i or c_i. ST i is unaware of z_i either. Following similar steps, if $i \notin \mathcal{N}$, i.e., x_i is a slack variable, ST j[3] ($x_j \in \mathbf{x}_B$) engages the auctioneer in comparing z_i and 0. Both ST j and the auctioneer are unaware of z_i. For these two cases, if the reduced cost is negative, the auctioneer will add i to $\mathcal{I}$. Thereafter, the auctioneer randomly picks a leaving non-basic variable with index k from $\mathcal{I}$ following line 17. Line 18 and 19 determine the leaving basic variable. Then, $\mathbf{B}$, $\mathbf{N}$, $\mathbf{x}_B$, and $\mathbf{x}_N$ are updated accordingly. The iteration continues until all non-basic variables generate non-negative reduced cost, i.e., the optimal solution is found.

Remark 1 When determining the leaving non-basic variable in line 17, different from the typical way of choosing one with the most negative reduced cost as introduced in Section II-D, the auctioneer randomly picks a leaving non-basic variable. This is because the ordering of the non-basic variables' reduced costs will enable the auctioneer to infer a nonuniform probability distribution upon the space of possible cost functions [18] and thus c_i's. However, the auctioneer can still optimally solve the LP problem under this modified revised simple method, because it suffices to choose any non-basic variable that improves the solution at each iteration [32].

[3]This ST can be determined as the one with the lowest ID number within current basic variables.

Algorithm 1 Privacy-Preserving LP Algorithm

Input: $\mathbf{B} = \mathbf{I}$, $\mathbf{N} = \mathbf{A}$, $\mathbf{c}_B = \mathbf{0}$, $\mathbf{c}_N = \mathbf{c'}$, $\mathbf{x}_B = \mathbf{s}$, $\mathbf{x}_N = \mathbf{x'}$, and $\mathcal{I} = \emptyset$

Output: $\mathbf{x}^*_N$, $\mathbf{x}^*_B$, and C'^*_t

1: **for** $x_i \in \mathbf{x}_N$ **do**
2: **if** $i \in \mathcal{N}$ **then**
3: Auctioneer obtains $\text{Enc}_i(z_i) = \text{Enc}_i(\mathbf{c}_B^{\top} \cdot \mathbf{B}^{-1}\mathbf{N}_i)$;
4: Auctioneer and ST i compare z_i and c_i via secure comparison;
5: **if** $z_i < c_i$ **then**
6: $\mathcal{I} = \mathcal{I} \cup i$;
7: **end if**
8: **else**
9: ST j ($x_j \in \mathbf{x}_B$) obtains $\text{Enc}_A(z_i) = \text{Enc}_A(\mathbf{c}_B^{\top} \cdot \mathbf{B}^{-1}\mathbf{N}_i)$;
10: ST j and the auctioneer compare z_i and 0 via secure comparison;
11: **if** $z_i < 0$ **then**
12: $\mathcal{I} = \mathcal{I} \cup i$;
13: **end if**
14: **end if**
15: **end for**
16: **if** $\mathcal{I} \neq \emptyset$ **then**
17: Auctioneer randomly picks $k \in \mathcal{I}$ and sets $\mathcal{I} = \emptyset$;
18: Calculates $\boldsymbol{\eta}_k = \mathbf{B}^{-1}\mathbf{N}_i$ and $\boldsymbol{\xi} = \mathbf{B}^{-1}\mathbf{b}$, or stops if the optimal solution is unbounded;
19: Determines the index l of the variable leaving the basic variable set following (5);
20: Updates $\mathbf{B}$ by replacing $\mathbf{B}_l$ with $\boldsymbol{\eta}_k$, $\mathbf{N}$ by replacing $\mathbf{N}_k$ with $\mathbf{B}_l$, as well as $\mathbf{x}_B$, and $\mathbf{x}_N$;
21: Broadcasts the updated values;
22: **Go to** line 1;
23: **else**
24: Auctioneer broadcasts $\mathbf{x}^*_N = \mathbf{x}_N$, $\mathbf{x}^*_B = \mathbf{x}_B$;
25: Computes $C'^*_t = \mathbf{c}_B^{\top}\mathbf{x}^*_B + Q_0$;
26: **end if**

Remark 2 One question left in Algorithm 1 is how the auctioneer obtains $\text{Enc}_i(z_i) = \text{Enc}_i(\mathbf{c}_B^{\top} \cdot \mathbf{B}^{-1}\mathbf{N}_i)$ without the information of c_i's. Here, $\text{Enc}_i(\cdot)$ stands for the encryption with ST i's Paillier public encryption key. We first express z_i as $\sum_{j=1}^{M+t-1+|\mathcal{N}_u|} c_j d_{ij}$, where d_{ij} represents the j-th element of vector $\mathbf{B}^{-1}\mathbf{N}_i$. The elements of $\mathbf{c}_B$ can be divided into two types, bids c_i's from STs and 0's of slack variables' coefficients. Thus, we have $z_i = \sum_{\{j | x_j \in \mathbf{x'} \cap \mathbf{x}_B\}} c_j d_{ij}$. Then we apply in our algorithm a privacy-preserving data aggregation scheme [33] developed based on Paillier cryptosystem to securely calculate z_i. First, each ST j ($x_j \in \mathbf{x'} \cap \mathbf{x}_B$) generates a random value r_{jp} and sends it to the rest STs p's ($x_p \in \mathbf{x'} \cap \mathbf{x}_B$). At the end of this step, each ST j receives $|\mathbf{x'} \cap \mathbf{x}_B| - 1$ random values from its peers. Next, each ST j computes R_j based on all collected random values

$$R_j = n + \sum_{\substack{\{p | x_p \in \mathbf{x'} \cap \mathbf{x}_B\} \\ p \neq j}} r_{jp} - \sum_{\substack{\{p | x_p \in \mathbf{x'} \cap \mathbf{x}_B\} \\ p \neq j}} r_{pj} \tag{11}$$

where n is the public modulus of the Paillier cryptosystem. Then, ST j encrypts $c_j d_{ij}$ by $g_i^{c_j d_{ij}} \cdot h^{R_j}$, and sends it to the auctioneer, where $g_i \in \mathbb{Z}_{n^2}^*$ is ST i's Paillier public encryption key, and $h \in \mathbb{Z}_n^*$ is a public random value. After collecting masked c_j's from $|\mathbf{x}' \cap \mathbf{x}_B|$ STs, the auctioneer calculates

$$\begin{aligned} & \prod_{\{j|x_j \in \mathbf{x}' \cap \mathbf{x}_B\}} g_i^{c_j d_{ij}} \cdot h^{R_j} \\ = \; & g_i^{\sum_{\{j|x_j \in \mathbf{x}' \cap \mathbf{x}_B\}} c_j d_{ij}} \cdot h^{\sum \{j|x_j \in \mathbf{x}' \cap \mathbf{x}_B\} R_j} \\ = \; & g_i^{\sum_{\{j|x_j \in \mathbf{x}' \cap \mathbf{x}_B\}} c_j d_{ij}} \cdot h^{|\mathbf{x}' \cap \mathbf{x}_B| \cdot n} = \text{Enc}_i(z_i). \end{aligned}$$

The last second equation comes from (11). We notice that $g_i^{\sum_{\{j|x_j \in \mathbf{x}' \cap \mathbf{x}_B\}} c_j d_{ij}} \cdot h^{|\mathbf{x}' \cap \mathbf{x}_B| \cdot n}$ is actually the Paillier encryption of $\sum_{\{j|x_j \in \mathbf{x}' \cap \mathbf{x}_B\}} c_j d_{ij}$ with random value $h^{|\mathbf{x}' \cap \mathbf{x}_B|}$ using ST i's public encryption key. Since the auctioneer does not have ST i's private decryption key, it cannot obtain the plaintext z_i. The reason we protect z_i from the auctioneer is that z_i is actually the linear combination of c_i's. Obtaining sufficient number of z_i's during multiple iterations, the auctioneer can generate a linear equation system and derive c_i's. Although ST i has a decryption key, it cannot decrypt $g^{c_j d_{ij}} \cdot h^{R_j}$ to obtain its peers' bids c_j's due to the random value h^{R_j}.

The computation of $\text{Enc}_A(z_i)$ at ST j ($x_j \in \mathbf{x}_B$) is similar to that at the auctioneer. Here, $\text{Enc}_A(\cdot)$ stands for the encryption with the auctioneer's Paillier encryption key. Although the auctioneer can decrypt $\text{Enc}_A(z_i)$, ST j won't share $\text{Enc}_A(z_i)$ with the auctioneer; otherwise z_i will expose ST j's own private information c_j. We also apply the similar privacy-preserving data aggregation approach to compute $C_t'^*$ in line 25. We do not calculate $\mathbf{c}^\top \mathbf{x}_B^*$ and Q_0 separately. The reason will be explained in Section V. In particular, we first express $C_t'^*$ as $\mathbf{c}^\top \mathbf{x}_B^* + \sum_{i \in \mathcal{N}_e} c_i \overline{x_i} + c_k x_k = \mathbf{c}^\top \mathbf{x}$. Then, by asking all STs to participate in data aggregation, the auctioneer can obtain $C_t'^*$ with individual c_i's hidden.

Remark 3 The last question left in Algorithm 1 is how the auctioneer and ST i (ST j and the auctioneer) compare z_i and c_i (z_i and 0) while preserving privacy. Let us take the comparison between z_i and c_i as an example. First, the auctioneer will not send $\text{Enc}_i(z_i)$ to ST i directly, because ST i can infer other STs' bids from sufficient number of z_i's by formulating and solving a linear equation system. With the knowledge of others' bids, ST i can manipulate the auction outcome and impair the auctioneer's revenue[4]. Second, ST i will not submit its private information c_i to the auctioneer for comparison. Therefore, we apply a Paillier cryptosystem based secure comparison mechanism [34] to enable the privacy-preserving comparison between z_i and c_i. The secure comparison protocol could be briefly described as follows. ST i first encrypts $-c_i$[5] into $\text{Enc}_i(-c_i)$ using its own Paillier encryption key. $\text{Enc}_i(-c_i)$ is then sent to the auctioneer. Choosing a large random number $r \in \mathbb{Z}_n$ and a relative small random number $r' \in \mathbb{Z}_n$, the auctioneer calculates $(\text{Enc}_i(-c_i)\text{Enc}_i(z_i))^r \text{Enc}_i(-r') = \text{Enc}_i(r(z_i - c_i) - r')$, where $\text{Enc}_i(z_i)$ is obtained via data aggregation ahead. $\text{Enc}_i(r(z_i - c_i) - r')$ is then sent back to ST i for decryption. Obviously, if $r(z_i - c_i) - r' > 0$, then $z_i - c_i > 0$; otherwise, $z_i - c_i < 0$. Since $z_i - c_i$ is masked by random numbers r and r', without the knowledge of them, ST i cannot infer z_i. In all, ST i is unaware of z_i and the auctioneer is unaware of both c_i and z_i during the secure comparison. The process that ST j and the auctioneer compare z_i and 0 is similar to above. Thus we skip its discussion here.

[4]For instance, if ST i has the highest bid 10, with the knowledge that the second highest bid is 9.9, ST i may quit from this auction and wait for the next one.

[5]In a modulo field n, negative numbers are shifted to the upper half of the range $[0, n-1]$, i.e., $[(n-1)/2+1, n-1]$, with $-1 = n-1 \mod n$

B. Privacy-Preserving BIP Algorithm

Based on the privacy-preserving LP algorithm proposed in the previous subsection, we are now ready to develop the privacy-preserving BIP algorithm allowing the auctioneer to optimally solve t-OOP without knowing c_i's. Its details are given by Algorithm 2. We denote by Live the set of unexplored subproblems. In each iteration, a subproblem K is selected for exploration from Live. Then, a branching is performed: by letting the selected subproblem's corresponding variable x_k be either 0 and 1, and relaxing binary constraints, two child subproblems, K_0 and K_1, are formulated. Algorithm 1 is then applied to solve these two child LP subproblems. Line 7 to line 15 discuss different actions this algorithm takes in different cases. First, in the case that the relaxed LP subproblem does not have any feasible solution, the subproblem is discarded (or fathomed). Second, if the relaxed LP subproblem has a feasible solution, but $C_t'^* \leq C_t^*$, the subproblem is also fathomed. Third, if $C_t'^* > C_t^*$ and the solution is an integral solution, the obtained result $C_t'^*$ and solution $\{\mathbf{x}_B^*, \mathbf{x}_N^*\}$ are kept as the current best finding. Fourth, otherwise, i.e., if $C_t'^* > C_t^*$ and the solution is not an integral solution, it is possible that a better integral solution exists. Thus, the child subproblem is then added to Live. The iteration continues until all subproblems have been explored.

C. Privacy-Preserving Pricing

As we discussed before, if an ST's bid is revealed at the end of an auction for pricing purpose, the auctioneer can utilize it to manipulate favorable outcomes of sequential auctions. Even though an ST's bid may vary in different auctions based on its current status, e.g., traffic load and etc., the auctioneer can still predict it by analyzing this ST's existing bids. Therefore, we need to protect bid privacy in pricing procedure as well.

Following (8), the charging price for a winning ST is the sum of all its charging price p_i^t's in all winning iterations H_i. Without loss of generality, we discuss how to calculate $p_i^t = C_{t,-\mathbf{i}} - (C_t - c_i)$ with c_i protected. Instead of obtaining $C_{t,-\mathbf{i}}$ and c_i separately, we propose to have the auctioneer know $C_{t,-\mathbf{i}} + c_i$ as a whole value. As $C_{t,-\mathbf{i}}$ can be obtained by recalculating t-OOP with x_i excluded from both the objective function and the constraint, $C_{t,-\mathbf{i}} + c_i$ can be directly derived by adding c_i to $C_{t,-\mathbf{i}}$. In particular, when calculating $C_{t,-\mathbf{i}}'^*$ in Algorithm 1, we propose all STs, including i, to participant in this data aggregation, where i always contributes c_i. Therefore, the auctioneer actually obtains $C_{t,-\mathbf{i}}'^* + c_i$ for each relaxed

Algorithm 2 Privacy-Preserving BIP Algorithm

Input: $\mathbf{c}$, $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $C_t^* = -\infty$, $Live = \{K_{ini}\}$
Output: $\mathbf{x}^*$, and C_t^*

```
while Live≠ ∅ do
    Pop out a subproblem K associated with variable x_k from Live to be processed;
    Live = Live/{K};
    Branch on x_k generating K_0 and K_1;
    for 0 ≤ i ≤ 1 do
        Solving K_i by Algorithm 1;
        if K_i does not has any feasible solution then
            Fathom K_i;
        else if C'_t* ≤ C*_t then
            Fathom K_i;
        else if x*_B and x*_N are integral then
            C*_t = C'_t*, x* = {x*_B, x*_N};
        else
            Live = Live ∪ {K_i};
        end if
    end for
end while
```

LP problem and thus $C_{t,-\mathbf{i}} + c_i$ in the pricing procedure. Since the auctioneer obtains $C_{t,-\mathbf{i}} + c_i$ as a whole value, it cannot identify c_i separately. Together with C_t obtained in spectrum allocation procedure, p_i^t is available at the auctioneer. Following the similar approach, the auctioneer can calculate all p_i^t's ($t \in H_i$) and thus p_i.

V. Performance Analysis

In this section, we first prove that our proposed PPER spectrum auction is economic-robust. Then, we analyze how the privacy of STs' bids is protected. We also conduct simulations to evaluate the performance of PPER, and compare it with an existing privacy-preserving spectrum auction scheme THEMIS [10], in terms of computation time, communication cost, and auction outcome.

A. Economic-Robustness Analysis

In the following, we will demonstrate that our proposed PPER spectrum auction is economic-robust. Since a winning ST can receive multiple spectrums which are determined in multiple iterations of auctions in our scheme, the economic property analysis is more complicated than that in the existing works. To prove the economic-robustness of the proposed spectrum auction scheme, we first have the following lemma:

Lemma 1: When the other STs' bids, i.e., $\mathbf{c}_{-\mathbf{i}}$, are fixed, if a BG that contains ST i with bid c_i wins in the t-th iteration, it also wins by the t-th iteration when ST i bids $c_i' > c_i$.

Proof: For a winning BG $\mathcal{G}_{W,t}$ ($t \in H_i$) that contains ST i with bid c_i and wins in the t-th iteration, its group bid is $C_t = c_{-i}^t + c_i$, where $c_{-i}^t = \sum_{j \in \{\mathcal{G}_{W,t} \setminus \{i\}\}} c_j$. When ST i bids $c_i' > c_i$, this BG's new group bid, denoted by C_t', is $C_t' = c_{-i}^t + c_i' > c_{-i}^t + c_i = C_t$.

For any BG $\mathcal{G}_s$ that does not contain ST i and loses in all t iterations when i bids with c_i, we denote its group bid when ST i bids with c_i and with c_i' by C_s and C_s', respectively. Since the other STs' bids remain the same, we have $C_s' = C_s \leq C_t < C_t'$. Therefore, the BGs which do not contain i and lose in all t iterations when i bids with c_i will still lose when i bids c_i'. Besides, for BGs also contain ST i but with their group bids lower than C_t, they won't beat C_t' when i bids c_i', since the bids from BGs containing ST i will increase by the same amount. In all, BG $\mathcal{G}_{W,t}$ must also win no later than the t-th iteration.

■

Using the above lemma, we can arrive at the following theorem.

Theorem 1: The proposed spectrum auction framework is incentive compatibility.

Proof: We need to show that for any ST i with any $c_i \neq v_i$ while the others' bids are fixed, the condition in (2) holds. Let $u_i(c_i, \mathbf{c}_{-\mathbf{i}})$ and $u_i(v_i, \mathbf{c}_{-\mathbf{i}})$ denote ST i's utility when it bids c_i and v_i, respectively. We first consider the scenario where $c_i > v_i$.

- **Case 1**: *ST i loses with both v_i and c_i*. In this case, $u_i(c_i, \mathbf{c}_{-\mathbf{i}}) = u_i(v_i, \mathbf{c}_{-\mathbf{i}}) = 0$ according to our definition in (1). Thus, (2) holds.
- **Case 2**: *ST i loses with v_i but wins with c_i*. In this case, obviously we have $u_i(v_i, \mathbf{c}_{-\mathbf{i}}) = 0$. For $u_i(c_i, \mathbf{c}_{-\mathbf{i}})$, it can be calculated by

$$\begin{aligned} u_i(c_i, \mathbf{c}_{-\mathbf{i}}) &= \sum_{t \in H_i} \left(v_i - C_{t,-\mathbf{i}} + (C_t - c_i)\right) \\ &= \sum_{t \in H_i} (C_t' - C_{t,-\mathbf{i}}) < 0, \end{aligned}$$

  where C_t' is group $\mathcal{G}_{W,t}$'s bid when ST i bids v_i. We have $C_t' = v_i + C_t - c_i < C_{t,-\mathbf{i}}$, since ST i loses when it bids v_i.
- **Case 3**: *ST i wins with v_i and loses with c_i*. Since $c_i > v_i$, according to Lemma 1, this will not happen.
- **Case 4**: *ST i wins with both v_i and c_i*. We denote the set of the indices of the iterations where i wins by bidding c_i and v_i by H_i and H_i', respectively. This case can be further divided into two subcases. In the first subcase, the set of winning BGs when ST i bids c_i and that when ST i bids v_i, denoted by $\mathcal{G}_W(c_i)$ and $\mathcal{G}_W(v_i)$, respectively, are the same. In the second one, $\mathcal{G}_W(c_i)$ and $\mathcal{G}_W(v_i)$ are different, it means at least one of the winning BGs when ST i bids v_i loses when i bids c_i according to Lemma 1. Since the first subcase can be treated as a special instance for the latter, we focus on the IC proof for the second subcase in the following.
  When ST i bids c_i, denote its utility attributed to the common BGs between $\mathcal{G}_W(c_i)$ and $\mathcal{G}_W(v_i)$ by $u_i^1(c_i, \mathbf{c}_{-\mathbf{i}})$ and the utility attributed to the other BGs by $u_i^2(c_i, \mathbf{c}_{-\mathbf{i}})$. When ST i bids v_i, denote its utility attributed to the common BGs between $\mathcal{G}_W(c_i)$ and $\mathcal{G}_W(v_i)$ by $u_i^1(v_i, \mathbf{c}_{-\mathbf{i}})$ which is exactly $u_i(v_i, \mathbf{c}_{-\mathbf{i}})$. Then, we have the following results.
  First, for those common BGs between $\mathcal{G}_W(c_i)$ and

$\mathcal{G}_W(v_i)$,

$$\begin{aligned} & u_i^1(c_i, \mathbf{c}_{-\mathbf{i}}) - u_i^1(v_i, \mathbf{c}_{-\mathbf{i}}) \\ = & \sum_{t \in (H_i \cap H_i')} (v_i - C_{t,-\mathbf{i}} + C_t - c_i) \\ - & \sum_{t' \in (H_i \cap H_i')} (v_i - C_{t',-\mathbf{i}} + C_{t'} - v_i). \end{aligned}$$

Since $\mathcal{G}_W(c_i)$ and $\mathcal{G}_W(v_i)$ are identical, we have $\sum_{t \in (H_i \cap H_i')} v_i = \sum_{t' \in (H_i \cap H_i')} v_i$. In addition, since the bids from any BG that does not include ST i when i bids either c_i or v_i are the same, the exclusion of ST i from the auction won't change their relative relationships as well. Therefore, we have $C_{t,-\mathbf{i}} = C_{t',-\mathbf{i}}$ and thus $\sum_{t \in (H_i \cap H_i')} C_{t,-\mathbf{i}} = \sum_{t' \in (H_i \cap H_i')} C_{t',-\mathbf{i}}$. In all, we arrive at $u_i^1(c_i, \mathbf{c}_{-\mathbf{i}}) = u_i^1(v_i, \mathbf{c}_{-\mathbf{i}})$.

Second, for any BG in $\mathcal{G}_W(c_i)$ but not in $\mathcal{G}_W(v_i)$, since $v_i + C_t - c_i = C_t' < C_t = C_{t,-\mathbf{i}}$, we have

$$u_i^2(c_i, \mathbf{c}_{-\mathbf{i}}) = \sum_{t \in H_i \setminus (H_i \cap H_i')} (v_i - C_{t,-\mathbf{i}} + (C_t - c_i)) < 0.$$

As a result, we can get

$$\begin{aligned} & u_i(c_i, \mathbf{c}_{-\mathbf{i}}) - u_i(v_i, \mathbf{c}_{-\mathbf{i}}) \\ = & u_i^1(c_i, \mathbf{c}_{-\mathbf{i}}) - u_i^1(v_i, \mathbf{c}_{-\mathbf{i}}) + u_i^2(c_i, \mathbf{c}_{-\mathbf{i}}) < 0. \end{aligned}$$

The proof is similar when $c_i < v_i$, which is omitted due to space limit. In general, $u_i(c_i, \mathbf{c}_{-\mathbf{i}}) \leq u_i(v_i, \mathbf{c}_{-\mathbf{i}})$ always hold, and hence the spectrum auction is IC. ■

***Theorem** 2:* The proposed spectrum auction framework is individual rationality.

Proof: For a winning ST i, its utility is expressed as

$$\begin{aligned} & u_i(c_i, \mathbf{c}_{-\mathbf{i}}) = \sum_{t \in H_i} (v_i - C_{t,-\mathbf{i}} + (C_t - c_i)) \\ = & \sum_{t \in H_i} (-C_{t,-\mathbf{i}} + C_t) > 0. \end{aligned}$$

For a losing ST i, its utility is 0. In all, ST i always gets non-negative utility. ■

***Theorem** 3:* The proposed spectrum auction framework is budget balance.

Proof: For a winning ST i, its clearing price is expressed as

$$p_i = \sum_{t \in H_i} p_i^t = \sum_{t \in H_i} (C_{t,-\mathbf{i}} - (C_t - c_i)) \geq 0$$

For a losing ST i, its clearing price is 0. Thus, the total revenue received by the auctioneer, i.e., $\sum_{i \in \mathcal{N}} p_i$, is non-negative. ■

With Theorem 1, 2 and 3, we conclude that the proposed spectrum auction scheme is economic-robust.

B. Privacy Analysis

We now analyze the STs' bid privacy is protected in both spectrum allocation and pricing procedures under the proposed PPER scheme. In particular, we focus on the privacy analysis of Algorithm 1, which is the main component of solving spectrum allocation and pricing problems.

TABLE I
NOTATIONS OF OPERATIONS.

Operations	Description
Exp	Exponentiation
Mul	Multiplication
Enc_1/Dec_1	Paillier Encryption/Decryption
Enc_2/Dec_2	RSA Encryption/Decryption

We start by examining the information known by the auctioneer when calculating $\text{Enc}_i(z_i)$ in Algorithm 1. As we described in Section IV-A, each ST j ($x_j \in \mathbf{x}' \cap \mathbf{x}_B$) submits $g_i^{c_j d_{ij}} \cdot h^{R_j}$ to the auctioneer. Although the auctioneer is able to obtain $\text{Enc}_i(z_i)$ by data aggregation, it cannot decrypt to obtain $c_j d_{ij}$ and thus infer c_j, as it does not have ST i's private decryption key. Although with the private decryption key, ST i cannot decrypt $g_i^{c_j d_{ij}} \cdot h^{R_j}$ to obtain c_i either due to the random number h^{R_j}. This data aggregation scheme is proven to be semantically secure [33]. For the similar reason, an ST's bid is also protected from the auctioneer and other STs when computing $\text{Enc}_A(z_i)$'s and $C_t'^*$. In Algorithm 1, since the auctioneer and ST i compare z_i and c_i via secure comparison, z_i and c_i are protected from ST i and the auctioneer, respectively. In addition, the auctioneer is unaware of z_i during comparison either. This is necessary as we explained in Section IV-A that any entity can reveal c_j's by collecting sufficient number of z_i's.

We now explain why we do not separately calculate $\mathbf{c}_B^\top \mathbf{x}_B^*$ and Q_0 when calculating $C_t'^*$. In algorithm 1, we calculate $\mathbf{c}^\top \mathbf{x}_B^* + \sum_{i \in \mathcal{N}_e} c_i \overline{x_i} + c_k x_k$ via privacy-preserving data aggregation. This is because if Q_0 is available at the auctioneer, it will have $Q_0(x_k = 0)$ and $Q_0(x_k = 1)$ for two subproblems K_0 and K_1, according to Algorithm 2. Moreover, we have $Q_0(x_k = 1) - Q_0(x_k = 0) = (\sum_{i \in \mathcal{N}_e} c_i \overline{x_i} + c_k) - (\sum_{i \in \mathcal{N}_e} c_i \overline{x_i}) = c_k$, which is ST k's bid. If the auctioneer only has the knowledge of $C_t'^*$, even though it knows two $C_t'^*$'s obtained under $x_k = 0$ and $x_k = 1$, it cannot infer c_k because the corresponding $\mathbf{c}_B^\top \mathbf{x}_B^*$'s under $Q_0(x_k = 0)$ and $Q_0(x_k = 1)$ are not the same also.

C. Simulation Results

We randomly deploy a number of SUs in a square network of area 1×1. The STs are randomly chosen and their SRs are randomly selected from the nodes within their transmission ranges. All STs' transmission ranges and interference ranges are set to 0.05 and 0.1, respectively. The STs' true valuations of (and hence their bids for) a spectrum are assumed to be i.i.d random variables uniformly distributed over (0,10]. Besides, there are totally 30 STs, 30 SRs, and 1-5 spectrums in the network. To secure the communication among STs when generating random value in data aggregation, RSA-1024 is adopted. For Paillier cryptosystem based operations, including data aggregation and secure comparison, we set its modulus $n = 1024$.

For the computation time of PPER, we focus on analyzing the time spent on cryptographic calculations since they are much more time-consuming than normal arithmetics.

We first discuss the computation related to data aggregation, including generating $\text{Enc}_i(z_i)$, $\text{Enc}_A(z_i)$, $C_t'^*$ and $C_{t,-\mathbf{i}}+c_i$ for pricing. In the process of generating $\text{Enc}_i(z_i)$, the auctioneer's computation is to multiply together all data received from STs, resulting in $(|\mathbf{x}' \cap \mathbf{x}_B| - 1) \times Mul$. An ST j's ($x_j \in \mathbf{x}' \cap \mathbf{x}_B$) computation includes: encrypting its generated random number with its peer's RSA encryption key, decrypting its received data by its own decryption key, and masking c_j with R_j. Thus, its computation complexity contains: $(|\mathbf{x}' \cap \mathbf{x}_B| - 1) \times Enc_2$, $(|\mathbf{x}' \cap \mathbf{x}_B| - 1) \times Dec_2$, $2 \times Exp$, and $1 \times Mul$. For generating $\text{Enc}_A(z_i)$, the computation complexity of an ST j ($x_j \in \mathbf{x}' \cap \mathbf{x}_B$) is the same above. If it is selected to compute $\text{Enc}_A(z_i)$, its computation complexity is added by $(|\mathbf{x}' \cap \mathbf{x}_B| - 1) \times Mul$. For generating $C_t'^*$, the auctioneer's computation complexity is $(|\mathbf{x}'| - 1) \times Mul$. The computation complexity of an ST j ($x_j \in \mathbf{x}'$) contains: $(|\mathbf{x}'| - 1) \times Enc_2$, $(|\mathbf{x}'| - 1) \times Dec_2$, $2 \times Exp$, and $1 \times Mul$. For generating $C_{t,-\mathbf{i}} + c_i$, the computation complexity at the auctioneer and STs is the same as that in generating $C_t'^*$.

We then discuss the computation related to secure comparison, including: comparing z_i and c_i, and z_i and 0. When the auctioneer and ST i compare z_i and c_i, the auctioneer's computation includes: encrypting $-r'$ and calculating $(\text{Enc}_i(z_i)\text{Enc}_i(-c_i))^r\text{Enc}_i(-r')$, resulting in $1 \times Enc_1$, $1 \times exp$, and $2 \times mul$. ST i's computation includes encrypting $-c_i$ and decrypting $\text{Enc}_i(r(z_i - c_i) - r')$, resulting in $1 \times Enc_1$ and $1 \times Dec_1$. When ST j and the auctioneer compare z_i and 0, the procedures are almost the same, except the roles exchange. Thus, the auctioneer's computation complexity becomes: $1 \times Enc_1$ and $1 \times Dec_1$, while ST j's computation complexity becomes: $1 \times Enc_1$, $1 \times exp$, and $2 \times mul$.

We show the computation time and communication cost at both ST and auctioneer in Table II and Table III, respectively. We notice that the average computation time at an ST is lower than that at the auctioneer, for the auctioneer has to participate in each secure comparison while an ST participates in one secure comparison. Besides, as only the STs associated with basic variables involve in data aggregation procedures, this also alleviates the computation burden at STs. From Table II and Table III, we find the ST has lower computation time and communication cost than the auctioneer. These results further validate our PPER scheme: we leave most of the computation and communication tasks to the auctioneer, which is rich in computation and energy resources, so as to save the limited resources at STs.

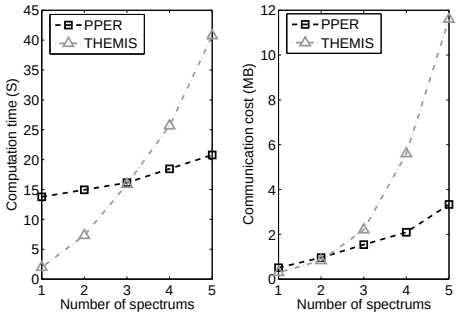
TABLE II
COMPUTATION TIME OF PPER.

Network Size	ST	Auctioneer	Total Comp. Time
$N = 20, L = 2$	3.62 s	5.72 s	8.34 s
$N = 30, L = 2$	5.43 s	9.51 s	14.94 s

TABLE III
COMMUNICATION COST OF PPER.

Network Size	ST	Auctioneer	Total Comp. Time
$N = 20, L = 2$	110.6 KB	136.9 KB	247.5 KB
$N = 30, L = 2$	295.1 KB	326.4 KB	621.5 KB

We then compare the the computation time and communication cost of PPER and THEMIS. Since THEMIS requires



(a) Computation time (b) Communication cost

Fig. 2. Computation time and communication cost comparison under different numbers of spectrums.

that all bidders choose their bids from a set of possible values, we set this number to 1000 following the parameter settings in [10].

Specifically, Fig. 2(a) shows the computation time of PPER and THEMIS under different numbers of spectrums. We find that PPER can be much more computationally efficient than THEMIS especially when $L > 3$. This is because THEMIS contains large amount of multiplications among Paillier Encryption data, while PPER is based on solving small-scale LP problems. Besides, the computation time of THEMIS increases fast since its possible node-spectrum allocation patterns increase exponentially to the number of spectrums. Fig. 2(b) demonstrates the communication cost between them under different numbers of spectrums. We can see that PPER introduces a lower communication cost when $L > 2$.

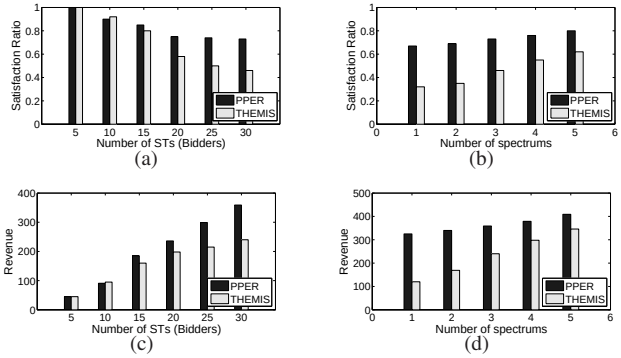


Fig. 3. Satisfaction ratio and revenue under different numbers of STs and spectrums.

Fig. 3 compares the satisfaction ratio and the auctioneer's revenue of the proposed PPER with those of THEMIS, under different numbers of STs and spectrums. Here, satisfaction ratio is defined as the ratio of the number of STs who have finally successfully delivered their traffics to the total number of STs.

As shown in Fig. 3(a), when the number of STs increases, THEMIS's satisfaction ratio drops significantly, while our PPER's satisfaction ratio remains relatively stable. Thus, when there are more STs in the network ($\geq$ 20), PPER achieves much higher satisfaction ratio than the other. Particularly, in the case that there are 30 STs in the network, the satisfaction

ratio of PPER and THEMIS are 0.73 and 0.46, respectively. As mentioned before, this is because in the existing auction schemes, it is not clear whom a winning ST communicates with and there can be more serious collisions in the network as the number of STs increases. Besides, THEMIS allocates spectrums in a greedy manner which further reduces its satisfaction ratio. Moreover, Fig. 3(b) compares the satisfaction ratio of these two schemes under different numbers of spectrums when there are 30 STs in the network. As the number of spectrums increases, the satisfaction ratio increases as well. We can see that when the spectrum resource is scarce, PPER achieves much higher satisfaction ratio than the other.

We also study the revenue generated by PPER and that by THEMIS in Fig. 3(c) and Fig. 3(d). We observe that under the same number of STs, our scheme achieves higher revenues than the other. Particularly, as shown in Fig. 3(c), in the case that there are 30 STs in the network, the revenues of PPER and THEMIS are 359 and 240, respectively. Besides, as shown in Fig. 3(d), our scheme achieves much higher revenues than the other, especially when there are not many available spectrums.

VI. Conclusions

In this paper, we have developed a privacy-preserving economic-robust spectrum auction scheme, called PPER. Specifically, we first construct an economic-robust auction framework which consists of two procedures: spectrum allocation and pricing. Then, a privacy-preserving auction scheme is proposed to protect the STs' bid privacy. We have analyzed the privacy of PPER and found that the STs' bid privacy can be well protected during the entire auction process. Extensive simulation results have demonstrated that our scheme achieves higher satisfaction ratio and revenue than previous work with low computation and communication costs.

References

[1] L. Gao, X. Wang, Y. Xu, and Q. Zhang, "Spectrum trading in cognitive radio networks: A contract-theoretic modeling approach," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 843–855, 2011.

[2] A. Gopinathan, Z. Li, and C. Wu, "Strategyproof auctions for balancing social welfare and fairness in secondary spectrum markets," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'11)*, Shanghai, China, April 2011.

[3] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, "Revenue generation for truthful spectrum auction in dynamic spectrum access," in *Proceeding of ACM MobiHoc*, New Orleans, Louisiana, US, May 2009.

[4] M. Al-Ayyoub and H. Gupta, "Truthful spectrum auctions with approximate revenue," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'11)*, Shanghai, China, April 2011.

[5] X. Zhou and H. Zheng, "Trust: A general framework for truthful double spectrum auctions," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'09)*, Rio de Janeiro, Brazil, April 2009.

[6] W. Wang, B. Li, and B. Liang, "District: Embracing local markets in truthful spectrum double auctions," in *Proc. of IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, SECON, 2011*, Salt Lake, UT, June 2011.

[7] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "ebay in the sky: Strategy-proof wireless spectrum auctions," in *Proceedings of ACM MobiCom*, San Francisco, CA, USA, September 2008.

[8] J. Huang, R. A. Berry, and M. L. Honig, "Auction-based spectrum sharing," *Journal of Mobile Networks and Applications*, vol. 11, no. 3, pp. 405–418, 2006.

[9] M. Li, P. Li, M. Pan, and J. Sun, "Economic-robust transmission opportunity auction in multi-hop wireless networks," in *Proceedings of IEEE INFOCOM*, Turino, Italy, April 2013.

[10] 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, 2011.

[11] P. Klemperer, "What really matters in auction design," *Journal of Economic Perspectives*, vol. 16, no. 1, pp. 169–189, 2002.

[12] Q. Huang, Y. Tao, and F. Wu, "Spring: A strategy-proof and privacy preserving spectrum auction mechanism," in *Proceedings of IEEE INFOCOM*, Turin, Italy, April 2013.

[13] H. Huang, X.-Y. Li, Y. e Sun, H. Xu, and L. Huang, "Pps: Privacy-preserving strategyproof social-efficient spectrum auction mechanisms," in *arXiv:1307.7792*, 2013.

[14] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 302–312, 1996.

[15] K. Suzuki, K. Kobayashi, and H. Morita, "Efficient sealed-bid auction using hash chain," in *Proceedings of the Third International Conference on Information Security and Cryptology*, Seoul, Korea, December 2000.

[16] M. Abe and K. Suzuki, "M+1-st price auction using homomorphic encryption," in *Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems*, Paris, France, February 2002.

[17] W. Du, "A study of several specific secure two-party computation problems," Ph.D. Thesis, Purdue University, 2001.

[18] J. Vaidya, "A secure revised simplex algorithm for privacy-preserving linear programming," in *Proceedings of the 23rd IEEE International Conference on Advanced Information Networking and Applications*, Bradford, United Kingdom, May 2009.

[19] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'10)*, San Diego, California, USA, March 2010.

[20] O. L. Mangasarian, "Privacy-preserving linear programming," *Optimization Letters*, vol. 5, no. 1, pp. 165–172, 2011.

[21] Y. Hong, J. Vaidya, and H. Lu, "Secure and efficient distributed linear programming," *Journal of Computer Security*, vol. 20, no. 5, p. 583-634, 2012.

[22] J. Li and M. J. Atallah, "Secure and private collaborative linear programming," in *Proceedings of the 2nd International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Atlanta, Georgia, November 2006.

[23] Y. Pochet and L. Wolsey, *Production Planning by Mixed Integer Programming*. Secaucus, 2006.

[24] *Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*. IEEE802.22, 2011.

[25] J. Perez-Romero, O. Salient, R. Agusti, and L. Giupponi, "A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation," in *Proceedings of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2007*, Dublin, Ireland, April 2007.

[26] H. Zhai and Y. Fang, "Impact of routing metrics on path capacity in multirate and multihop wireless ad hoc networks," in *Proc. of the IEEE International Conference on Network Protocols, ICNP 2006*, Santa Barbara, CA, November 2006.

[27] M. Pan, C. Zhang, P. Li, and Y. Fang, "Joint routing and link scheduling for cognitive radio networks under uncertain spectrum supply," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'11)*, Shanghai, China, April 2011.

[28] G. B. Dantzig and W. Orchard-Hays, *Notes on linear programming: Part v - alternate algorithm for the revised simplex method using product form for the inverse. Technical Report RM-1268*. The RAND Corporation, 1953.

[29] G. B. Dantzig, *Maximization of a Linear Function of Variables Subject to Linear Inequalities*. John Wiley and Sons, 1951.

[30] S. I. Gass, *Linear Programming Methods and Applications*. McGraw-Hill Book Company, 1969.

[31] M. Babaiof and N. Nisan, "Concurrent auctions across the supply chain," *Journal of Artificial Intelligence Research*, pp. 595–629, May 2004.

[32] M. E. Dyer and A. M. Frieze, "Random walks, totally unimodular matrices and a randomised dual simplex method," *Mathematical Programming*, pp. 1–16, 1994.

[33] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in *Proceedings of ACNS*, Singapore, June 2012.

[34] F. Kerschbaum, D. Biswas, and S. de Hoogh, "Performance comparison of secure comparison protocols," in *Proceedings of DEXA*, Linz, Austria, 2009.