SPRING: A Strategy-Proof and Privacy Preserving Spectrum Auction Mechanism

Qianyi Huang, Yixin Tao, and Fan Wu*
Shanghai Key Laboratory of Scalable Computing and Systems
Department of Computer Science and Engineering
Shanghai Jiao Tong University, China
{xywqn, tomtao26}@sjtu.edu.cn; fwu@cs.sjtu.edu.cn

***Abstract*—The problem of dynamic spectrum redistribution has been extensively studied in recent years. Auction is believed to be one of the most effective tools to solve this problem. A great number of strategy-proof auction mechanisms have been proposed to improve spectrum allocation efficiency by stimulating bidders to truthfully reveal their valuations of spectrum, which are the private information of bidders. However, none of these approaches protects bidders' privacy. In this paper, we present SPRING, which is the first Strategy-proof and PRivacy preservING spectrum auction mechanism. We not only rigorously prove the properties of SPRING, but also extensively evaluate its performance. Our evaluation results show that SPRING achieves good spectrum redistribution efficiency with low overhead.**

I. Introduction

The fast growing wireless technology is exhausting the limited radio spectrum. Due to traditional static, expensive, and inefficient spectrum allocation by government, the utilization of radio spectrum is low in spatial and temporal dimensions. On one hand, many spectrum owners are willing to lease out or sell idle spectrum and receive proper payoff. On the other hand, many new wireless applications, starving for spectrum, would like to pay for using the spectrum. Therefore, redistribution of idle radio spectrum is highly important. Open markets, such as Spectrum Bridge [20], have already appeared to improve spectrum utilization by providing services for buying, selling, and leasing idle spectrum.

Due to its fairness and allocation efficiency, auction has become a popular marketing tool to redistribute radio spectrum. In recent years, a number of spectrum auction mechanisms (*e.g.*, [2], [5], [6], [8], [25], [27]–[29], [31], [32]) have been proposed to stimulate the bidders to truthfully reveal their valuations of spectrum/channels in the auction. However, spectrum/channel valuations are the private information of the bidders. Once the valuations are revealed to a corrupt auctioneer, she may exploit such knowledge to her advantage, either in future auctions or by reneging on the sale [15]. Therefore, privacy preservation has been regarded as a major issue in auction design. Unfortunately, none of the existing spectrum auction mechanisms provides any guarantee on privacy preservation.

This work was supported in part by the State Key Development Program for Basic Research of China (Grant No. 2012CB316201), in part by China NSF grant 61170236, 61272443, 61133006, 61073152, and in part by Shanghai Science and Technology fund 12PJ1404900 and 12ZR1414900. The opinions, findings, conclusions, and recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding agencies or the government.

* F. Wu is the corresponding author.

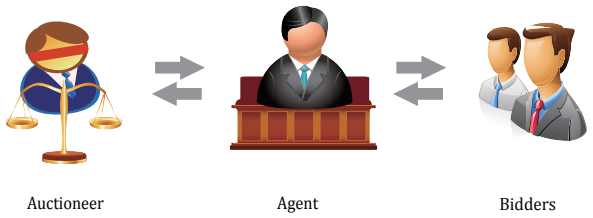


Fig. 1. Auction framework of SPRING.

In a privacy preserving auction (*e.g.*, [15]), any party in the auction can only know the winners together with their charges for the goods and never gain any information beyond the outcome of the auction. However, spectrum is different from traditional goods, due to its spatial reusability, by which two spectrum users can share the same wireless channel simultaneously once they are well-separated (*i.e.*, out of interference range of each other). Thus, existing privacy preserving auction mechanisms cannot be directly applied to spectrum auctions.

Designing a feasible privacy preserving spectrum auction mechanism has its own challenges. The first challenge is strategy-proofness, which applies to auctions in general. In a strategy-proof auction, bidders can maximize their benefits by bidding truthfully. It eliminates market manipulation and misbehavior. The second challenge is bid privacy. True valuations of the spectrum may divulge bidders' profits for serving their subscribers. Bidding truthfully imposes significant risks for bidders' privacy. Both the auctioneer and other participants are supposed to respect the privacy of bidders.

In this paper, we consider the joint problem of designing both strategy-proof and privacy preserving auction mechanisms for spatial reusable radio spectrum. We propose SPRING, which is a Strategy-proof and PRivacy preservING spectrum auction mechanism. As shown in Fig. 1, we introduce an agent in SPRING, who can interact with both the auctioneer and the bidders. The information stored at both the auctioneer and the agent is protected by cryptographic tools, such that neither of them can infer any sensitive information without the help of the other. As long as the agent and the auctioneer do not collude, SPRING can guarantee both strategy-proofness and privacy preservation.

978-1-4673-5946-7/13/$31.00 ©2013 IEEE

We summarize our contributions in this paper as follows.

- To the best of our knowledge, SPRING is the first strategy-proof and privacy preserving auction mechanism for spectrum redistribution.
- We propose a novel and practical technique, called SPRING, to guarantee privacy preservation in a generic strategy-proof spectrum auction mechanism (*e.g.*, [27], [32]). We also extend SPRING to adapt to multi-channel bids, and it still achieves both strategy-proofness and privacy preservation.
- We implement SPRING and extensively evaluate its performance. Our evaluation results show that SPRING achieves good efficiency on spectrum redistribution, while inducing only a small amount of overhead.

The remainder of this paper is organized as follows. In Section II, we briefly review the related work. In Section III, we present technical preliminaries. In Section IV, we present the detailed design of SPRING for the single channel request case. In Section V, we extend SPRING to support multi-channel bids. In Section VI, we show the evaluation results of SPRING. Finally, we conclude our work and point out potential directions for future work in Section VII.

II. Related Work

Spectrum allocation mechanisms have been studied extensively in recent years. A number of works have been presented for market-driven dynamic spectrum auctions. For instance, [27], [31], [32] are early works on auction-based spectrum allocation mechanisms, achieving both strategy-proofness and economic-robustness. Deek *et al.* proposed *Topaz* [5] to guard against time-based cheating in online spectrum auctions. Al-Ayyoub and Gupta [2] designed a polynomial-time truthful spectrum auction mechanism with a performance guarantee on revenue. Xu *et al.* [28], [29] and Yu *et al.* [30] proposed efficient spectrum allocations in multi-channel wireless networks. TAHES [8] addresses both heterogeneous spectrums and interference graph variation. Dong *et al.* [6] tackled the spectrum allocation problem in cognitive radio networks via combinatorial auction. Gao and Wang [10] proposed several algorithms that enable selfish players to converge to the min-max coalition-proof Nash equilibrium (MMCPNE) in channel allocation scheme. However, none of the existing spectrum auction mechanisms provides any guarantee on privacy preservation.

Extensive work has focused on privacy preserving mechanism design for over twenty years. In [14], differential privacy [7] was introduced as a solution concept. In [21], the authors addressed efficiency and privacy tradeoffs in mechanism design and provided a general framework for analyzing the tradeoff. Brandt and Sandholm [3] investigated unconditional full privacy in sealed-bid auctions. In [4], [12], [17], [19], the authors employed various cryptography techniques to achieve security in various auction schemes. Unfortunately, when applied to spectrum auctions, these existing solutions either require exponential complexity, or lead to significant degradation of spectrum utilization. Jointly considering the characteristics of spectrum auction and the privacy of bidders, we are the first to investigate strategy-proof and privacy preserving mechanisms for spectrum auction.

III. Preliminaries

In this section, we first briefly review some important solution concepts from mechanism design, and then present our auction model together with a generic strategy-proof auction for spectrum allocation. Finally, we introduce several useful tools from cryptography.

A. Solution Concepts

We review the solution concepts used in this paper. A strong solution concept from mechanism design is *dominant strategy*.

Definition 1 (Dominant Strategy [16] [9])**.** *Strategy s_i is player i's dominant strategy in a game, if for any strategy $s_i' \neq s_i$ and any other players' strategy profile s_{-i}:*

$$u_i(s_i, s_{-i}) \geq u_i(s_i', s_{-i}).$$

Apparently, a dominant strategy of a player is a strategy that maximizes her utility, regardless of what strategy profile the other players choose.

The concept of dominant strategy is the basis of *incentive-compatibility*, which means that there is no incentive for any player to lie about her private information, and thus revealing truthful information is a dominant strategy for each player. An accompanying concept is *individual-rationality*, which means that every player truthfully participating in the auction is expected to gain no less utility than staying outside. We now introduce the definition of *Strategy-Proof Mechanism*.

Definition 2 (Strategy-Proof Mechanism [13] [24])**.** *A mechanism is strategy-proof when it satisfies both incentive-compatibility and individual-rationality.*

In the field of privacy preservation, k-anonymity [22] is a commonly used criteria for evaluating privacy preserving schemes. A scheme provides k-anonymity protection when a person cannot be distinguished from at least $k-1$ other individuals.

Definition 3 (k-anonymity [22])**.** *A privacy preserving scheme satisfies k-anonymity, if a participant cannot be identified by the sensitive information with probability higher than $1/k$.*

In this paper, we consider the problem of privacy preserving in a semi-honest model, in which each party honestly follows the protocol, but attempts to infer additional information from the messages received during the execution.

B. Auction Model

As shown in Fig. 1, we model the process of spectrum allocation as a sealed-bid auction, in which there is an *auctioneer*, an *agent*, and a group of *bidders*. There are a number of orthogonal and homogenous spectrum channels that can be leased out to a set of bidders. In contrast to existing works (*e.g.*, [27], [31], [32]), we have an additional trustworthy authority, called agent, who can communicate with both the

auctioneer and the bidders. Bidders simultaneously submit their bids (encrypted by the method proposed in this paper) for channels via the agent to the auctioneer, such that no bidder can learn other participants' bids. The auctioneer decides the allocation of channels and the charges for the winners.

We consider that there is a set $\mathbb{C} = \{1, 2, \ldots, c\}$ of orthogonal and homogenous channels. Different from the allocation of traditional goods, wireless channels can be spatially reused, meaning that more than one well-separated bidders can work on the same channel simultaneously, provided that they do not interfere with each other.

We also consider that there is a set $\mathbb{N} = \{1, 2, \ldots, n\}$ of bidders. Each bidder $i \in \mathbb{N}$ requests a single channel (in Section IV) or multiple channels (in Section V), and has a valuation v_i per channel. The per channel valuation may be the revenue gained by the bidder for serving her subscribers, which is also referred to as *type* in literature, and is private to the bidder.

Let $\vec{v} = (v_1, v_2, \ldots, v_n)$ denote the valuation profile of the bidders. In the auction, the bidders choose their bids, denoted by $\vec{b} = (b_1, b_2, \ldots, b_n)$, which are based on their types, and submit the encrypted bids simultaneously to the auctioneer via the agent.

The auctioneer determines the set of winners $\mathbb{W} \subseteq \mathbb{N}$, channel allocation to the bidders $\vec{a} = (a_1, a_2, \ldots, a_n)$, and the charging profile $\vec{p} = (p_1, p_2, \ldots, p_n)$.

Then the utility u_i of bidder $i \in \mathbb{N}$ can be defined as the difference between her valuation on the channels that she wins and the charge p_i:

$$u_i = v_i a_i - p_i.$$

We assume that the bidders are rational. The objective of each bidder is to maximize her utility and she has no preference over different outcomes with equivalent utility. We also assume that the bidders do not collude with each other.

In contrast to the bidders, the overall objective of the auction mechanism is to achieve good channel utilization and satisfaction ratio, while guaranteeing strategy-proofness and privacy preservation. Here, channel utilization is the average number of bidders allocated to each channel; satisfaction ratio is the percentage of winning bidders in the auction.

C. Generic Strategy-Proof Spectrum Auction

In this subsection, we present a generic strategy-proof spectrum auction mechanism, which is general enough to capture the essence of a category of strategy-proof spectrum auction mechanisms (*e.g.*, [27], [32]). The generic spectrum auction presented here works in the case of single channel auction. In Section V, we will show how to extend it to adapt to multi-channel bids.

In the generic spectrum auction, a channel can be leased to several bidders if they can transmit and receive signals simultaneously with an adequate Signal to Interference and Noise Ratio (SINR). We model the interference of the bidders by a conflict graph. Bidders are first divided into non-conflicting groups by any existing graph coloring algorithm (*e.g.*, [26]) in a bid-independent way:

$$\mathbb{G} = \{g_1, g_2, \ldots, g_m\},$$

$$\textit{s.t.}, \; g_j \cap g_l = \emptyset, \forall g_j, g_l \in \mathbb{G}, j \neq l \text{ and } \bigcup_{g_j \in \mathbb{G}} g_j = \mathbb{N}.$$

A group bid σ_j for each group $g_j \in \mathbb{G}$ is calculated as

$$\sigma_j = |g_j| \cdot \min\{b_i | i \in g_j\}.$$

All bidder groups are ranked by their group bids in non-increasing order with bid-independent tie breaking:

$$G' : \sigma'_1 \geq \sigma'_2 \geq \ldots \geq \sigma'_m.$$

Bidders from the top $w = \min(c, m)$ groups are winners. Each winning group is charged with σ'_{w+1} (0, if σ'_{w+1} does not exist). The charge is shared evenly among the bidders in each winning group. Formally, a bidder i from a winning group g_j is charged with price

$$p_i = \begin{cases} \sigma'_{w+1}/|g_j| & \text{if } m > c, \\ 0 & \text{otherwise.} \end{cases}$$

Essentially, the generic spectrum auction guarantees strategy-proofness, because the charge for a winner is independent of her bid. Due to limitations of space, we do not formally prove it.

Theorem 1. *The generic spectrum auction is a strategy-proof mechanism.*

D. Cryptographic Tools

In this paper, we employ two cryptographic tools, including order preserving encryption and oblivious transfer.

1) Order Preserving Encryption: OPES [1] is a representative scheme to encrypt numeric data while preserving the order. It enables any comparison operation to be directly applied on the encrypted data.

Intuitively, we can protect the privacy of bidders in the auction by encrypting the bids in a way that preserves the order and carrying out comparisons directly on the cipher text/value.

2) Oblivious Transfer: Oblivious Transfer (OT) [18] describes a paradigm of secret exchange between two parties, a sender and a receiver.

The receiver can access one of the z secrets from the sender, without getting any information about the remaining $z - 1$ secrets, while the sender has no idea which of the z secrets was accessed. Algorithm 1 shows the pseudo-code of OT_z^1 proposed in [23], where q is a large prime, g and h are two generators of G_q, which is a cyclic group of order q, and Z_q is a finite additive group of q elements. As long as $\log_g h$ is not revealed, g and h can be used repeatedly. SPRING employs an efficient 1-out-of-z oblivious transfer (OT_z^1) of integers [23].

IV. SPRING

In this section, we present SPRING, which is a strategy-proof and privacy preserving spectrum auction mechanism.

Algorithm 1 1-out-of-z Oblivious Transfer (OT_z^1)

Initialization:
System parameters: (g, h, G_q);
Sender's input: $s_1, s_2, \cdots, s_z \in G_q$;
Receiver's choice: $\alpha, 1 \leq \alpha \leq z$;
1: Receiver sends $y = g^r h^\alpha, r \in_R Z_q$;
2: Sender sends $c_i = (g^{k_i}, s_i(y/h^i)^{k_i}), k_i \in_R Z_q, 1 \leq i \leq z$;
3: By $c_\alpha = (d, f)$, receiver computes $s_\alpha = f/d^r$.

A. Design Rational

SPRING integrates cryptographic tools with the generic spectrum auction mechanism to achieve both strategy-proofness and privacy preservation. The main idea of SPRING is to separate the information known by different parties in the auction, so that no party in the auction has enough knowledge to infer any sensitive information with confidence higher than $1/k$, while maintaining the functionality of the generic spectrum auction. We illustrate the design challenges and our idea in this subsection.

(1) Information Separation

If there is a single central authority (auctioneer) carrying out the auction, it is inevitable that the sensitive information (*i.e.*, each bidder's bid) is revealed to the auctioneer. To prevent this threat, we introduce a new entity, called agent. It is the agent's duty to tell the auctioneer the minimal amount of information necessary for deciding the winners and their charges. However, the information should not be fully accessed by the agent to prevent sensitive information leakage. So, we apply an end-to-end asymmetric encryption scheme between the auctioneer and the bidders, so that the agent cannot decrypt the bidding messages.

(2) Bid Encryption

Since the auctioneer needs to find the lowest bid in each bidder group without knowing the exact values of bids from group members, we need a method to map the bids from the bidding space to another value space, while maintaining the comparison relation. We integrate the idea of order preserving encryption to enable such a mapping and prevent the auctioneer from learning the distribution of bids. We let the agent do the order preserving encryption before the auction. When bidding, the bidders contact the agent to get the mapped bids via oblivious transfer, which prevents the agent from knowing which bids are chosen. Later, the agent collects end-to-end encrypted bidding messages from bidders. Only the auctioneer can decrypt the bidding messages, extract mapped bids, and find the lowest mapped bid. The auctioneer can consult the agent to get the original value of the lowest mapped bid.

B. Design Details

SPRING works in four steps shown as follows.

Step 1: Initialization

Before running the spectrum auction, SPRING setups necessary system parameters. SPRING defines a set of possible bid values as

$$\beta = \{\beta_1, \beta_2, \ldots, \beta_z\},$$

in which $\beta_1 < \beta_2 < \ldots < \beta_z$, and requires that each bidder i's bid $b_i \in \beta$.

The agent maps each bid value $\beta_x \in \beta$ to γ_x, while maintaining the order, using the order preserving encryption scheme OPES.

$$\gamma_x = OPES(\beta_x), \ \textit{s.t.}, \ \gamma_1 < \gamma_2 < \ldots < \gamma_z.$$

Here, $\gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_z\}$ is a set of secrets of the agent. The agent also initializes the parameters of oblivious transfer by determining the large prime q and two generators of cyclic group G_q: (g, h).

SPRING employs an asymmetric key encryption scheme. We suppose that the auctioneer holds a private key Key_{priv}, and the matching public key Key_{pub} is distributed to the bidders. SPRING also employs a digital signature scheme, in which each bidder $i \in \mathbb{N}$ holds a signing key sk_i, and publishes the corresponding verification key pk_i.

Step 2: Bidding

Each bidder $i \in \mathbb{N}$ chooses a bid $b_i = \beta_x \in \beta$ according to her per channel valuation v_i, and then interacts with the agent through a 1-out-of-z oblivious transfer to receive $\hat{b}_i = \gamma_x$, which is the order-preserving-encrypted value of β_x.

- Bidder i randomly picks $r \in Z_q$, and sends $y = g^r h^x$ to the agent.
- The agent replies with $c = \{c_1, c_2, \ldots, c_z\}$, in which

$$c_l = \left(g^{k_l}, \gamma_l \left(y/h^l\right)^{k_l}\right), k_l \in_R Z_q, 1 \leq l \leq z.$$

- The bidder picks $c_x = (d, f)$ from c, and computes

$$\hat{b}_i = \frac{f}{d^r} = \frac{\gamma_x \left(y/h^x\right)^{k_x}}{\left(g^{k_x}\right)^r} = \frac{\gamma_x \left(g^r h^x/h^x\right)^{k_x}}{\left(g^{k_x}\right)^r} = \gamma_x.$$

Upon receiving $\hat{b}_i$, bidder i randomly picks a nonce r_i, and encrypts $\left[\hat{b}_i, r_i\right]$ using the auctioneer's public key Key_{pub}:

$$e_i = Encrypt\left(\left[\hat{b}_i, r_i\right], Key_{pub}\right),$$

where $Encrypt()$ is the asymmetric encryption function. Bidder i then submits the following tuple as a bid to the agent

$$\left[i, e_i, Sign(e_i, sk_i)\right],$$

where $Sign()$ is the signing function.

For each tuple $[i, e_i, sign_i]$ received, the agent checks its validity. If

$$Verify(e_i, sign_i, pk_i) = True,$$

where $Verify()$ is the signature verification function, the tuple is accepted. Otherwise, it is discarded.

After collecting all the bids, the agent groups the bidders in a bid-independent way, as in the generic strategy-proof spectrum auction, and publishes the grouping result and encrypted bids, as shown in Table I. To satisfy k-anonymity, we require that each bidder group must contain at least k bidders.

In the table, bidder j_i is the ith member in group g_j, and $e_{j,1}, e_{j,2}, \ldots, e_{j,|g_j|}$ are encrypted bids from bidders in group g_j. Note that the order of $e_{j,i}$'s is irrelevant to the sequence of bidders in group g_j, which means that there is no one-to-one correspondence between $e_{j,i}$ and bidder j_i in any group.

TABLE I
INFORMATION PUBLISHED BY THE AGENT.

Group ID	Bidder ID	Encrypted Bid
1	1_1,1_2,. . .,$1_{\|g_1\|}$	$e_{1,1}, e_{1,2}, \ldots, e_{1,\|g_1\|}$
2	2_1,2_2,. . ., $2_{\|g_2\|}$	$e_{2,1}, e_{2,2}, \ldots, e_{2,\|g_2\|}$
$\vdots$	$\vdots$	$\vdots$
m	m_1, m_2,. . ., $m_{\|g_m\|}$	$e_{m,1}, e_{m,2}, \ldots, e_{m,\|g_m\|}$

Step 3: Opening

For each group $g_l \in \mathbb{G}$, the auctioneer decrypts the bids using her private key to get $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$:

$$\left[\hat{b}_{l,i}, r_{l,i}\right] = Decrypt\left(e_{l,i}, Key_{priv}\right), \forall i \in g_l,$$

where $Decrypt()$ is the asymmetric decryption function.

Since $\hat{b}_{l,i}$'s are computed by the order preserving encryption scheme, the lowest bid in group g_l must also be mapped to the smallest order-preserving-encrypted bid in g_l. Therefore, the auctioneer can locate the lowest bid $\hat{b}_l^{min}$ in group g_l by finding the smallest one in $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$:

$$\hat{b}_l^{min} = \min\left\{\hat{b}_{l,i} | i \in g_l\right\}.$$

Then, the auctioneer resorts to the agent to fetch the original value b_l^{min} of $\hat{b}_l^{min}$:

$$b_l^{min} = OPES^{-1}(\hat{b}_l^{min}),$$

where $OPES^{-1}()$ is the reverse function of the order preserving encryption scheme.

The auctioneer now can calculate the group bid of g_l:

$$\sigma_l = |g_l| \cdot b_l^{min}.$$

Similarly, the auctioneer calculates the group bids $\sigma_1, \sigma_2, \ldots, \sigma_m$ and sorts them in non-increasing order:

$$\sigma_1' \geq \sigma_2' \geq \ldots \geq \sigma_m'.$$

Same as the generic strategy-proof spectrum auction, winners $\mathbb{W}$ are the bidders from top $w = \min(c, m)$ groups:

$$\mathbb{W} = \bigcup_{j=1}^{w} g_j',$$

where g_j' is the group with jth highest group bid. In order to achieve strategy-proofness, each winning bidder group is charged with the group bid σ_{w+1}' of the $(w+1)$th group. (We set $\sigma_{w+1}' = 0$, if the $(w+1)$th group does not exist.) The charge is shared evenly among all group members, hence each bidder i in winning group g_l is charged with

$$p_i = \sigma_{w+1}'/|g_l|.$$

C. Illustrative Example

The following example may help to illustrate our mechanism. Fig. 2 shows the interference range of seven bidders (A - G). They are competing for one channel. Assume that

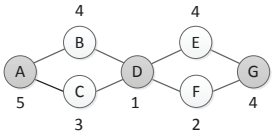


Fig. 2. Conflict graph.

$\beta = \{1, 2, 3, 4, 5\}$ and the number beside each bidder denotes her bid. For clarity and simplicity, we ignore the nonce and the procedures of digital signature/verification.

In the initialization step, the agent applies $OPES$ on β to get $\gamma = \{3, 7, 10, 11, 15\}$. The seven bidders interact with the agent through a 1-out-of-5 oblivious transfer to receive their order-preserving-encrypted bids (*i.e.*, $\hat{b}_A = 15, \hat{b}_B = 11, \ldots, \hat{b}_G = 11$). Each bidder i encrypts her $\hat{b}_i$ with the auctioneer's public key Key_{pub} and submit the result e_i to the agent.

According to the conflict graph, the bidders are split into two groups: $g_1 = \{A, D, G\}$, $g_2 = \{B, C, E, F\}$. The agent publishes the grouping result and the encrypted bids from each group, as shown in Table II.

TABLE II

Group ID	Bidder ID	Encrypted Bid
1	A, D, G	e_D, e_A, e_G
2	B, C, E, F	e_E, e_F, e_B, e_C

The auctioneer decrypts the encrypted bids and locates the lowest bid in each group, which turns out to be $\hat{b}_1^{min} = 3$, $\hat{b}_2^{min} = 7$. Then she resorts to the agent for the original values of $\hat{b}_1^{min}$ and $\hat{b}_2^{min}$, resulting in $b_1^{min} = 1$, $b_2^{min} = 2$. $\sigma_1 = 3 \times 1 = 3$, $\sigma_2 = 4 \times 2 = 8$, thus $\sigma_2 > \sigma_1$. Therefore, g_2 is the winning group and B, C, E, F each is charged with $\sigma_1/4 = 3/4$.

D. Analysis

We will show the strategy-proofness, k-anonymity, as well as some other attractive properties of SPRING.

The strategy-proofness of SPRING is inherited from the generic strategy-proof spectrum auction. Therefore, we omit the proof here and directly draw the following conclusion, due to limitations of space.

Theorem 2. *SPRING is a strategy-proof spectrum auction mechanism.*

Next, we focus on the k-anonymity of SPRING.

Theorem 3. *SPRING guarantees k-anonymity.*

Proof: In SPRING, there are two central authorities, including the auctioneer and the agent. The auctioneer knows the lowest bid in each group, but does not know which bidder it belongs to. The agent knows the encrypted bids, but has no

way to decrypt any of them. Since no other party can get even more information than the auctioneer or the agent, we focus on privacy protection against the auctioneer and the agent in this proof. We recall that each valid bidder group must contain at least k bidders.

On one hand, bidder i gets $\hat{b}_i = \gamma_x$ through a 1-out-of-z oblivious transfer from the agent, who is unaware of which γ_x has been accessed by the bidder. Bidder i then sends the encrypted bid e_i to the agent, who cannot decrypt e_i without knowing the private key of the asymmetric encryption scheme. Although the agent may know the lowest bid in group g_l later when the auctioneer consults her, she still cannot infer its bidder owning to the nouce. So, the agent can not distinguish the bidder of the lowest bid in group g_l from at least k bidders.

On the other hand, although the auctioneer can decrypt an anonymous ciphertext e to get $\hat{b}$, she can only reversely map the lowest $\hat{b}_{min}$ to the original bid b_{min} for each group, resorting to the agent. However, the auctioneer still cannot infer the bidder, to which b_{min} belongs out of at least k members in group g_l.

So, neither the agent, nor the auctioneer, can identify any bidder's bid with probability higher than $1/k$.

Therefore, we can conclude that SPRING guarantees k-anonymity. ∎

Besides strategy-proofness and k-anonymity, SPRING also achieves the following nice properties.

- *Low Communication Overhead*: When z is constant, the communication overhead induced by SPRING is $\mathcal{O}(n)$, where n is the number of bidders.
- *Low Computation Overhead*: The cryptographic tools adopted by SPRING are light weighted schemes, which only induce a small amount of computation overhead. Our evaluation results show that the computation overhead of SPRING is rather low.

V. Extension to Multi-Channel Bids

In the previous section, we propose a strategy-proof and privacy preserving auction mechanism, in which each bidder bids for a single channel. In this section, we extend SPRING to adapt to the scenario in which a bidder can bid for multiple channels. Similarly, our extension achieves both strategy-proofness and k-anonymity.

We now allow each bidder $i \in \mathbb{N}$ to demand d_i channels. Let $\vec{d} = (d_1, d_2, \ldots, d_n)$ denote the demand profile of bidders.

We assume that each bidder has an identical valuation on different channels. In the auction, each bidder i submits not only her encrypted bid per channel v_i, but also the number of channels demanded d_i. We also assume that the bidders do not cheat the demands.

To extend SPRING to adapt to multi-channel bids, we introduce *virtual group*, and update bidding and opening steps of SPRING. Note that the basic version of SPRING presented in Section IV is a special case of the extended SPRING.

A. Virtual Group

In the extended SPRING, the bidders from the same group may demand different numbers of channels. To represent the various demands in a bidder group, we introduce the concept of *virtual group*.

Given a bidder group $g_l \subseteq \mathbb{N}$, let $\hat{d}_l$ be the maximum channel demand in group g_l:

$$\hat{d}_l = \max\{d_i | i \in g_l\}.$$

A virtual group $\tilde{g}_l^j \subseteq g_l$ is the set of bidders, who demand at least j channels in bidder group g_l:

$$\tilde{g}_l^j = \{i | i \in g_l \wedge d_i \geq j\}, 1 \leq j \leq \hat{d}_l.$$

Algorithm 2 shows the pseudo-code of virtual group generation. We find the maximum channel demand $\hat{d}_l$ in group g_l (lines 2-4), and iteratively pick the bidders demanding at least j channels to form virtual group $\tilde{g}_l^j$, which is added into the set G_l of virtual groups generated from group g_l (lines 5-8).

Algorithm 2 Virtual Group Generation— vgrouping(g_l)

Input: Bidder group g_l, demand profile $\vec{d}$.
Output: Set of virtual groups G_l.

```
1: G_l ← ∅; d̂_l ← 0;
2: for all i ∈ g_l do
3:     d̂_l ← max(d̂_l, d_i);
4: end for
5: for j ← 1, ..., d̂_l do
6:     g̃_l^j ← {i | i ∈ g_l ∧ d_i ≥ j};
7:     G_l ← G_l ∪ {g̃_l^j};
8: end for
   Return G_l;
```

In the extended SPRING, an original bidder group g_l is replaced by $\hat{d}_l$ virtual groups. The group bid $\tilde{\sigma}_l^j$ of virtual group $\tilde{g}_l^j$ is defined as

$$\tilde{\sigma}_l^j = \left|\tilde{g}_l^j\right| \cdot \min\{b_i | i \in g_l\}.$$

Note that in order to guarantee k-anonymity, the lowest bid in group g_l, instead of virtual group $\tilde{g}_l^j$, is used to calculate the group bids of virtual groups.

B. Extension Details

The procedures of initialization are the same as those in the basic SPRING. Due to limitations of space, we focus on the differences in the steps of bidding and opening.

Step 1: Initialization

Please refer to Section IV-B for details.

Step 2: Bidding

In order to include the information of channel demands, the tuple submitted by bidder i to the agent must have one more element d_i:

$$[i, e_i, d_i, Sign(e_i || d_i, sk_i)],$$

where $||$ is the concatenation operation.

The agent collects the bidding messages, verifies the validity, and publishes the grouping results and encrypted bids. This time, beside each bidder's ID, there is a corresponding channel demand, as shown in Table III.

TABLE III
INFORMATION PUBLISHED BY THE AGENT.

Group ID	Bidder ID & Demand	Encrypted Bid
1	$[1_1, d_{1_1}],\ldots,[1_{\lvert g_1\rvert}, d_{\lvert g_1\rvert}]$	$e_{1,1},\ldots,e_{1,\lvert g_1\rvert}$
2	$[2_1, d_{2_1}],\ldots,[2_{\lvert g_2\rvert}, d_{\lvert g_2\rvert}]$	$e_{2,1},\ldots,e_{2,\lvert g_2\rvert}$
$\vdots$	$\vdots$	$\vdots$
m	$[m_1, d_{m_1}],\ldots,[m_{\lvert g_m\rvert}, d_{\lvert g_m\rvert}]$	$e_{m,1},\ldots,e_{m,\lvert g_m\rvert}$

Step 3: Opening

The auctioneer is informed of the grouping result and encrypted bids from Table III published by the agent. She decrypts the encrypted bids to get $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$ for each $g_l \in \mathbb{G}$. Resorting to the agent, the auctioneer retrieves the original value of the lowest bid b_l^{min} of each $g_l \in \mathbb{G}$.

The auctioneer invokes Algorithm 2 to form virtual groups:

$$\tilde{\mathbb{G}} = \bigcup_{g_l \in \mathbb{G}} G_l.$$

For each virtual group $\tilde{g}_l^j \in \tilde{\mathbb{G}}$, the auctioneer calculates the virtual group bid:

$$\tilde{\sigma}_l^j = \left|\tilde{g}_l^j\right| \cdot b_l^{min}.$$

Next, the auctioneer sorts all the virtual groups according to their group bids in non-increasing order:

$$\tilde{\sigma}_1'' \geq \tilde{\sigma}_2'' \geq \ldots \geq \tilde{\sigma}''_{\sum_{g_l \in \mathbb{G}} \hat{d}_l}.$$

Auction winners $\mathbb{W}'$ are the bidders in the top $w' = \min(c, \sum_{g_l \in \mathbb{G}} \hat{d}_l)$ virtual groups:

$$\mathbb{W}' = \bigcup_{j=1}^{w'} g_j'',$$

where g_j'' is the jth highest bid virtual group. The number of channels each bidder $i \in \mathbb{W}'$ wins is

$$a_i = \sum_{1 \leq j \leq w' \wedge i \in g_j''} 1.$$

Since a bidder may be in multiple virtual groups, the previous method of charging can no longer be applied. We present a new charging method as shown in Algorithm 3. In Algorithm 3, we remove all the virtual groups generated from the bidder group, to which the winning bidder i belongs, and sort the rest virtual groups by virtual group bid in non-increasing order (lines 1-2). Then, for each channel h won by bidder i, we locate the virtual group in the sorted list, after which wins a channel, bidder i cannot win channel h. If such a virtual group does not exist, then channel h is free of charge for bidder i. Otherwise, the located virtual group's bid is used to calculate the charge for bidder i on channel h. The charge on channel h is set to $\sigma_t^{\triangle}/|\tilde{g}_l^h|$. The total charge for bidder i is the sum of charges on all the channels won (lines 3-9).

Finally, the auctioneer releases the set of winners $\mathbb{W}'$, the channel allocation profile $\vec{a}$, and the charge profile $\vec{p}$.

Similarly, we get the following theorem.

Algorithm 3 Charging Algorithm— charging(i)

Input: Set of virtual groups $\tilde{\mathbb{G}}$ and corresponding virtual group bids $\left(\tilde{\sigma}_l^j\right)_{\tilde{g}_l^j \in \tilde{\mathbb{G}}}$, winner $i \in g_l$.
Output: Charge p_i.
1: $\tilde{\mathbb{G}}' \leftarrow \tilde{\mathbb{G}} \setminus \left\{\tilde{g}_l^j | 1 \leq j \leq \hat{d}_l\right\}$;
2: Sort the virtual groups in $\tilde{\mathbb{G}}'$ by virtual group bid in non-increasing order $\sigma_1^{\triangle} \geq \sigma_2^{\triangle} \geq \ldots \geq \sigma^{\triangle}_{\sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k}$;
3: $p_i \leftarrow 0$;
4: **for** $h \leftarrow 1, \ldots, a_i$ **do**
5: $\quad t \leftarrow \min\left(c - h + 1, \sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k\right)$;
6: $\quad$ **if** $t = c - h + 1$ **then**
7: $\quad\quad p_i \leftarrow p_i + \sigma_t^{\triangle}/|\tilde{g}_l^h|$;
8: $\quad$ **end if**
9: **end for**
Return p_i;

Theorem 4. *SPRING guarantees strategy-proofness and k-anonymity, despite of multi-channel bids.*

Due to space limitations, proof is omitted here (Please refer to [11] for the proof).

VI. EVALUATION

We have implemented SPRING and evaluated its performance on the efficiency of spectrum auction and overheads introduced. In this section, we present our evaluation results.

A. Efficiency

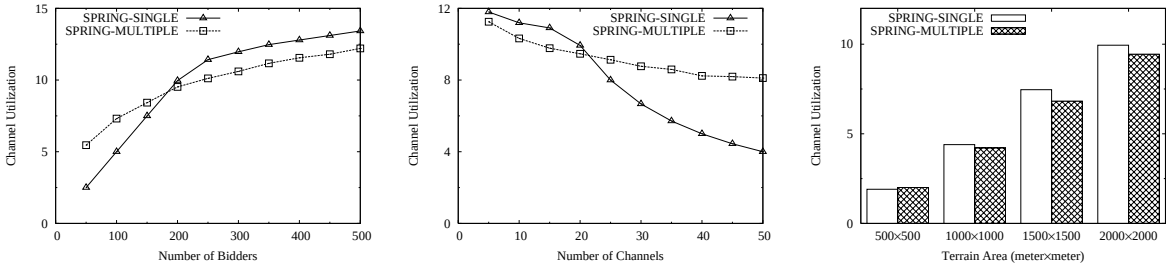
In the evaluation, we measure two metrics on spectrum allocation efficiency, including channel utilization and satisfaction ratio.

- *Channel utilization*: Channel utilization is the average number of bidders allocated to each channel.
- *Satisfaction ratio*: Satisfaction ratio is the percentage of bidders, who get at least one channel in the auction.

We vary the number of bidders from 50 to 500, the number of channels from 5 to 50, and the terrain area from 500 meters $\times$ 500 meters to 2000 meters $\times$ 2000 meters. In each set of evaluations, we vary a factor among bidder number, channel number, and terrain area, and fix the other two. The default value for bidder number, channel number, and terrain area, is 200, 20, and 2000 meters $\times$ 2000 meters, respectively. The bidders are randomly distributed in the terrain area, and the interference range is set to 425 meters. In the case of multi-channel demand, we randomly generate the demand of each bidder from $\{1, 2, 3, 4, 5\}$.

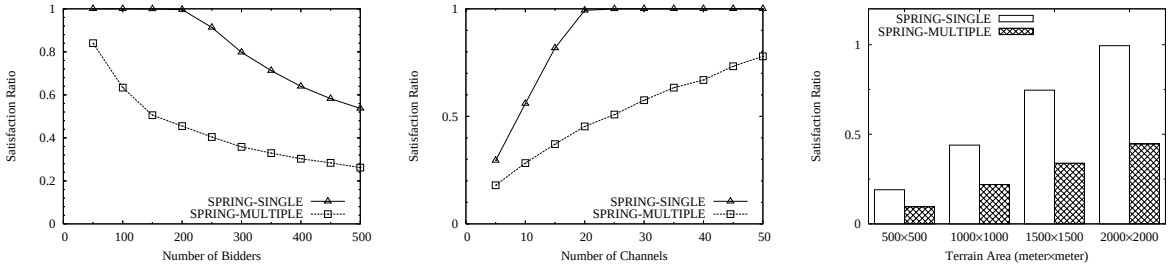
1) Results on Channel Utilization: Fig. 3 shows the evaluation results of SPRING on channel utilization.

Fig. 3(a) shows the channel utilizations achieved by SPRING, when we fix the number of channels and terrain area, and vary the number of bidders. Here we observe that, when the number of bidders is less than 200, the channel utilization of SPRING-SINGLE is lower than that of SPRING-MULTIPLE. This is because the channels are over supplied.



(a) Effect of number of bidders. (b) Effect of number of channels. (c) Effect of size of terrain area.

Fig. 3. Channel utilizations of SPRING, when bidders bid for single and multiple channels.



(a) Effect of number of bidders. (b) Effect of number of channels. (c) Effect of size of terrain area.

Fig. 4. Satisfaction ratios of SPRING, when bidders bid for single and multiple channels.

When we allow the bidders to demand multiple channels, the channels can be better exploited. However, with growth of the number of bidders, especially when the number of bidders is larger than or equal to 200, the channels supplied become more and more scarce compared with the number of bidders, and the competition among the bidders become more and more intense. The introduction of virtual group makes the average (virtual) group size smaller than the single-channel bid case, and thus results in a lower channel utilization.

Fig. 3(b) shows the channel utilizations achieved by SPRING, when varying the number of channels and fixing the other two factors. When the number of channels is no more than 20, SPRING-MULTIPLE has a lower channel utilization than SPRING-SINGLE, due to the smaller average (virtual) group size. However, with more than 20 channels supplied, SPRING-MULTIPLE has a higher channel utilization than SPRING-SINGLE, due to higher demands from the bidders.

Fig. 3(c) shows the case, in which we vary the size of terrain area and fix the other two factors. When the terrain area is 500 meters $\times$ 500 meters or 1000 meters $\times$ 1000 meters, most of the (virtual) groups contain only 1 or 2 bidders, thus the difference between SPRING-SINGLE and SPRING-MULTIPLE is very small. However, with the increment of terrain area, the difference between SPRING-SINGLE and SPRING-MULTIPLE on average size of (virtual) groups becomes larger and larger , resulting in the channel utilization of SPRING-MULTIPLE lower than that of SPRING-SINGLE.

2) Results on Satisfaction Ratio: Fig. 4 shows the evaluation results of SPRING on satisfaction ratio.

Fig. 4(a) shows the satisfaction ratio achieved by SPRING, when varying the number of bidders and fixing the other two factors. We can see that when the number of bidders is less than 200, SPRING-SINGLE's satisfaction ratio approximates to 1, meaning that almost every bidder gets a channel in the auction. With the increasing number of bidders, satisfaction ratios of both SPRING-SINGLE and SPRING-MULTIPLE decrease as a result of more interferences. SPRING-MULTIPLE always achieves a lower satisfaction ratio than SPRING-SINGLE, because SPRING-MULTIPLE allows bidders to win multiple channels, leading to the fact that more bidders cannot even obtain a single channel at all.

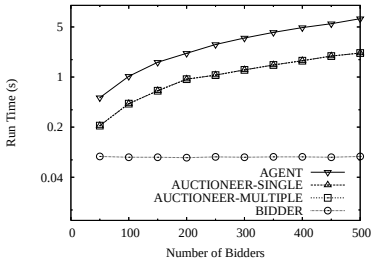
Fig. 4(b) shows the case, in which we vary the number of channels and fix the other two factors. We can see that 20 channels satisfy almost all bidders in the case of SPRING-SINGLE. We also find that the satisfaction ratio of SPRING-SINGLE with 10 channels is almost equal to that of SPRING-MULTIPLE with 30 channels. This is because the demands of bidders in SPRING-MULTIPLE is almost triple of that in SPRING-SINGLE, given the same number of bidders.

Fig. 4(c) shows the case, in which we vary the size of terrain area and fix the other two factors. Again, we can see that SPRING-SINGLE always has a higher satisfaction ratio than SPRING-MULTIPLE in the evaluation.

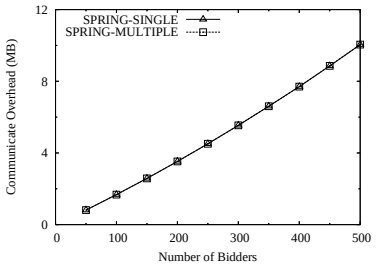
B. Overhead

We implement SPRING using JavaSE-1.7 with packages java.security and javax.crypto, and use RSA with modulus of 1024 bits to do encryption/decryption and digital signature/verfication. Bidders can choose one out of 1000 predefined bids in the auction, and get 128 bits of order-preserving-encrypted value through oblivious transfer with the agent. The running environment is *Intel(R) Core(TM) i7* 2.67GHz and Windows 7.

Fig. 5(a) shows the computation overhead of the agent, the auctioneer, and each bidder, as a function of the number of bidders. We can see that the computation overhead is mainly



(a) Computation overhead.



(b) Communication overhead

Fig. 5. Computation and communication overheads induced by SPRING.

on the agent, because the agent is responsible for oblivious transfer and bidder grouping. The computation overhead of agent is 0.515 seconds for 50 bidder, and 6.520 seconds for 500 bidders. The auctioneer has a lower computation overhead than the agent. The computation overhead of each bidder is very small.

Fig. 5(b) shows the overall communication overhead induced by SPRING. The communication overhead induced is mainly from the oblivious transfer. In the oblivious transfer, the agent needs to transfer 128 bits for each of the 1000 possible bids to every bidder.

Observing the computation and communication overheads shown above, we can conclude that the overheads induced by SPRING is small enough to be applied to wireless devices.

VII. Conclusion and Future Work

In this paper, we have presented the first strategy-proof and privacy preserving auction mechanism for spectrum redistribution, namely SPRING. SPRING is good for both single-channel request and multi-channel request auctions. For both cases, we have theoretically proven the properties of SPRING. We have implemented SPRING and extensively evaluated its performance. Evaluation results have demonstrated that SPRING achieves good efficiency on spectrum redistribution, in terms of channel utilization and satisfaction ratio, while inducing only a small amount of computation and communication overhead.

As for future work, one possible direction is to design a strategy-proof and privacy preserving double spectrum auction, which protects the privacy of both bidders and sellers. Another possible direction is to provide privacy preservation for combinatorial spectrum auctions.

References

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *SIGMOD'04*, June 2004.

[2] M. Al-Ayyoub and H. Gupta, "Truthful spectrum auctions with approximate revenue," in *INFOCOM'11*, Apr. 2011.

[3] F. Brandt and T. Sandholm, "On the existence of unconditionally privacy-preserving auction protocols," *ACM Transactions on Information and System Security*, vol. 11, no. 2, pp. 1–21, May 2008.

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

[5] L. B. Deek, X. Zhou, K. C. Almeroth, and H. Zheng, "To preempt or not: Tackling bid and time-based cheating in online spectrum auctions," in *INFOCOM'11*, Apr. 2011.

[6] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *INFOCOM'12*, Mar. 2012.

[7] C. Dwork, "Differential privacy," in *ICALP'06*, July 2006.

[8] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "TAHES: Truthful double auction for heterogeneous spectrums," in *INFOCOM'12*, Mar. 2012.

[9] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.

[10] L. Gao and X. Wang, "A game approach for multi-channel allocation in multi-hop wireless networks," in *MobiHoc'08*, May 2008.

[11] Q. Huang, Y. Tao, and F. Wu, "SPRING: A strategy-proof and privacy preserving spectrum auction mechanism," available at http://www.cs.sjtu.edu.cn/~fwu/res/Paper/HTW12TR-SPRING.pdf, Tech. Rep., 2012.

[12] M. Jakobsson and A. Juels, "Mix and match: Secure function evaluation via ciphertexts," in *ASIACRYPT'00*, Dec. 2000.

[13] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic Theory*. Oxford Press, 1995.

[14] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *FOCS'07*, Oct. 2007.

[15] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *EC'99*, Oct. 1999.

[16] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. MIT Press, 1994.

[17] K. Peng, C. Boyd, E. Dawson, and K. Viswanathan, "Robust, privacy protecting and publicly verifiable sealed-bid auction," in *ICICS'02*, Dec. 2002.

[18] M. O. Rabin, "How to exchange secrets with oblivious transfer," Aiken Computation Lab, Harvard University, Tech. Rep., 1981.

[19] K. Sako, "An auction protocol which hides bids of losers," in *PKC'00*, Jan. 2000.

[20] Spectrum Bridge, Inc., http://www.spectrumbridge.com.

[21] X. Sui and C. Boutilier, "Efficiency and privacy tradeoffs in mechanism design," in *AAAI'11*, Aug. 2011.

[22] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge based Systems*, vol. 10, no. 5, pp. 557–570, Oct. 2002.

[23] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," *IEEE Transactions on Computers*, vol. 53, no. 2, pp. 232–240, Feb. 2004.

[24] H. Varian, "Economic mechanism design for computerized agents," in *USENIX Workshop on Electronic Commerce*, 1995.

[25] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H.-H. Chen, "Spectrum sharing in cognitive radio networks – an auction-based approach," *IEEE Transactions on System, Man and Cybernetics–Part B: Cybernetics*, vol. 40, no. 3, pp. 587–596, June 2010.

[26] D. B. West, *Introduction to Graph Theory, Second edition*. Prentice Hall, 1996.

[27] F. Wu and N. Vaidya, "SMALL: A strategy-proof mechanism for radio spectrum allocation," in *INFOCOM'11*, Apr. 2011.

[28] P. Xu, X.-Y. Li, S. Tang, and J. Zhao, "Efficient and strategyproof spectrum allocations in multichannel wireless networks," *IEEE Transactions on Computers*, vol. 60, no. 4, pp. 580–593, Apr. 2011.

[29] P. Xu, X. Xu, S. Tang, and X.-Y. Li, "Truthful online spectrum allocation and auction in multi-channel wireless networks," in *INFOCOM'11*, Apr. 2011.

[30] Q. Yu, J. Chen, Y. Fan, X. Shen, and Y. Sun, "Multi-channel assignment in wireless sensor networks: A game theoretic approach," in *INFOCOM'10*, Mar. 2010.

[31] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "ebay in the sky: Strategy-proof wireless spectrum auctions," in *MobiCom'08*, Sep. 2008.

[32] X. Zhou and H. Zheng, "TRUST: A general framework for truthful double spectrum auctions," in *INFOCOM'09*, Apr. 2009.