# Towards Privacy Preservation in Strategy-Proof Spectrum Auction Mechanisms for Noncooperative Wireless Networks

Fan Wu, *Member, IEEE, ACM*, Qianyi Huang, *Student Member, ACM*, Yixin Tao, and Guihai Chen, *Member, IEEE*

***Abstract*—The problem of dynamic spectrum redistribution has been extensively studied in recent years. Auctions are believed to be among 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 PRIDE, which is a PRIvacy-preserving anD stratEgy-proof spectrum auction mechanism. PRIDE guarantees $k$-anonymity for both single- and multiple-channel auctions. Furthermore, we enhance PRIDE to provide $\ell$-diversity, which is an even stronger privacy protection than $k$-anonymity. We not only rigorously prove the economic and privacy-preserving properties of PRIDE, but also extensively evaluate its performance. Our evaluation results show that PRIDE achieves good spectrum redistribution efficiency and fairness with low overhead.**

***Index Terms*—Privacy, radio spectrum management.**

## 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 efficiency 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. To tackle this artificial spectrum deficit by static spectrum allocation, secondary spectrum markets have emerged.

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], [27], [29]–[31], [36], and [37]) have been proposed. As specified on its official Web site [7], it is the FCC's mission to provide high-quality communication services to all wireless users. Thus, social welfare is put before revenue in spectrum auctions. In a strategy-proof auction (defined in Section III), bidders can maximize their utility by reporting their true valuations to the auctioneer. Thus, it eliminates bidders' strategic behavior, and the auctioneer can allocate the spectrum to bidders who value it most. 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 [18]. 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.

In an ideally privacy-preserving auction (e.g., [18]), 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 the spatial reusability of spectrum. Existing works on privacy-preserving auctions are designed for conventional commodities. They cannot fully exploit the spatial reusability of spectrum. Second, strategy-proofness and bid privacy are somewhat contradictory objectives. Strategy-proofness encourages bidders to reveal their true valuations of the spectrum, whereas bid privacy tends to prevent the auctioneer and other participants from learning the bidders' true valuations.

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 PRIDE, which is a PRIvacy-preserving anD stratEgy-proof spectrum auction mechanism. As shown in Fig. 1, we introduce an agent in PRIDE, who can interact with both the auctioneer and the bidders. We design a simple but effective order-preserving encryption scheme to enable the auctioneer to compare bids without knowledge of their exact values. Bidders interact with the agent via oblivious transfer to receive their order-preserving encrypted bids without revealing their original bids to the agent. As long as the agent and the auctioneer do not collude,

Manuscript received April 30, 2013; revised December 01, 2013 and February 19, 2014; accepted April 23, 2014; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor A. Capone. Date of publication May 29, 2014; date of current version August 14, 2015. This work was supported in part by the State Key Development Program for Basic Research of China under 973 Project 2014CB340303 and 2012CB316201, the China NSF under Grants 61272443 and 61133006, the Shanghai Science and Technology Fund under Grants 12PJ1404900 and 12ZR1414900, and the Program for Changjiang Scholars and Innovative Research Team in University (IRT1158, PCSIRT), China.

F. Wu, Y. Tao, and G. Chen are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: fwu@cs.sjtu.edu.cn; gchen@cs.sjtu.edu.cn; tomtao26@sjtu.edu.cn).

Q. Huang is with the Hong Kong University of Science and Technology, Hong Kong (e-mail: qianyi.huang@ust.hk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TNET.2014.2322104

1063-6692 © 2014 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

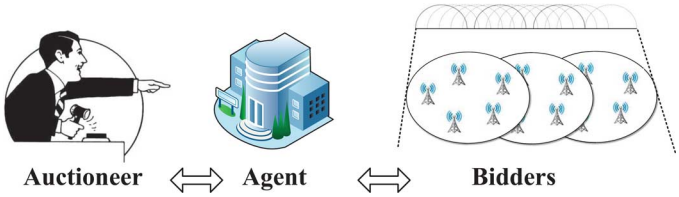



Fig. 1. Auction framework of PRIDE.

PRIDE can guarantee both strategy-proofness and privacy preservation.

We summarize our contributions in this paper as follows.

- To the best of our knowledge, PRIDE is the first strategy-proof and privacy-preserving auction mechanism for spectrum redistribution.
- We propose a novel and practical technique, called PRIDE, to guarantee $k$-anonymous privacy preservation in a generic strategy-proof spectrum auction mechanism (e.g., [29] and [37]). In Section V, we extend PRIDE to adapt to multichannel bids, and it still achieves both strategy-proofness and $k$-anonymity. We further enhance PRIDE to provide a stronger privacy protection. In Section VI, we present enhanced PRIDE, which guarantees $\ell$-diversity.
- We implement PRIDE and extensively evaluate its performance. Our evaluation results show that both PRIDE and enhanced PRIDE achieve good efficiency and fairness 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 PRIDE for the single-channel request case. In Section V, we extend PRIDE to support multichannel bids. We present enhanced PRIDE in Section VI, which provides stronger privacy protection. In Section VII, we show the evaluation results of PRIDE. Finally, we conclude our work and point out potential directions for future work in Section VIII.

## 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, [29], [36], and [37] are early works on auction-based spectrum allocation mechanisms, achieving both strategy-proofness and economic-robustness. 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. Deek *et al.* proposed *Topaz* [5] to guard against time-based cheating in online spectrum auctions. *Topaz* models the spectrum allocation as a 3-D-bin problem (time, space, and frequency) and applies critical charging to guarantee truthfulness. Reference [31] is another piece of work on online spectrum auctions, which achieves efficiency, truthfulness, and asymptotically optimum competitive ratios. Al-Ayyoub and Gupta [2] designed a polynomial-time truthful spectrum auction mechanism with a performance guarantee on revenue. Xu *et al.* [30] considered spectrum allocation under many scenarios (e.g., the bidders are single-minded or not). They designed approximation algorithms to maximize social efficiency and strategy-proof mechanisms to charge the bidders. Yu *et al.* [34] exploited network topology and routing information to allocate channels in wireless sensor networks. They proved that the problem is NP-hard and further proposed a distributed game-based algorithm, which can converge to an NE in finite iterations and is suboptimal. TAHES [8] is a truthful double auction mechanism for heterogeneous spectrum. It considers a more realistic scenario, where different channels have different characteristics. Buyers may access different sets of channels due to their different locations, and different channels have different interference ranges. Dong *et al.* [6] tackled the spectrum allocation problem in cognitive radio networks via combinatorial auction. They allow bidders to request for any combination of time-slots and frequency slots. Hoefer *et al.* [12] put forward the first approximation algorithm for combinatorial auctions with conflict graph. They mainly focused on edge-weighted graphs, which is compatible with a large number of interference models. Hoefer and Kesselheim [11] further studied bidders with symmetric or submodular valuations, which are natural interpretations in secondary spectrum auctions. However, none of the existing spectrum auction mechanisms provides any guarantee on privacy preservation. Recently, Huang *et al.* [13] proposed SPRING, which is the first privacy-preserving and strategy-proof spectrum auction mechanism in noncooperative wireless networks.

According to [3], existing works on privacy-preserving auctions mainly fall into the following three categories:

1) An additional third party (e.g., [18]) cooperates with the auction authority to run the auctions. The auction authority and the third party are responsible for complementary work, however neither of them can learn private information without collusion. Our design belongs to this category.
2) Multiple symmetric auction servers (e.g., [21]) jointly determine the auction outcome. Computation is performed in a distributed manner. Generally, we assume a fraction (e.g., two-thirds or half) of the auction servers are trustworthy.
3) Bidder-resolved protocols (e.g., [3]) do not rely on any auction authority or third parties. Bidders themselves jointly determine the auction outcome.

Unfortunately, existing works on privacy-preserving auctions are designed for traditional commodities, which can be allocated to only one bidder. When applied to spectrum auctions, these existing solutions cannot exploit the spatial reusability of the spectrum. Thus, they can lead to significant degradation of spectrum utilization. Assuming that we directly apply privacy-preserving $(M+1)$st-price auction in spectrum auctions, each channel can be allocated to only one bidder, resulting in extremely low channel utilizations. 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 scheme for

spectrum allocation. Finally, we introduce several useful tools from cryptography.

### A. Solution Concepts

We review the solution concepts used in this paper. Intuitively, mechanisms are a set of rules designed to achieve a specific outcome. Let $s_i$ denote player $i$'s strategy and $s_{-i}$ denote the strategy profile of all the players except player $i$. Let $u_i(s_i, s_{-i})$ be the utility of player $i$ when the strategy of player $i$ is $s_i$, and the strategy profile of the other players is $s_{-i}$. A strong solution concept from mechanism design is *dominant strategy*.

*Definition 1 (Dominant Strategy [9], [19]):* 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 $s_{-i}$, the utility $u_i$ of the player $i$ always satisfies the following condition:

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

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 nonparticipation. We now introduce the definition of *Strategy-Proof Mechanism*.

*Definition 2 (Strategy-Proof Mechanism [17], [26]):* A mechanism is strategy-proof when it satisfies both incentive-compatibility and individual-rationality.

In the field of privacy preservation, $k$-anonymity [23] is a commonly used criteria for evaluating privacy-preserving schemes. A scheme provides $k$-anonymous protection when a person cannot be distinguished from at least $k-1$ other individuals.

*Definition 3 ($k$-Anonymity [23]):* 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 [15], [25], [32].

### 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 small service providers (*bidders*). The auctioneer may be a primary user who tends to lease her idle channel in order to receive proper payoff during her idle time. The auctioneer may also be a specialized third-party platform for spectrum management, such as Spectrum Bridge [22]. There are a number of orthogonal and homogenous spectrum channels that can be leased out to a set of bidders, such as WiFi access points, who want to temporarily lease channels to serve their customers in particular geographic regions. In contrast to existing works (e.g., [29], [36], and [37]), we have an additional authority, called agent, who can communicate with both the auctioneer and the bidders. The agent is a nonprofit party, and we require that the agent should be a well-established organization. Therefore, the government or some trustworthy nonprofit organizations are suitable to play the role of the agent. 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, a channel can be leased to several bidders if they can transmit and receive signals simultaneously with an adequate signal-to-interference-plus-noise ratio (SINR).

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 (defined in Section VII) while guaranteeing strategy-proofness and privacy preservation.

### C. Generic Strategy-Proof Spectrum Auction

In this section, 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., [29] and [37]). 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, we model the interference of the bidders by a conflict graph. Each bidder is a node, and any pair of bidders in the interference range of each other is connected by an edge in the conflict graph. With the method proposed in [35], we can construct a conservative conflict graph, however with higher link reliability. The interference model in [35] is based on SINR, and thus we can get a conflict graph that satisfies the SINR constraints. Bidders are first divided into

nonconflicting groups by any existing graph coloring algorithm (e.g., [28]) in a bid-independent way

$$\mathbb{G} = \{g_1, g_2, \ldots, g_m\},$$
$$\text{s.t. } g_j \cap g_l = \emptyset, \forall g_j, g_l \in \mathbb{G}, j \neq l \text{ and } \bigcup_{g_j \in \mathbb{G}} g_j = \mathbb{N}.$$

A group bid $\sigma_j$ 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 nonincreasing order with bid-independent tie-breaking

$$G' : \sigma_1 \geq \sigma'_2 \geq \cdots \geq \sigma'_m.$$

Bidders from the top $w = \min(c, m)$ groups are winners. Each winning group is charged with $\sigma'_{w+1}$ (0, if $\sigma'_{w+1}$ 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.

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

Please refer to Appendix A for the proof.

### D. Cryptographic Tools

In this paper, we employ three cryptographic tools, including order-preserving encryption, oblivious transfer, and secure multiparty computation.

*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 of bids and carrying out comparisons directly on the cipher text/value.

*2) Oblivious Transfer:* Oblivious Transfer (OT) [20] describes a paradigm of secret exchange between two parties, a sender and a receiver.

The sender has $z$ secrets, $s_1, s_2, \ldots, s_z$. She will disclose one of the secrets $s_\alpha$ to the receiver at the receiver's choice $\alpha$. After they communicate, the receiver knows only $s_\alpha$, and she has no idea of the other $z-1$ secrets. The sender does not know which secret was accessed. In PRIDE, the agent acts as the sender and bidders are the receivers. Algorithm 1 shows the pseudocode of $OT_z^1$ proposed in [24], 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. PRIDE employs an efficient 1-out-of-$z$ oblivious transfer $(OT_z^1)$ of integers [24].

*3) Secure Multiparty Computation (SMC):* SMC, first proposed by Yao [33], has recently become appropriate for some realistic scenarios. We employ SMC in PRIDE to locate the lowest bid in each group. It enables a number of participants to carry out comparisons while preserving the privacy of their inputs.

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

**Initialization:**
**System parameters:** $(g, h, G_q)$;
**Sender's input:** $s_1, s_2, \ldots, s_z \in G_q$;
**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 $s_\alpha = f/d^r$

## IV. PRIDE

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

### A. Design Rational

PRIDE integrates cryptographic tools with the generic spectrum auction mechanism to achieve both strategy-proofness and privacy preservation. The main idea of PRIDE 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 section.

*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. Thus, 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.

*3) Outcome Verification:* Different from traditional privacy-preserving auctions, it is not easy for bidders to verify the correctness of auction outcome. We adopt the idea of SMC [33] to enable bidders from the same group to find the lowest bid, and thus verify the auction outcome.

### B. Design Details

PRIDE works in four steps shown as follows.

*Step 1: Initialization:* Before running the spectrum auction, PRIDE sets up necessary system parameters. PRIDE defines a set of possible bid values as

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

in which $\beta_1 < \beta_2 < \cdots < \beta_z$, and requires each bidder $i$ to pick her bid $b_i$ from $\beta$.

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

$$\gamma_x = OPES(\beta_x),\ s.t.,\ \gamma_1 < \gamma_2 < \cdots < \gamma_z.$$

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 $G_q$: $(g, h)$.

PRIDE employs an asymmetric key encryption scheme. We suppose that the auctioneer holds a private key $Key_{\text{priv}}$, and the matching public key $Key_{\text{pub}}$ is distributed to the bidders. PRIDE 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 $\beta_x$.

- 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

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

- 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 encrypts $\hat{b}_i$ using the auctioneer's public key $Key_{\text{pub}}$

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

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

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

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 $k + 1$ bidders. In the table, bidder $j_i$ is the $i$th 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 $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$

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

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 $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$

$$\hat{b}_l^{\min} = \min\left\{\hat{b}_{l,i} | 1 \le i \le |g_l|\right\}.$$

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 nonincreasing order

$$\sigma'_1 \ge \sigma'_2 \ge \cdots \ge \sigma'_m.$$

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 the $j$th highest group bid. In order to achieve strategy-proofness, each winning bidder group is charged with the group bid $\sigma'_{w+1}$ 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

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

Besides the set of winners $\mathbb{W}$ and their charges $(p_i)_{i \in \mathbb{W}}$, the auctioneer also announces $\sigma'_{w+1}$ for public verification.

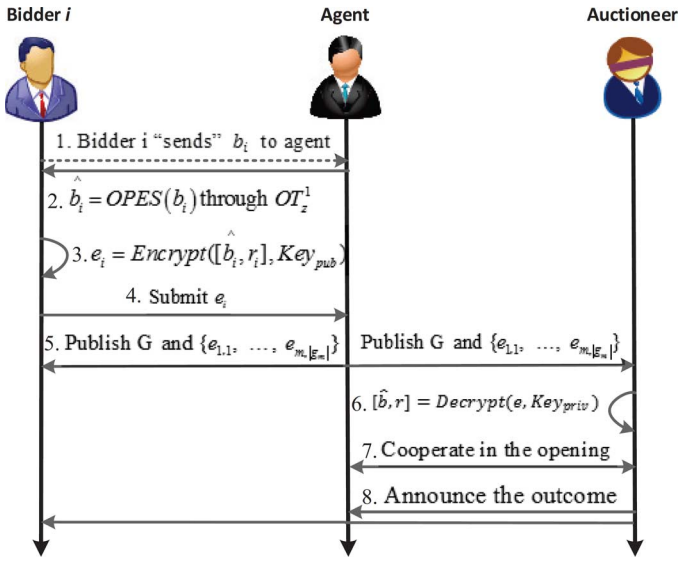



Fig. 2. Message flow. 1 and 2 represent oblivious transfer. The dotted arrow in 1 means that in fact the bidder does not send her bid to the agent directly. 1–5 belong to the step of bidding, and 6–8 belong to the step of opening.

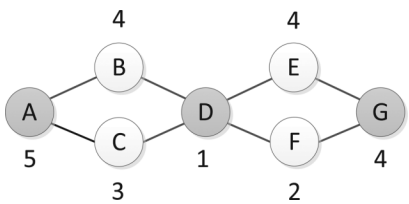



Fig. 3. Conflict graph.

*Step 4: Verification:* This is an optional step. Any bidder group $g_l$, in which bidders doubt the outcome of the auction, can figure out the lowest bid $b_l^{\min} = \min\{b_i | i \in g_l\}$ in the group by SMC [33] without disclosing their own inputs. Then, the relation between $b_l^{\min} \cdot |g_l|$ and $\sigma'_{w+1}$ can be verified.

Fig. 2 shows the message flow in PRIDE.

### C. Illustrative Example

The following example may help to illustrate our mechanism. Fig. 3 shows the interference range of seven bidders ($A$—$G$). They are competing for one channel. Assume that $\beta = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and the number beside each bidder denotes her bid. For clarity and simplicity, we ignore the procedures of digital signature/verification.

In the initialization step, the agent applies $OPES$ on $\beta$ to get $\gamma = \{3, 7, 10, 11, 15, 20, 23, 35, 90\}$. The seven bidders interact with the agent through a 1-out-of-9 oblivious transfer to receive their order-preserving-encrypted bids (i.e., $\hat{b}_A = 15, \hat{b}_B = 11, \hat{b}_C = 10, \hat{b}_D = 3, \hat{b}_E = 11, \hat{b}_F = 7, \hat{b}_G = 11$). Each bidder $i$ encrypts her $\hat{b}_i$ with the auctioneer's public key $Key_{\text{pub}}$ and submits 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.

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 $b_1^{\min} = 1$, $b_2^{\min} = 2$

TABLE II
INFORMATION PUBLISHED BY THE AGENT

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

$$\sigma_1 = 3 \times 1 = 3$$
$$\sigma_2 = 4 \times 2 = 8$$

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 PRIDE.

The strategy-proofness of PRIDE 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:* PRIDE is a strategy-proof spectrum auction mechanism.

Next, we focus on the $k$-anonymity of PRIDE.

*Theorem 3:* PRIDE guarantees $k$-anonymity.

*Proof:* In PRIDE, there are two central authorities, the auctioneer and the agent. The auctioneer knows the lowest bid in each group, but does not know to which bidder it belongs. 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 $k + 1$ bidders.

We distinguish the following two cases.

- *Case 1*: Bidder $i$ belongs to a bidder group $g_l$ that is satisfied with the outcome of the auction.
  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 $\gamma_x$ 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. So, the agent can not identify the bidder of the lowest bid in group $g_l$ from at least $k + 1$ 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 $k + 1$ members in the group.
  Thus, neither the agent, nor the auctioneer, can identify any bidder's bid with probability higher than $1/(k + 1)$.
- *Case 2*: Bidder $i$ belongs to a bidder group $g_l$, which wants to verify the auction outcome. This case only diverges from the previous one in the public verification step. Therefore, we focus on the verification step here.

Since secure multiparty computation is applied to find the lowest $b_l^{\min}$ in group $g_l$, any group member cannot identify the owner of $b_l^{\min}$ from the rest of the $k$ bidders.

Therefore, we can conclude that PRIDE guarantees $k$-anonymity.

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

- *Public verifiability*: It enables bidder groups to verify the outcome of the auction in public verification step.
- *Nonrepudiation*: No bidder can deny her bid after the auction since her signature is required to be verified when the bidder submits her bid to the agent.
- *Low communication overhead*: The communication overhead induced by PRIDE is $\mathrm{O}(z \times n)$, mainly due to oblivious transfer.
- *Low computation overhead*: The cryptographic tools adopted by PRIDE are light-weighted schemes, which only induce a small amount of computation overhead. Our evaluation results show that the computation overhead of PRIDE is rather low.

## V. Extension to Multichannel Bids

In Section V, we propose a strategy-proof and privacy-preserving auction mechanism, in which each bidder bids for a single channel. In this section, we extend PRIDE 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 $b_i$, but also the number of channels demanded $d_i$. We also assume that the bidders do not cheat the demands for two reasons. On one hand, the auction only allocates the channels to the bidders up to their demands. A bidder's demand definitely cannot be contented if she lowers the demand. On the other hand, overdemanding may result in winning more than enough channels. Although the bidder has no valuation on the extra channels, she still needs to pay for them.

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

### A. Virtual Group

In the extended PRIDE, 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 $g_l$

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

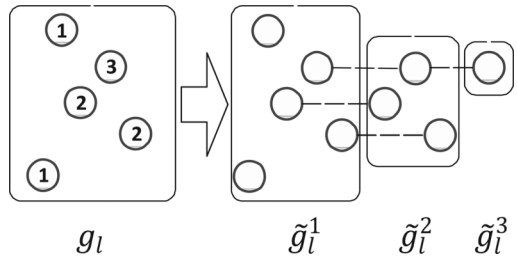



Fig. 4. Toy example.

**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: $G_l \leftarrow \emptyset$; $\hat{d}_l \leftarrow 0$;
2: **for all** $i \in g_l$ **do**
3: $\quad \hat{d}_l \leftarrow \max(\hat{d}_l, d_i)$;
4: **end for**
5: **for** $j \leftarrow 1, \ldots, \hat{d}_l$ **do**
6: $\quad \tilde{g}_l^j \leftarrow \{i | i \in g_l \wedge d_i \geq j\}$;
7: $\quad G_l \leftarrow G_l \cup \{\tilde{g}_l^j\}$;
8: **end for**
**Return** $G_l$;

Algorithm 2 shows the pseudocode 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). Fig. 4 shows our idea of virtual group generation. Each number in a circle denotes the demand of a bidder.

In the extended PRIDE, 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 and verification are the same as those in the basic PRIDE. 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.

*Step 3: Opening:* The auctioneer is informed of the grouping results 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 nonincreasing order

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

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 virtual group with the $j$th highest bid. 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 nonincreasing order (lines 1 and 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 charging profile $\vec{p}$.

*Step 4: Verification:* Please refer to Section IV-B for details.

### C. Analysis

Again, we show that PRIDE satisfies both strategy-proofness and $k$-anonymity, in the case of multichannel bids.

*Theorem 4:* PRIDE is a strategy-proof spectrum auction mechanism, despite multichannel bids.

Please refer to Appendix B for the proof.

Since PRIDE does not reveal any more information to any party, in the case of multichannel bids, we have the following theorem.

*Theorem 5:* PRIDE guarantees $k$-anonymity in the case of multichannel bids.

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 | $[2_1, d_{2_1}], \ldots, [2_{\lvert g_2\rvert}, d_{\lvert g_2\rvert}]$ | $e_{2,1}, \ldots, e_{2,\lvert g_2\rvert}$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $m$ | $[m_1, d_{m_1}], \ldots, [m_{\lvert g_m\rvert}, d_{\lvert g_m\rvert}]$ | $e_{m,1}, \ldots, e_{m,\lvert g_m\rvert}$ |

**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 nonincreasing order $\sigma_1^{\triangle} \geq \sigma_2^{\triangle} \geq \cdots \geq \sigma^{\triangle}_{\sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k}$;
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** $p_i$;

Besides strategy-proofness and $k$-anonymity, PRIDE for multichannel bids also has good properties, including public verifiability, nonrepudiation, and low communication and computation overhead. Due to limitations of space, we do not illustrate the details again.

## VI. PRIDE WITH $\ell$-DIVERSITY

In Sections IV and V, we require that each valid bidder group must contain at least $k+1$ bidders. Hence, we guarantee $k$-anonymity for PRIDE. However, as pointed out in [16], $k$-anonymity is vulnerable to the homogeneity attack and the background knowledge attack. Unfortunately, PRIDE also suffers from these attacks. We consider group $g_j$ in the extreme case, where

$$\hat{b}_j^{\min} = \hat{b}_{j,1} = \hat{b}_{j,2} = \cdots = \hat{b}_{j,|g_j|}$$

which implies that

$$b_j^{\min} = b_{j,1} = b_{j,2} = \cdots = b_{j,|g_j|}.$$

When the auctioneer consults the agent for the original value $b_j^{\min}$ of $\hat{b}_j^{\min}$, the auctioneer also knows the bids of all bidders in $g_j$.

Beyond $k$-anonymity, *$\ell$-diversity* [16] provides more powerful privacy protection. We give the formal definition of $\ell$-diversity principle as follows.

*Principle 1 ($\ell$-Diversity Principle [16]):* A group of indistinguishable tuples are $\ell$-diverse if they contain at least $\ell$ "well-represented" values for the sensitive attributes.

In PRIDE, a bidder group contains a group of indistinguishable bidders and their bids are the sensitive attributes. The authors in [16] provide two concrete instantiations of the $\ell$-diversity principle. In our study, we adopt one instantiation of the $\ell$-diversity principle based on the information-theoretic notion of entropy.

*Definition 4 (Entropy $\ell$-Diversity [16]):* A scheme satisfies entropy $\ell$-diversity if for every group of indistinguishable tuples, we have

$$-\sum_{s\in S} p(s)\log(p(s)) \geq \log(\ell)$$

where $p(s) = \frac{n(s)}{\sum_{s'\in S} n(s')}$ is the fraction of tuples in the group with sensitive attribute value equal to $s$, and $S$ is the domain of the sensitive attribute.

Besides the above drawbacks of $k$-anonymity, we recall the illustrative example in Section IV-C. The auctioneer can infer extra sensitive information by comparing mapped bids from different groups. The auctioneer can infer that the lowest bidder in group $g_1$ is also the lowest bidder among all bidders. She can also infer that the highest bidder is also in $g_1$.

To prevent privacy divulgence in the above situations, we propose enhanced PRIDE in this section. Next, we show our design rational of enhanced PRIDE, which is free from the weaknesses mentioned above.

### A. Design Rational

In order to provide diversity in bids, we can introduce some random factors in the bidding procedure. We can allow a bidder to randomly choose her mapped bid from a continuous integer interval. Consequently, even if all bidders from a bidder group have the same bid, they may choose different mapped bids. It is equivalent to random tie-breaking, providing diversity in mapped bids.

Furthermore, the auctioneer only needs to compare bids within a bidder group and does not need to compare bids from different bidder groups. Hence, the agent can carry out different order-preserving encryptions for different groups in the bidding procedure, such that the auctioneer cannot infer any extra sensitive information.

### B. Design Details

The procedures of winner determination and charging are the same as those in Section IV (single channel auction) and Section V (multichannel bids). Due to limitations of space, we focus on the differences in the step of initialization, bidding, and opening.

*Step 1: Initialization:* For each $g_j \in \mathbb{G}$, the agent maps each $\beta_x \in \beta$ to a contiguous integer interval

$$\theta_{x,j} = \left\{\gamma^L_{x,j}, \gamma^L_{x,j}+1, \ldots, \gamma^H_{x,j}\right\}$$
$$\text{s.t. } \gamma^L_{1,j} < \gamma^H_{1,j} < \gamma^L_{2,j} < \gamma^H_{2,j} < \cdots < \gamma^L_{z,j} < \gamma^H_{z,j}.$$

Here, $\gamma_j = \left\{\gamma^L_{1,j}, \gamma^H_{1,j}, \gamma^L_{2,j}, \gamma^H_{2,j}, \ldots, \gamma^L_{z,j}, \gamma^H_{z,j}\right\}$ is a set of secrets of the agent. For different groups $g_j, g'_j \in \mathbb{G}$, $\gamma_j, \gamma'_j$ can be different. Hence, the auctioneer cannot infer extra sensitive information by comparing mapped bids from different groups.

Furthermore, we require that the interval $\theta_{x,j}$ must contain more than $\ell$ elements for any $1 \leq x \leq z$ and $g_j \in \mathbb{G}$.

*Step 2: Bidding:* Each bidder $i \in g_j$ chooses a bid $b_i = \beta_x \in \beta$ according to her per channel valuation $v_i$, and then interacts with the agent through oblivious transfer to receive the lower and upper limits of the corresponding interval $\theta_{x,j}$.

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

$$c_k = \left(g^{r_k}, \gamma^L_{k,j}\left(y/h^k\right)^{r_k}, \gamma^H_{k,j}\left(y/h^k\right)^{r_k}\right)$$

  where $r_k \in_R Z_q, 1 \leq k \leq z$.
- The bidder picks $c_x = (d, f, u)$ from $c$ and computes

$$\frac{f}{d^r} = \frac{\gamma^L_{x,j}\left(y/h^x\right)^{r_x}}{\left(g^{r_x}\right)^r} = \frac{\gamma^L_{x,j}\left(g^r h^x/h^x\right)^{r_x}}{\left(g^{r_x}\right)^r} = \gamma^L_{x,j}$$
$$\frac{u}{d^r} = \frac{\gamma^H_{x,j}\left(y/h^x\right)^{r_x}}{\left(g^{r_x}\right)^r} = \frac{\gamma^H_{x,j}\left(g^r h^x/h^x\right)^{r_x}}{\left(g^{r_x}\right)^r} = \gamma^H_{x,j}.$$

- Bidder $i$ randomly picks $\hat{b}_i \in \theta_{x,j}$ as her mapped bid.

*Step 3: Opening:* The auctioneer can locate the smallest mapped bid $\hat{b}^{\min}_j$ in group $g_j$ from $\left\{\hat{b}_{j,1}, \hat{b}_{j,2}, \ldots, \hat{b}_{j,|g_j|}\right\}$. Then, the auctioneer resorts to the agent to fetch the original value $b^{\min}_j$ of $\hat{b}^{\min}_j$

$$b^{\min}_j = \left\{\beta_k | \gamma^L_{k,j} \leq \hat{b}^{\min}_j \leq \gamma^H_{k,j}\right\}.$$

The auctioneer can calculate group bids, determine the winners and their charges according to Section IV-B or V-B, respectively.

*Step 4: Verification:* Please refer to Section IV-B for details.

### C. Analysis

From Theorems 2 and 4, we can directly conclude that enhanced PRIDE also guarantees strategy-proofness. Next, we focus on the $\ell$-diversity of enhanced PRIDE. Recall that we require the interval $\theta_{x,j}$ must contain more than $\ell$ elements for any $1 \leq x \leq z$ and any $g_j \in \mathbb{G}$. We have the following theorem.

*Theorem 6:* Enhanced PRIDE satisfies entropy $\ell$-diversity.

Please refer to Appendix C for the proof.

In enhanced PRIDE, the agent has to send the lower and upper limits of mapped bid intervals to the bidders via oblivious transfer, whereas the agent in Sections IV and V only needs to send the mapped bids to the bidders. Hence, enhanced PRIDE induces a bit more computation and communication overheads. Detailed evaluation results are shown in Section VII.

## VII. Evaluation

We have implemented PRIDE and evaluated its performance in terms of efficiency, fairness, and overheads introduced. In this section, we present our evaluation results. Since PRIDE and enhanced PRIDE employ the same procedure for resource allocation, we only show the performance of PRIDE when considering efficiency and fairness.

### A. Efficiency

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

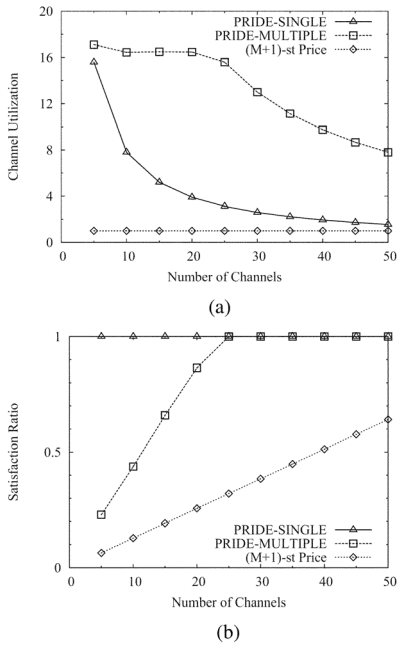



Fig. 5. Efficiency of PRIDE on a practical conflict graph. (a) Channel utilization. (b) Satisfaction ratio.

- *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 utilize the conflict graph collected by Zhou *et al.* [35]. This dataset contains 78 APs of the Google WiFi network, covering a 7-km$^2$ residential area in Mountain View, CA, USA. In the case of multichannel demand, we randomly generate the demand of each bidder from $\{1, 2, 3, 4, 5\}$. We compare PRIDE with the natural generalization of privacy-preserving $(M + 1)$st-price auction to spectrum auctions, where $M$ is set to be the number of channels.

We vary the number of channels in the auction. The results are shown in Fig. 5. With the increasing number of channels, the channels become oversupplied. As a result, the channels cannot be fully utilized, and the channel utilizations are decreasing. In PRIDE-MULTIPLE, bidders can request for more than one channel, thus the resources can be better exploited. Consequently, the channel utilizations of PRIDE-MULTIPLE are higher than PRIDE-SINGLE. Satisfaction ratios of both PRIDE-SINGLE and PRIDE-MULTIPLE are increasing with the number of channels. It is intuitive that more channels can satisfy more bidders' requests.

In this practical conflict graph, there are only 78 APs. In our simulation, in order to validate the efficiency of PRIDE with a larger number of bidders, we generate larger conflict graphs with more bidders. Same as [4], we set interference range to be 1.7 times transmission range. The outdoor transmission range of IEEE 802.11n is about 250 m. Therefore, the interference range is set to 425 m.

We vary the number of bidders from 50 to 500, the number of channels from 5 to 50, and the terrain area from $500 \times 500$ m$^2$ to $2000 \times 2000$ m$^2$. 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 $2000 \times 2000$ m$^2$, respectively. The bidders are randomly distributed in the terrain area.

*1) Results on Channel Utilization:* Fig. 6 shows the evaluation results of PRIDE on channel utilization.

Fig. 6(a) shows the channel utilizations achieved by PRIDE 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 PRIDE-SINGLE is lower than that of PRIDE-MULTIPLE. This is because the channels are oversupplied. 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 to the number of bidders, and the competition among the bidders becomes 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. 6(b) shows the channel utilizations achieved by PRIDE, when varying the number of channels and fixing the other two factors. When the number of channels is no more than 20, PRIDE-MULTIPLE has a lower channel utilization than PRIDE-SINGLE due to the smaller average (virtual) group size. However, with more than 20 channels supplied, PRIDE-MULTIPLE has a higher channel utilization than PRIDE-SINGLE due to higher demands from the bidders.

Fig. 6(c) shows the case in which we vary the size of terrain area and fix the other two factors. When the terrain area is $500 \times 500$ or $1000 \times 1000$ m$^2$, most of the (virtual) groups contain only one or two bidders, thus the difference between PRIDE-SINGLE and PRIDE-MULTIPLE is very small. However, with the increment of terrain area, the difference between PRIDE-SINGLE and PRIDE-MULTIPLE on average size of (virtual) groups becomes larger and larger, resulting in that the channel utilization of PRIDE-MULTIPLE is lower than that of PRIDE-SINGLE.

*2) Results on Satisfaction Ratio:* Fig. 7 shows the evaluation results of PRIDE on satisfaction ratio.

Fig. 7(a) shows the satisfaction ratio achieved by PRIDE, 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, PRIDE-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 PRIDE-SINGLE and PRIDE-MULTIPLE decrease as a result of more interferences. PRIDE-MULTIPLE always achieves a lower satisfaction ratio than PRIDE-SINGLE because PRIDE-MULTIPLE allows bidders to win multiple channels, leading to the fact that more bidders cannot obtain any channel at all.

Fig. 7(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 PRIDE-SINGLE. We also find that the satisfaction ratio of PRIDE-SINGLE with 10 channels is almost equal to that of PRIDE-MULTIPLE with 30 channels. This is because the demands of bidders in PRIDE-MULTIPLE are almost triple of those in PRIDE-SINGLE, given the same number of bidders.

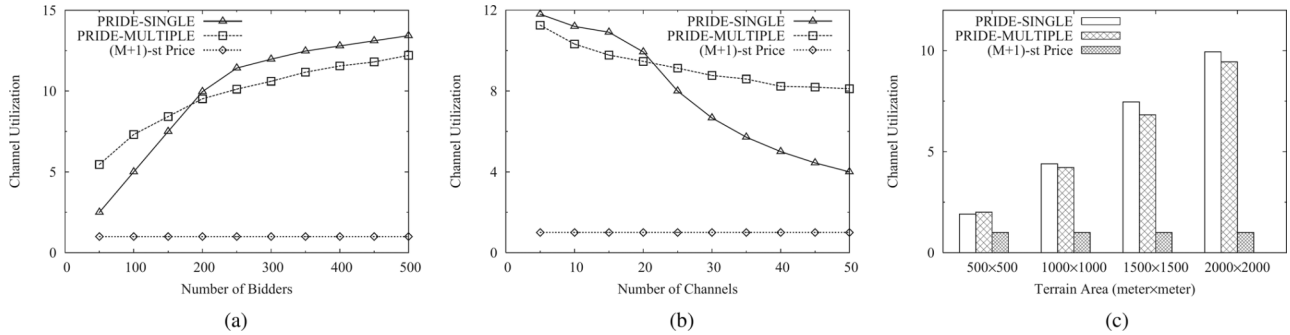



Fig. 6. Channel utilizations of PRIDE when bidders bid for single and multiple channels. (a) Effect of number of bidders. (b) Effect of number of channels. (c) Effect of size of terrain area.

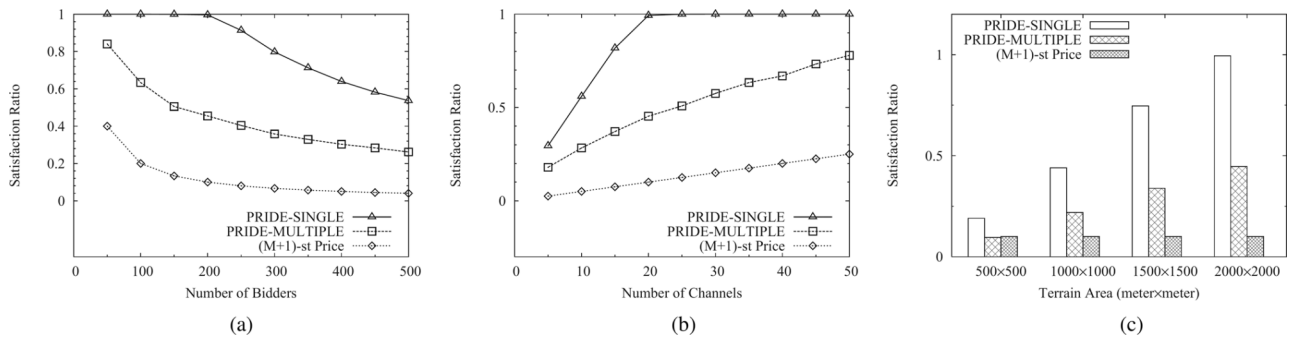



Fig. 7. Satisfaction ratios of PRIDE when bidders bid for single and multiple channels. (a) Effect of number of bidders. (b) Effect of number of channels. (c) Effect of size of terrain area.

Fig. 7(c) shows the case, in which we vary the size of terrain area and fix the other two factors. Again, we can see that PRIDE-SINGLE always has a higher satisfaction ratio than PRIDE-MULTIPLE.

Comparing PRIDE to $(M+1)$st-price auction, evaluation results show that PRIDE achieves better channel utilizations and satisfaction ratios. This is reasonable because PRIDE is designed for spectrum auctions, allocating channels based on bidders' interference conditions, whereas existing $(M+1)$st-price auction just allocates channels exclusively to bidders.

### B. Fairness

Fairness is an important performance criterion in all resource allocation schemes [14]. In this section, we use Jain's fairness index [14] to evaluate the fairness of spectrum allocation by PRIDE.

Under the scenario of spectrum auction, Jain's fairness index is defined as

$$J = \frac{(\sum_{i\in\mathbb{W}} a_i)^2}{|\mathbb{W}| \cdot \sum_{i\in\mathbb{W}} a_i^2}$$

where $\mathbb{W}$ is the set of winners and $a_i$ is the number of channels assigned to bidder $i$. The index ranges from $1/|\mathbb{W}|$ (in the worst case) to 1 (in the best case). We have run both PRIDE-SINGLE and PRIDE-MULTIPLE on the practical conflict graph collected by Zhou *et al.* [35]. The results are shown in Fig. 8.

In the case of PRIDE-SINGLE, $a_i = 1$ for any $i \in \mathbb{W}$. Thus, $J = 1$. In the case of PRIDE-MULTIPLE, when the number of channels is 10, the fairness index is 0.9466. PRIDE-MULTIPLE guarantees fair allocation when the resources are limited. When the number of channels increases, the fairness index decreases a little bit. This is due to unequal demands in PRIDE-MULTIPLE. With the increasing number of channels, bidders with higher demands have the chance to win more channels. However, bidders with lower demands cannot receive channels more than their demands. Thus, the results seem to be a little bit "unfair."

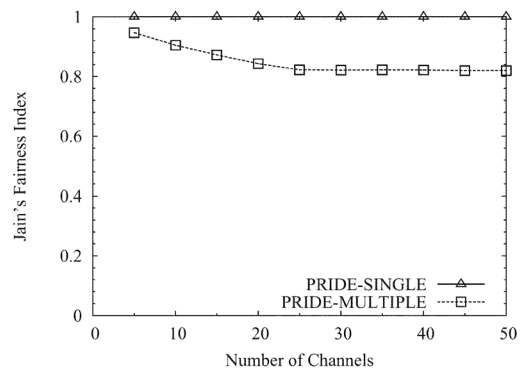



Fig. 8. Jain's fairness index of PRIDE on a practical conflict graph.

Similar to Section VII-A, we also show the Jain's fairness index of PRIDE for the larger conflict graphs with more bidders. The default value for bidder number and channel number are 200 and 20, respectively. The results are shown in Fig. 9. Fig. 9(a) shows that the fairness index increases with the number of bidders, which indicates that PRIDE tends to allocate resources more fairly with more participants. Out of the same reason, Fig. 9(b) shows the similar trend with Fig. 8.

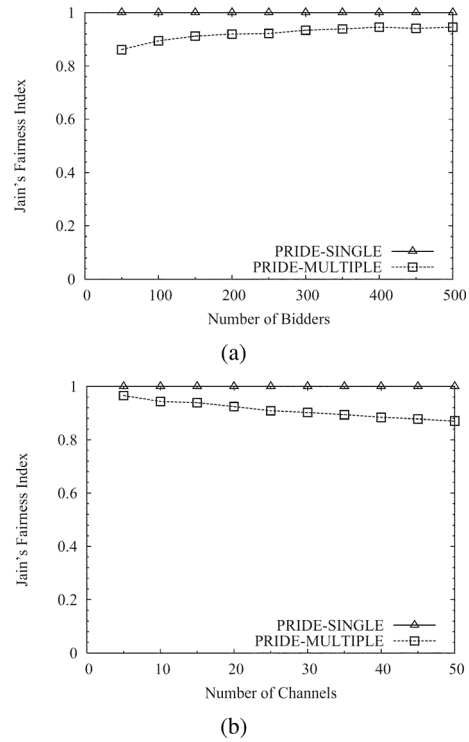



Fig. 9. Jain's fairness index of PRIDE on larger conflict graphs. (a) Effect of number of bidders. (b) Effect of number of channels.

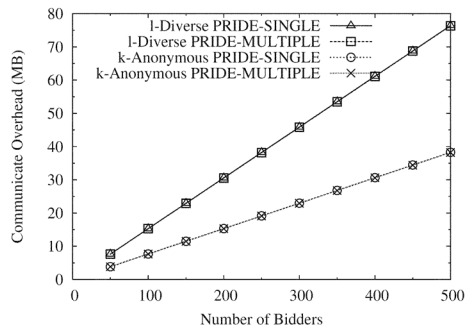



Fig. 10. Communication overheads.

## C. Overhead

PRIDE integrates cryptographic tools to protect bidders' privacy. A practical privacy-preserving scheme should have low overheads, including computation and communication overheads, that can be afforded by wireless devices.

We implement PRIDE 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 predefined bids in the auction and get 128 bits of order-preserving-encrypted value or 128 bits of lower and upper limits of the order-preserving-encrypted interval through oblivious transfer with the agent. The running environment is Intel Core i7 2.67 GHz and Windows 7.

Fig. 10 shows the overall communication overhead induced by $k$-Anonymous PRIDE and $\ell$-Diverse PRIDE. The communication overhead induced is mainly from the oblivious transfer. In the oblivious transfer, the agent needs to transfer 128 bits

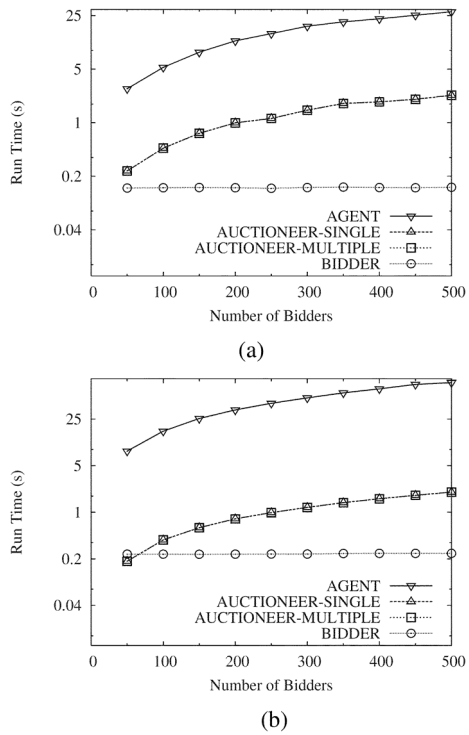
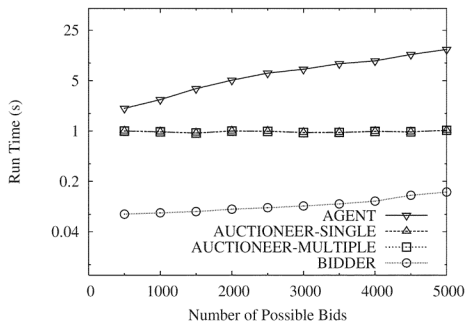



Fig. 11. Computation overheads with growing number of bidders. (a) $k$-Anonymous PRIDE. (b) $\ell$-Diverse PRIDE.

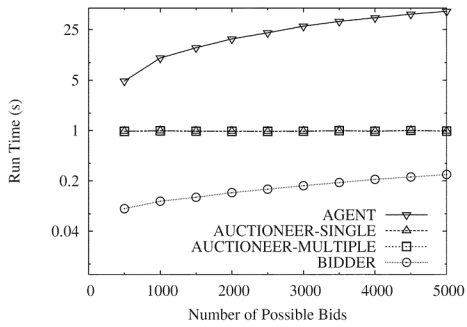
for each of the 5000 possible bids to every bidder. The communication overhead of $\ell$-Diverse PRIDE is roughly twice of $k$-Anonymous PRIDE. In $\ell$-Diverse PRIDE, the agent needs to send lower and upper limits of each mapped interval via oblivious transfer to bidders, whereas in $k$-Anonymous PRIDE, the agent only needs to send the mapped values to bidders.

Fig. 11(a) shows the computation overhead of the agent, the auctioneer, and each bidder as a function of the number of bidders with 5000 predefined bids in $k$-Anonymous PRIDE. We can see that the computation overhead is mainly on the agent because the agent is responsible for oblivious transfer and bidder grouping. The computation overhead of agent is 2.769 s for 50 bidders, and 27.970 s for 500 bidders. The agent can precompute some intermediate results of the oblivious transfer before the bidding phase to save the computation time during bidding. After receiving all bidders' bid, the agent can compute bidder grouping offline. After submitting their bids, bidders are not involved in burdensome computation. Hence, they are not required to stay connected with the agent nor the auctioneer. They can just wait for the auctioneer to broadcast the results. Furthermore, parallel computing is also an approach to speed up computation. The auctioneer has a lower computation overhead than the agent. The computation overhead of each bidder is very small.

Fig. 11(b) shows the computation overhead of the agent, the auctioneer, and each bidder in $\ell$-Diverse PRIDE with 5000 predefined bids. We can see that the computation overhead of $\ell$-Diverse PRIDE is larger compared to $k$-Anonymous PRIDE. It is owning to the fact that the agent carries out different order-preserving encryptions for different groups and the agent needs to send lower and upper limits of each mapped interval to bidders




(a)




(b)

Fig. 12. Computation overheads with growing number of possible bids. (a) $k$-Anonymous PRIDE. (b) $\ell$-Diverse PRIDE.

via oblivious transfer. The auctioneer and bidders still have a low computation overhead.

Fig. 12(a) shows the computation overhead of each party, as a function of the number of predefined bids in $k$-Anonymous PRIDE. Similarly, Fig. 12(b) shows the computation overhead of $\ell$-Diverse PRIDE. We can see that the computation overhead increases with the number of predefined bids since the computation overheads of order-preserving encryptions and oblivious transfer grow linearly with the number of predefined bids.

Observing the computation and communication overheads shown above, we can conclude that the overheads induced by both $k$-Anonymous PRIDE and $\ell$-Diverse PRIDE is small enough to be applied to wireless devices.

## VIII. Conclusion and Future Work

In this paper, we have presented the first strategy-proof and privacy-preserving auction mechanism for spectrum redistribution, namely PRIDE. PRIDE is good for both single-channel request and multichannel request auctions. For both cases, we have theoretically proven the properties of PRIDE. We have implemented PRIDE and extensively evaluated its performance. Evaluation results have demonstrated that PRIDE achieves good efficiency and fairness on spectrum redistribution 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.

## Appendix A
## Proof of Theorem 1

*Proof:* First, we will show each bidder can gain no less utility from truthful participation than nonparticipation. Considering a bidder $i \in g_j$ with valuation $v_i$, her utility is

$$u_i = v_i a_i - p_i$$

where

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

when $g_j$ is a winning group; otherwise, $p_i = 0$.

When bidder $i$ is a winner, i.e., $a_i = 1$,

$$v_i \cdot |g_j| \geq b_j^{\min} \cdot |g_j| = \sigma_j \geq \sigma'_{w+1}$$
$$u_i \geq v_i - \sigma'_{w+1}/|g_j| = v_i \cdot |g_j|/|g_j| - \sigma'_{w+1}/|g_j| \geq 0.$$

When bidder $i$ is a loser

$$u_i = 0.$$

Hence, $u_i \geq 0$ in both cases. It satisfies individual-rationality.

Next, we will show that each bidder cannot increase her utility by bidding a bid other than her true valuation. Since $p_i$ is independent of the bidder's bid $b_i$, the utility function is a function on $a_i$. We distinguish two cases.

- The bidder $i$ is in a winning group, i.e., $a_i = 1$. She cannot increase her utility by proposing a bid other than her true valuation.
- The bidder $i$ is not in a winning group when bidding her true valuation, i.e., $a_i = 0$, $b_i = v_i$ and $\sigma_j \leq \sigma'_{w+1}$. When the bidder $i$ holds the smallest bid in group $g_j$ when bidding truthfully, she can make $g_j$ a winning group by reporting a higher bid $b'_i > b_i$ to increase the $g_j$'s group bid. Her utility (when she cheats) is

  $$u'_i = v_i - p'_i \leq v_i - \sigma'_{w+1}/|g_j| \leq u_i - b_i = 0 = u_i.$$

  The first inequality follows from

  $$p'_i \geq \sigma'_{w+1}/|g_j|.$$

  The second inequality follows from

  $$\sigma_j \leq b_i \cdot |g_j| \leq \sigma'_{w+1}.$$

Hence, truthful bidding is the dominant strategy for all bidders. It satisfies incentive-compatibility.

Therefore, the generic spectrum auction is a strategy-proof mechanism. □

## Appendix B
## Proof of Theorem 4

*Proof:* We consider an arbitrary bidder $i \in g_l$ in the auction. Her utility is

$$u_i = v_i a_i - p_i$$
$$= v_i a_i - \sum_{h=1}^{a_i} p_i^h$$

where

$$p_i^h = \begin{cases} \sigma^{\triangle}_{c-h+1}/|\tilde{g}_l^h|, & \text{if } \sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k \geq c-h+1 \\ 0, & \text{otherwise.} \end{cases}$$

Since $p_i^h$'s are independent of the bidder $i$'s bid $b_i$, the utility is a function on the number of allocated channels $a_i$.

Suppose $a_i$ is the number of channels won by bidder $i$, when she bids truthfully, i.e., $b_i = v_i$. We then distinguish two cases.

- The bidder $i$ wins more channels (i.e., $a_i' > a_i$) by bidding another value $b_i' \neq b_i$. This happens only when the bidder $i$ holds the smallest bid in group $g_l$ when bidding truthfully and wins more channels by raising her bid (i.e., $b_i' > b_i$) to increase the virtual groups' bids. Let $h(a_i < h \leq a_i')$ be the $h$th additional channel won by the bidder $i$. Then, $p_i^h > 0$ because otherwise the bidder would win this channel when bidding truthfully. The utility obtained on this channel is

$$\begin{aligned} u_i^h &= v_i - p_i^h \\ &= v_i - \sigma^{\triangle}_{c-h+1}/|\tilde{g}_l^h| \\ &= v_i - b_l'^{\min}|\tilde{g}_l^h|/|\tilde{g}_l^h| \\ &= v_i - b_l'^{\min} \\ &\leq v_i - b_i \\ &= 0. \end{aligned}$$

  Therefore, getting any more channel does not increase the bidder $i$'s utility.
- The bidder $i$ wins less channels (i.e., $a_i' < a_i$) by bidding another value $b_i' \neq b_i$. Since the charging algorithm guarantees that

$$p_i^h \leq b_i \qquad \forall 1 \leq h \leq a_i$$

  the utility obtained on the $h$th channel is always nonnegative

$$u_i^h = v_i - p_i^h \geq v_i - b_i = 0.$$

  Therefore, losing any channel cannot benefit bidder $i$. Consequently, bidding truthfully is every bidder's dominant strategy, and thus PRIDE satisfies incentive-compatibility.

Furthermore, since any bidder who loses in the auction is free of charge, and also since any winner is charged on each channel with price not exceeding her bid, PRIDE also satisfies individual-rationality.

Therefore, we can conclude that PRIDE is a strategy-proof spectrum auction mechanism, despite of multichannel bids. □

## APPENDIX C
## PROOF OF THEOREM 6

*Proof:* The agent carries out different order-preserving encryptions for different groups, hence the auctioneer cannot infer any sensitive information by comparing bids from different groups.

The group bid of $g_j$ is defined as

$$\sigma_j = |g_j| \cdot b_j^{\min}.$$

It only depends on $b_j^{\min}$ and is independent of $\hat{b}_j^{\min}$. Hence, when bidder $i \in g_j$ with bid $b_i = \beta_x$ chooses her mapped bid $\hat{b}_i$, she has no preference over elements in $\theta_{x,j} = \{\gamma_{x,j}^L, \gamma_{x,j}^L + 1, \ldots, \gamma_{x,j}^H\}$. We assume that there are $\ell'$ elements in $\theta_{x,j}$, where $\ell' \geq \ell$. Bidder $i$ picks $\hat{b}_i = \theta_k \in \theta_{x,j}$ $(1 \leq k \leq \ell')$ with probability

$$p(\theta_k) = 1/\ell'.$$

We consider the extreme case where all bidders in $g_j$ have the same bid

$$b_j^{\min} = b_{j,1} = b_{j,2} = \cdots = b_{j,|g_j|} = \beta_x.$$

Then, the entropy of their mapped bids satisfies

$$\begin{aligned} &-\sum_{s=1}^{\ell'} p(\theta_s)\log(p(\theta_s)) \\ &\quad = -\sum_{s=1}^{\ell'} 1/\ell' \cdot \log(1/\ell') \\ &\quad = \log(\ell') \\ &\quad \geq \log(\ell). \end{aligned}$$

Hence, it satisfies entropy $\ell$-diversity in the extreme case, for any $g_j \in \mathbb{G}$.

Therefore, enhanced PRIDE satisfies entropy $\ell$-diversity. □

## ACKNOWLEDGMENT

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.

## REFERENCES

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. SIGMOD*, Jun. 2004, pp. 563–574.
[2] M. Al-Ayyoub and H. Gupta, "Truthful spectrum auctions with approximate revenue," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2813–2821.
[3] F. Brandt and T. Sandholm, "On the existence of unconditionally privacy-preserving auction protocols," *Trans. Inf. Syst. Security*, vol. 11, no. 2, pp. 1–21, May 2008.
[4] M. Cheng, X. Gong, and L. Cai, "Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3770–3779, Jul. 2009.
[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 *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2219–2227.
[6] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2282–2290.
[7] Federal Communications Commission, Washington, DC, USA, "Federal Communications Commission (FCC)," [Online]. Available: http://www.fcc.gov/.
[8] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "TAHES: truthful double auction for heterogeneous spectrums," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 3076–3080.
[9] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA, USA: MIT Press, 1991.
[10] L. Gao and X. Wang, "A game approach for multi-channel allocation in multi-hop wireless networks," in *Proc. MobiHoc*, May 2008, pp. 303–312.
[11] M. Hoefer and T. Kesselheim, "Secondary spectrum auctions for symmetric and submodular bidders," in *Proc. EC*, Jun. 2012, pp. 657–671.
[12] M. Hoefer, T. Kesselheim, and B. Vöcking, "Approximation algorithms for secondary spectrum auctions," in *Proc. SPAA*, Jun. 2011, pp. 177–186.
[13] Q. Huang, Y. Tao, and F. Wu, "SPRING: A strategy-proof and privacy preserving spectrum auction mechanism," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 827–835.

[14] R. K. Jain, D.-M.W. Chiu, and W. R. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," Eastern Research Laboratory, Digital Equipment Corporation, 1984.
[15] Y. Lindell and B. Pinkas, "Privacy preserving data mining," in *Proc. CRYPTO*, Aug. 2000, pp. 36–54.
[16] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: privacy beyond k-anonymity," in *Proc. ICDE*, Apr. 2006, p. 24.
[17] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic Theory*. Oxford, U.K.: Oxford Press, 1995.
[18] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proc. EC*, Oct. 1999, pp. 129–139.
[19] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.
[20] M. O. Rabin, "How to exchange secrets with oblivious transfer," Aiken Computation Lab, Harvard University, Cambridge, MA, USA, Tech. Rep., 1981.
[21] K. Sako, "An auction protocol which hides bids of losers," in *Proc. PKC*, Jan. 2000, pp. 422–432.
[22] Spectrum Bridge, Inc., Lake Mary, FL, USA, "Spectrum Bridge, Inc.," [Online]. Available: http://www.spectrumbridge.com
[23] L. Sweeney, "K-anonymity: a model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.
[24] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," *IEEE Trans. Comput.*, vol. 53, no. 2, pp. 232–240, Feb. 2004.
[25] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in *Proc. SIGKDD*, Jul. 2002, pp. 639–644.
[26] H. Varian, "Economic mechanism design for computerized agents," in *Proc. USENIX Workshop Electron. Commerce*, 1995, vol. 1, p. 2.
[27] 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 Trans. Syst., Man Cybern. B, Cybern.*, vol. 40, no. 3, pp. 587–596, Jun. 2010.
[28] D. B. West, *Introduction to Graph Theory*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 1996.
[29] F. Wu and N. Vaidya, "SMALL: A strategy-proof mechanism for radio spectrum allocation," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 81–85.
[30] P. Xu, X.-Y Li, S. Tang, and J. Zhao, "Efficient and strategyproof spectrum allocations in multichannel wireless networks," *IEEE Trans. Comput.*, vol. 60, no. 4, pp. 580–593, Apr. 2011.
[31] P. Xu, X. Xu, S. Tang, and X.-Y Li, "Truthful online spectrum allocation and auction in multi-channel wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 26–30.
[32] Z. Yang, S. Zhong, and R. N. Wright, "Privacy-preserving classification of customer data without loss of accuracy," in *Proc. SDM*, Apr. 2005, pp. 92–102.
[33] A. C. Yao, "Protocols for secure computations (extended abstract)," in *Proc. FOCS*, 1982, pp. 160–164.
[34] Q. Yu, J. Chen, Y. Fan, X. Shen, and Y. Sun, "Multi-channel assignment in wireless sensor networks: A game theoretic approach," in *Proc. IEEE INFOCOM*, Apr. 2010, pp. 1–9.
[35] X. Zhou *et al.*, "Practical conflict graphs for dynamic spectrum distribution," in *Proc. SIGMETRICS*, Jun. 2013, pp. 5–16.
[36] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "eBay in the sky: strategy-proof wireless spectrum auctions," in *Proc. MobiCom*, Sep. 2008, pp. 2–13.
[37] X. Zhou and H. Zheng, "TRUST: A general framework for truthful double spectrum auctions," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 99–1007.

**Fan Wu** (M'14) received the B.S. degree in computer science from Nanjing University, Nanjing, China, in 2004, and the Ph.D. degree in computer science and engineering from the State University of New York at Buffalo, Buffalo, NY, USA, in 2009.

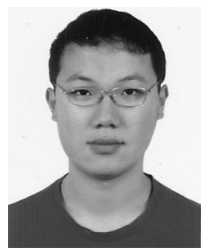
He is an Associate Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. He has visited the University of Illinois at Urbana-Champaign (UIUC), Urbana, IL, USA, as a Post-Doctoral Research Associate. His research interests include wireless networking, economic incentives for cooperation, and peer-to-peer computing.

Dr. Wu is a member of the Association for Computing Machinery (ACM). He received Excellent Young Scholar Award of Shanghai Jiao Tong University in 2011 the and Pujiang Scholar Award in 2012.

**Qianyi Huang** received the B.S. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2013, and is currently pursuing the Ph.D. degree in computer science and engineering at Hong Kong University of Science and Technology, Hong Kong.

Her research interests lie in privacy preservation and resource management in wireless networks.

Miss Huang is a student member of the Association for Computing Machinery (ACM) and CCF.



**Yixin Tao** is a student with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China.

His research interests lie in game theory, mechanism design, and resource management in wireless networking.

**Guihai Chen** (M'13) received the B.S. degree from Nanjing University, Nanjing, China, the M.Engineering degree from Southeast University, Nanjing, China, and the Ph.D. degree from the University of Hong Kong, Hong Kong, all in computer science.

He visited Kyushu Institute of Technology, Fukuoka, Japan, in 1998 as a Research Fellow, and the University of Queensland, Brisbane, Australia, in 2000 as a Visiting Professor. During 2001 to 2003, he was a Visiting Professor with Wayne State University, Detroit, MI, USA. He is a Distinguished Professor and Deputy Chair with the Department of Computer Science, Shanghai Jiao Tong University, Shanghai, China. He has published more than 200 papers in peer-reviewed journals and refereed conference proceedings in the areas of wireless sensor networks, high-performance computer architecture, peer-to-peer computing, and performance evaluation.

Prof. Chen is a member of the IEEE Computer Society. He has also served on technical program committees of numerous international conferences.