Wireless Netw (2012) 18:113–128
DOI 10.1007/s11276-011-0390-3

Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer

Miao Pan · Xiaoyan Zhu · Yuguang Fang

Published online: 8 October 2011

Abstract Spectrum auction is an enabling technology for improving the spectrum efficiency of unused licensed bands (white spaces) in wireless networks. However, the back-room dealing (i.e., the frauds of the untrustworthy auctioneer and the bid-rigging between the greedy bidders and the insincere auctioneer) poses serious security challenges, leading to failures of all existing secure auction designs in allocating spectrum bands. In this paper, we propose a secure combinatorial spectrum auction (*SCSA*) by utilizing homomorphic encryption to prevent the back-room dealing. The idea in *SCSA* is to incorporate cryptographic techniques into the spectrum auction to address the frauds and bid-rigging. It computes and reveals the results of spectrum auction while the actual bidding values of bidders are kept confidential. *SCSA* also provides a corresponding procedure in implementing the combinatorial spectrum auction under the interference constraints. We show that compared with existing secure spectrum auction designs against the untrustworthy auctioneer, *SCSA* is much more efficient in both communication and computational complexity; and compared with other spectrum auction designs with security consideration, *SCSA* can effectively thwart the back-room dealings due to the untrustworthy auctioneer without too much performance degradation.

Keywords Cognitive radio · Secure spectrum auctions · Homomorphic encryption · Untrustworthy auctioneer

M. Pan · Y. Fang
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA
e-mail: miaopan@ufl.edu

X. Zhu · Y. Fang (✉)
National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China
e-mail: fang@ece.ufl.edu; miaopa@ufl.edu

X. Zhu
e-mail: xyzhu@mail.xidian.edu.cn

1 Introduction

In recent years, more and more people, families and companies rely on wireless services for their daily life and business. The accompanied dilemma between the booming growth of wireless services and the scarcity of radio spectrum has shoved the fixed spectrum allocation of Federal Communications Commission (FCC) off the edge, and poured out numerous new techniques, which allow the opportunistic access to the under-utilized spectrum bands [1–4]. Inspired by the mechanisms in microeconomics [5–7], auction seems to be one of the most promising solutions to the problem of vacant spectrum allocation to the potential unlicensed users [8–11].

In general, conventional auctions can be classified into several categories by different criteria [12], i.e., open or sealed auction according to the bidding manner, first price auction, secondary price auction, Vickery auction [13], or Vickrey-Clarke-Groves (VCG) auction (also known as Generalized Vickrey Auction, i.e., GVA) according to the pricing strategy, and single item or combinatorial auction according to the number of auctioned goods [14, 15]. Depending on the requirements, these auction mechanisms can be applied to different scenarios. For instance, the most widely used auctioneer-favored auction, English auction [12], is an open first price auction, in which the bidder with the highest bid wins the auction and pays at the price of his bid. This kind of open auction enables the auctioneer to

maximize his monetary gains, but it is not strategy-proof. In English auction, each bidder has to come up with a delicate strategy to win, which inevitably leads to great complexity and a long auction time. On the contrary, the sealed secondary price auction can ensure the bidders submit their bids with true evaluation values and shorten the auction time. However, it often results in unsatisfactory revenue for the auctioneer. Equivalent to sealed secondary price auction for single item auction, VCG auction has been proved to be incentive compatible, Pareto efficient, and individual rational [12]. Under certain assumptions, VCG auction is the only mechanism that can satisfy all the above three properties while maximizing the expected revenue of the auctioneer [16]. As for the security issues in auction design, there has been considerable work on designing electronic auction with different features, such as fairness [17, 18], confidentiality, anonymity and so on [19].

Despite their attractive features, the aforementioned traditional auctions cannot be hammered into the spectrum auction design directly. Unlike common goods in conventional auctions, spectrum is reusable among bidders under the spatial interference constraints, i.e., bidders geographically far apart can reuse the same frequency simultaneously. Even though interference is only a local effect, the spatial reuse of frequency makes the problem of finding the optimal spectrum allocation NP-complete [20, 21], leading to the failures of almost all conventional auction mechanisms based on optimal allocations [8]. Besides, this unique property of spectrum reuse *butterflies* the effect of the local back-room dealing (i.e., untruthful bidding, collusion among the bidders, frauds of the auctioneer, and bid-rigging between bidders and auctioneer) to the whole network within the coverage of the auctioneer. Therefore, designing a secure spectrum auction is highly challenging but imperative.

Given that truthfully bidding and collusion among the bidders have been well investigated in the existing literature [8, 9, 11, 22], a secure spectrum auction design should also consider the frauds of the untrustworthy auctioneer and the bid-rigging between the bidders and the insincere auctioneer[1]. Specifically, a fraud is a deception made by the insincere auctioneer, who may commit frauds by overcharging the winning bidders with the forged price for his personal monetary gain, which then undermines the spectrum auction system. Bid-rigging is defined as the conspiracy between the insincere auctioneer and greedy

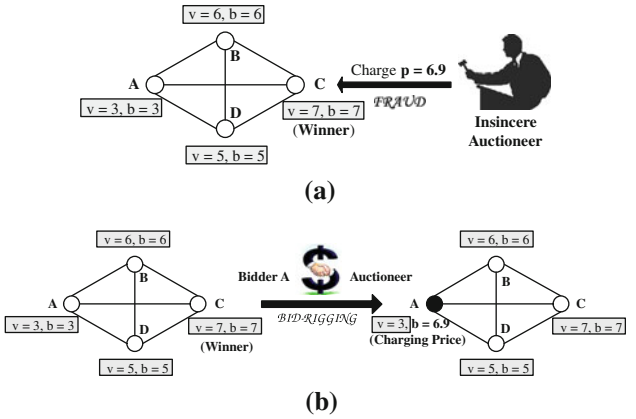


Fig. 1 Challenges to secure spectrum auction design. **a** Frauds of the insincere auctioneer. **b** Bid-rigging between the auctioneer and the bidders

bidders with an aim to illegally fixing the price, sharing the spoils and manipulating the spectrum auction.

Taking the scenario shown in Fig. 1 for example, there is only one spectrum band available for auction and sealed secondary price auction is employed[2]. In Fig. 1(a), the winning bid (i.e., the highest bid) is 7 and the charging price (i.e., the second highest bid) should be 6 for the winner *C*. However, by fabricating a dummy bid close to the highest bid at 6.9, the insincere auctioneer can obtain higher revenue. Since the auction is sealed and no bidders are able to check the bids of others during the auction, the auctioneer may abuse his unsupervised authority by carrying out frauds, which would not be exposed by the bidders unless the winning bidders can verify each bid from their interfering neighbors later after the spectrum auction. In Fig. 1(b), we show an example of bid-rigging between the auctioneer and the bidders. Suppose node *A* is a greedy bidder who can collude with the auctioneer. Since all the bidding values are open to the auctioneer for appropriately sorting the bids and allocating the bands, the auctioneer can conspire with *A* by revealing the winning bid of *C* to *A*. Node *A* may bid far more than his true evaluation value so that the auctioneer is able to charge more from winner *C*, and shares the spoils with *A*. In this way, no flaws can be found by the winners, even if they take the trouble in verifying each bid after the auction.

In this paper, by considering frequency reuse and applying cryptographic techniques, we design a novel secure combinatorial spectrum auction scheme, *SCSA*, to purge the possible frauds and bid-riggings. The contributions of this proposed auction are four-folded:

[1] In this paper, greedy bidders and insincere auctioneer are different from malicious attackers, though all of them may impair the performance of the spectrum auction. Greedy bidders and insincere auctioneer are rational because they do not attempt to attack others on sacrificing their own profits. Malicious attackers always try to degrade the performance of the auction even with huge cost.

[2] VCG is equivalent to the sealed secondary price auction for a single item case.

(1) *SCSA* provides an effective procedure to auction the spectrum bands by considering the interference constraints. To counter the NP-completeness of spectrum allocation in view of the frequency reuse, *SCSA* decomposes the whole network into small subnetworks according to the number of bidders, and auctions the spectrum bands in subnetworks one by one. Meanwhile, each bidder maintains a local conflict-table. A bidder is able to update his conflict-table and broadcast the spectrum occupancy information to his neighbors when detecting changes of the environment.

(2) *SCSA* is able to support combinatorial spectrum auction consisting of bands with diverse characteristics rather than the single-band spectrum auction consisting of bands only with uniform characteristics in previous works [8, 11, 20, 23]. Besides, since *SCSA* employs a variant of *VCG* (V^2CG) auction [14] in the subnetworks, each bidder is no longer required to declare his bidding values for every possible allocation of unoccupied bands as in Pan et al. [23]. In *SCSA*, a bidder only needs to submit his bids for the bunches[3] of spectrum bands which he is interested in.

(3) *SCSA* leverages homomorphic encryption [24–26] to mask the bidding values of each bidder with a vector of ciphertexts, which enables the auctioneer to find the maximum value, randomize the bids and charge the bidders securely. The auctioneer could compute and reveal the results of spectrum auction, while the actual bidding values of bidders are kept secret from the other bidders and even from the auctioneer.

(4) *SCSA* secures the spectrum auction effectively against frauds and bid-riggings without much performance degradation. By simulations and analysis, we show that compared with our previous secure spectrum auction design without assumption that the auctioneer is trustworthy, *THEMIS* [23], *SCSA* is much more efficient in communication and computation complexity while achieving similar performance to the existing auction designs with the assumption that the auctioneer is trustworthy in terms of spectrum utilization, the revenue of the auctioneer and bidders' satisfactory degree as well.

The remainder of the paper is organized as follows. We start with reviewing some of related work in Sect. 2. In Sect. 3, we outline the system model and briefly introduce VCG auction and homomorphic encryption as the preliminaries. Then, we illustrate the multi-hop auction procedure of *SCSA* in Sect. 4, and elaborate on the encryption design of subnetwork auction in Sect. 5. We present the performance analysis in Sect. 6, and finally draw concluding remarks in Sect. 7.

[3] In this paper, "bunch" denotes a subset of goods/spectrum bands in the auction.

2 Related work

To deal with the mutual interference between neighboring bidders, Gandhi et al. [20] has proposed the conflict graph and a general framework for wireless spectrum auctions. Based on these concepts, a truthfully bidding spectrum auction, *VERITAS*, is given by Zhou et al. [8]. The notion of critical neighbor/value is proposed and employed to guarantee the strategy-proof property. However, the bidders in *VERITAS* must be risk-seeking [27]. Otherwise, if the bidders are only greedy, but still rational and risk neutral, bidders will not have incentive to bid arbitrarily high or low with the concern of overpayment or losing in an auction [16]. In the sealed secondary price/VCG auction, if a risk neutral bidder has no information about the bids of the other bidders, the dominant strategy for him is to bid with his true evaluation value [12, 28]. Zhou et al. [8] also provide an efficient allocation algorithm, which assigns bidders with spectrum bands sequentially from the bidder with the highest bid to the one with the lowest bid by considering the complex heterogeneous interference constraints. However, the validity of this algorithm is challenged by a special scenario in Wu et al. [11], which shows that it is not always appropriate to allocate the spectrum bands to the bidder with the highest bid in case that the sum of the neighboring bids is much higher than the highest bid. In addition, the collusion among the bidders is described in Wu et al. [11]. As a possible solution, the nodes with negligible interference can be grouped together as virtual bidders, and hence the multi-winner spectrum auction [11] can be transformed into a traditional single-winner auction and the payment or revenue among the participating bidders can be shared. However, it should be noted that the issue of group partition itself is NP-complete under interference constraints [21].

On the other hand, to thwart untrustworthy auctioneer, homomorphic encryption is widely used in traditional auction designs (e.g., VCG auction) to hide the bidding values, and determine the winner of the auction and calculate the payment of the winning bidder [29–31]. Considering the frequency reuse in allocating spectrum bands, in our previous work [23], we extend the application of homomorphic encryption into the secure spectrum auction design, and propose *THEMIS* to purge the frauds and bid-riggings. But *THEMIS* cannot support combinatorial spectrum auction. In addition, *THEMIS* requires each bidder to submit their bids for every possible allocation of the available spectrum bands, which leaves the room of

efficiency improvement for the future secure spectrum auction designs. This paper is one way to improve the efficiency.

3 System model and preliminaries

3.1 Overview

We consider a typical spectrum auction setting, where the auctioneer auctions the unutilized spectrum bands $\mathcal{S} = \{1, 2, \ldots, s\}$ to $\mathcal{N} = \{1, 2, \ldots, n\}$ nodes/bidders located in the geographic region as shown in Fig. 2. The available $\mathcal{S}$ spectrum bands are supposed to have different characteristics to different nodes (in the subsequent development, we use the nodes and bidders interchangeably) in terms of the frequency, the segment type of the band (i.e., contiguous segment or discontinuous one), and the location of the bidders, etc. [32–34], so that bidders may submit different bids for different combinations of the spectrum bands. Considering the frequency reuse [21, 20], i.e., adjacent nodes must not use the same bands simultaneously while geographically well-separated ones can, we represent the interference relationship among bidders by a conflict graph, which can be constructed from either physical model [35] or protocol model [36] as described in Zhou et al. [8], Zhou and Zheng [9], Wu et al. [11], Gandhi et al. [20]. As shown in Fig. 2, the edges stand for mutual interference between corresponding nodes. Moreover, we assume that spectrum auctions take place periodically[4], the bidders are static in each period, and there is a common channel[5] for necessary information exchange between the auctioneer and bidders.

The other notations and definitions related to the spectrum auction are summarized as follows.

- *A Feasible Allocation*—$\boldsymbol{\lambda} = (\lambda(1), \lambda(2), \ldots, \lambda(n))$ denotes a feasible allocation for a set of spectrum bands $\mathcal{S}$, where $\lambda(i)$ represents the bunch of bands allocated to bidder i with the following conditions: $\bigcup_i \lambda(i) \subseteq \mathcal{S}$, and for all $i \neq j$, $\lambda(i) \cap \lambda(j) = \emptyset$. For instance, for $\mathcal{N} = \{1, 2\}$ and $\mathcal{S} = \{1, 2\}$, $\boldsymbol{\lambda} = (\lambda(1) = \{2\}, \lambda(2) = \{1\})$ is a feasible allocation, i.e., allocating spectrum band 2 to bidder 1 and allocating band 1 to bidder 2.

[4] The auction period should not be too long (e.g., months or years) to make dynamic spectrum allocation infeasible, and it should not be too short (e.g., seconds or minutes) to incur overwhelming overhead in spectrum trading. The typical duration is hours or days as shown in Giupponi et al. [37]. In the rest of paper, we assume that all the spectrum auctions are of fixed duration, so that the time parameter is not included, and we only need to focus on a specific period for the design of secure spectrum auction.

[5] It is like the common control channel (CCC) proposed in [2], or the common pilot channel (CPC) in Perez-Romero et al. [38]

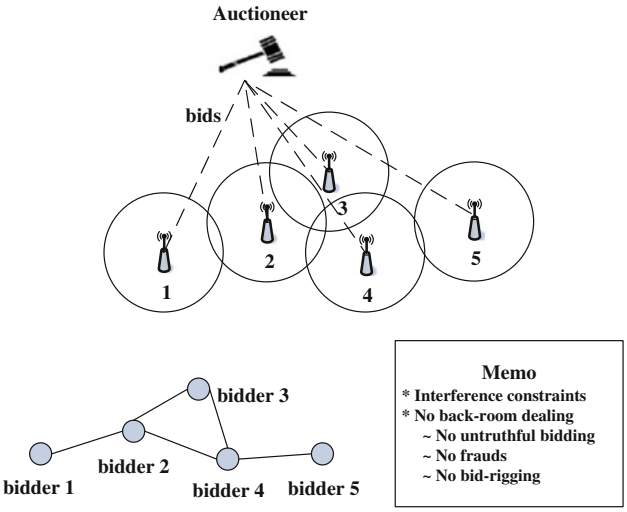


Fig. 2 System architecture, conflict graph, and secure spectrum auction memo

- *Allocation Set*—$\mathcal{N}^{\mathcal{S}} = \{\boldsymbol{\lambda} : \mathcal{S} \to \mathcal{N}\}$ denotes the set of allocations of spectrum bands $\mathcal{S}$ to bidders $\mathcal{N}$.
- *Bidding Values*—$b_i(\lambda(i))$ indicates the bidding values of node i for the bunch of spectrum bands $\lambda(i)$.
- *Evaluation Values*—$v_i(\lambda(i))$ represents the true evaluation values of node i for the bunch of spectrum bands $\lambda(i)$. In case that the auction is incentive compatible, v_i equals to b_i.
- *Charging Price*—p_i is the price charged by the auctioneer for allocating the spectrum bands to winning bidder i.
- *Bidder's Utility*—u_i stands for the utility of bidder i. It is defined as $u_i(\lambda(i)) = v_i(\lambda(i)) - p_i$ for the bunch of spectrum bands $\lambda(i)$.
- *Auctioneer's Revenue*—R denotes the monetary gains of the auctioneer. It is simply expressed as $R = \sum_{i=1}^{n} p_i$.

3.2 VCG auction

As one of the most widely used auction schemes, VCG auction is proved to be individual rational, Pareto efficient, and incentive compatible [13]. In VCG, the dominant strategy for a bidder to win the auction and maximize his utility is to declare his true evaluation values regardless of the bidding actions of the other bidders. VCG auction consists of the following procedures.

Bidding: For a bunch of goods $\lambda(i)$, bidder i submits his sealed bid $b_i(\lambda(i))$ to the auctioneer.

Allocation: The auctioneer selects a Pareto efficient allocation $\boldsymbol{\lambda}^* = (\lambda^*(1), \lambda^*(2), \ldots, \lambda^*(n)) \in \mathcal{N}^{\mathcal{S}}$ based on bidding values, i.e.,

$$\boldsymbol{\lambda}^* = \underset{\boldsymbol{\lambda}\in\mathcal{N}^S}{\operatorname{argmax}} \left(\sum_i b_i(\lambda(i)) \right). \tag{1}$$

Then, the goods are assigned according to $\boldsymbol{\lambda}^*$.

Charging: Assume $\boldsymbol{\lambda}^*_{\sim i} = (\lambda^*_{\sim i}(1), \lambda^*_{\sim i}(2), \ldots, \lambda^*_{\sim i}(n))$ is an allocation without bidder i satisfying the following inequality

$$\sum_{j\neq i} b_j\left(\lambda^*_{\sim i}(j)\right) \geq \sum_{j\neq i} b_j(\lambda(j)). \tag{2}$$

Then, the payment of bidder i is defined as

$$p_i = \sum_{j\neq i} b_j\left(\lambda^*_{\sim i}(j)\right) - \sum_{j\neq i} b_j(\lambda^*(j)). \tag{3}$$

So, the utility of bidder i is $u_i(\lambda^*(i)) = v_i(\lambda^*(i)) - p_i$. It can also be expressed as

$$\begin{aligned} u_i(\lambda^*(i)) &= v_i(\lambda^*(i)) - \left(\sum_{j\neq i} b_j\left(\lambda^*_{\sim i}(j)\right) - \sum_{j\neq i} b_j(\lambda^*(j)) \right) \\ &= \left[v_i(\lambda^*(i)) + \sum_{j\neq i} b_j(\lambda^*(j)) \right] - \sum_{j\neq i} b_j\left(\lambda^*_{\sim i}(j)\right), \end{aligned} \tag{4}$$

where the last term is determined independently of bidder i's bidding values, so that bidder i can maximize his utility by maximizing the two terms within the square bracket. Since

$$\sum_i b_i(\lambda^*(i)) \geq \sum_i b_i(\lambda(i)), \tag{5}$$

to maximize his utility, the dominant strategy of bidder i is to submit $b_i(\cdot) = v_i(\cdot)$, i.e., to bid with his true evaluation values.

3.3 Homomorphic encryption

Homomorphic encryption is such a probabilistic[6] asymmetric public key encryption that satisfies special features such as homomorphic addition/multiplication, indistinguishability and self-blinding [25, 26, 39–41]:

- **Homomorphic addition/multiplication:** Given $\mathscr{E}$ is the homomorphic encryption of a message M, $\mathscr{E}(\cdot)$ is additive homomorphic, i.e., $\mathscr{E}(M_1 + M_2) = \mathscr{E}(M_1)\,\mathscr{E}(M_2)$ (e.g., Paillier cryptosystem [25, 26] and Benaloh cryptosystem [40])/multiplicative homomorphic, i.e., $\mathscr{E}(M_1 M_2) = \mathscr{E}(M_1)\mathscr{E}(M_2)$ (e.g., ElGamal encryption [39]).
- **Indistinguishability:** $\mathscr{E}(\cdot)$ is considered indistinguishable if the same plaintext M is encrypted twice, these two ciphertexts are totally different, and no one can succeed in distinguishing the corresponding original plaintexts with a probability significantly greater than 1/2 (i.e., random guessing) unless he decrypts the ciphertexts.
- **Self-blinding:** Any ciphertext can be publicly changed into another one without affecting the plaintext, which means a different randomized ciphertext $\mathscr{E}'(M)$ can be computed from the ciphertext $\mathscr{E}(M)$ without knowing either the decryption key or the original plaintext.

[6] The term "probabilistic encryption" is typically used in reference to public key encryption algorithms. Probabilistic encryption uses the randomness in an encryption algorithm, so that when encrypting the same plaintext for several times, it will yield different ciphertexts.

4 Multi-hop spectrum auction procedure

In parallel with the encryption design to thwart the untrustworthy auctioneer, *SCSA* provides a supporting conflict-table-driven auction procedure to implement the spectrum auction as well. In this section, we describe the multi-hop spectrum auction procedure. Then, we elaborate the encryption design of the proposed *SCSA* in the next section.

Similar to the table-driven routing algorithms, we allow each bidder to maintain a local conflict-table reflecting the interference constraints. The local conflict-table can be constructed based on the conflict-matrix derived from the conflict graph as demonstrated in Wu et al. [11]. A bidder needs to update his bids if any of his neighboring nodes in the conflict-table wins spectrum bands or the number of available bands for auction with his interference range has changed. Considering spatial reuse, in *SCSA*, the whole network is divided into small subnetworks based on the interference range and the location of the bidders. Subnetwork i consists of all the nodes within the circle area centered at the location of bidder i with the radius of bidder i's interference range. Auction is executed in one subnetwork after another until each node has been the center. Note that the spectrum band allocation and price charged for the winning bidders depend both on the results of the subnetwork auctions and on the location of the winning bidders when taking the interference constraints into account.

The detailed procedure of *SCSA* is presented as follows.

Preparation: Each bidder sets up two tables, a conflict-table for the interfering nodes and a price-charged table for a series of charging prices for the spectrum bands he won. Bidders fill in the conflict-table with current interfering neighbors and initialize the price-charged table with zeros. For any bidder $i \in \mathcal{N}$, he encloses his identity, location information and his own bidding values b_i for the bunches of spectrum bands in which he is interested into his bid.

The identity and location information of bidder i are public to the auctioneer for subnetwork division, allocating spectrum bands and charging prices, but b_i is masked using homomorphic encryption. Then, bidders submit their encrypted bids to the auctioneer.

Start-up: Due to the NP-completeness of spectrum allocation problem, there is no feasible optimal choice for the auctioneer to start the subnetwork spectrum auctions with a designated bidder in order to maximize his revenue. Therefore, the auctioneer can initiate the subnetwork auctions with a randomly chosen bidder, say, node i, where bidder i is regarded as the center of the current subnetwork, and his interference range is set to be the radius of the subnetwork.

Bidder Indexing: The auctioneer sorts the bidders within the subnetwork according to their Euclidean distances from the center i. The closer to the center, the smaller index the bidder is labeled. The auctioneer stores the index information in a distance vector $\mathcal{D}$, whose element d_j denotes the distance between the j-th node from the center i.

Subnetwork Auction: After indexing the bidders, the auctioneer collects the bids and carries out the secure combinatorial spectrum auction within the subnetwork by using homomorphic encryption. The results of the subnetwork auction, i.e., the set of winners and the set of the corresponding charging prices, are published. Details of encryption design for the secure subnetwork spectrum auction are elaborated in Sect. 5.

Allocation & Payment: Determined by both subnetwork auction results and location of the winners, the allocation of spectrum bands and the payment are different in the following three cases:

- *Case 1:* If the current center, bidder i, is not one of the winners, the auctioneer needs to check the elements in the winner set $\mathcal{W}$, choose the winning bidder with the smallest index to be the next center, and set his interference range as the radius of the next subnetwork. According to the results of the current subnetwork auction, all the winning bidders store the spectrum bands they won and the corresponding charging prices into their price-charged tables. After that, the current center, bidder i, is deleted from the conflict-tables of his neighbors. The subnetwork spectrum auction centered at node i ends, and the auction goes to ***Bidder Indexing*** of the next center for the next subnetwork auction.
- *Case 2:* If the center, bidder i, is the only winner of the auction, and he is charged at p_i for the bunch of bands λ, he will compare the current charging price p_i with the previous charging prices stored in his price-charged table and pay the highest one of all the prices for the bunch of spectrum bands[7]. Then, the center node broadcasts his spectrum occupancy information and his neighbors eliminate him from their conflict-tables. After that, the auctioneer sets the node with the smallest index as the next center. The auction goes to ***Bidder Indexing*** for the next subnetwork auction.
- *Case 3:* Provided that there are more winners than the current center i, the process is the same as in *Case 2*, except that the auctioneer would rather take the node with the smallest index in the winning set $\mathcal{W}$ as the next center for the consideration of computational efficiency.

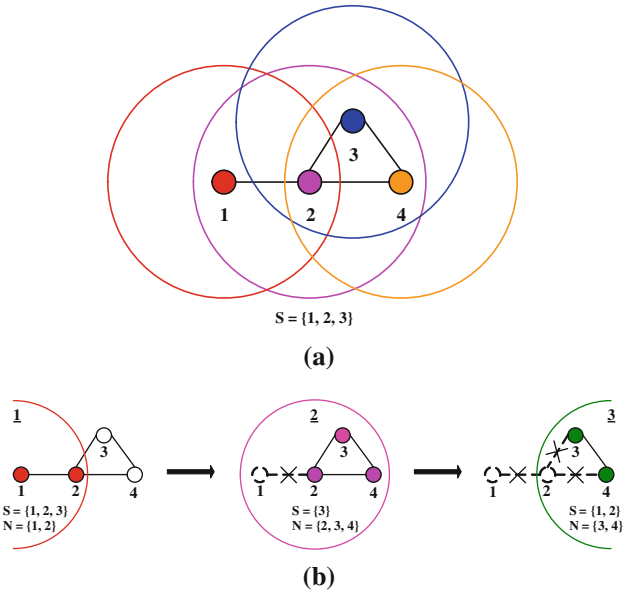


Fig. 3 An illustrative example for multi-hop spectrum auction procedure. **a** The topology of the example. **b** Subnetwork decomposition for spectrum auctions

Example 1 We present an example with the simple topology shown in Fig. 3 to further illustrate the subnetwork decomposition and multi-hop spectrum auction procedure, where $\mathcal{N} = \{1, 2, 3, 4\}$ and $\mathcal{S} = \{1, 2, 3\}$. As shown in Fig. 3, suppose that in subnetwork $\underline{1}$, bidder 1 won the spectrum bunch including band 1 and 2. Then, as for the spectrum auction in subnetwork $\underline{2}$, bidder 1 is deleted from the conflict-table of bidder 2, and only band 3 is auctioned among bidder 2, 3 and 4. Furthermore, assume bidder 2 won the auction in subnetwork $\underline{2}$. Then, considering spatial reuse, spectrum band 1 and 2 are auctioned between bidder 3 and 4.

[7] Paying the highest price in the price-charged table is to guarantee the center, bidder i, to beat other competitors in the previous subnetwork auctions, where i is not the center.

5 Design of secure subnetwork auction

Now, the only problem left is how to securely carry out the spectrum auction in each subnetwork. Since VCG auction has been proved to be incentive-compatible from the bidder side, we can modify it with cryptographic tools to prevent the insincere behaviors from the auctioneer side and apply it into spectrum auctions of the subnetworks. In this section, we first develop an equivalent variant of VCG auction, V^{2}CG auction, to allow bidders to submit bids for the bunches of bands they are interested in. Then, we elaborate on how to use homomorphic encryption to establish the subnetwork auction against untrustworthy auctioneer.

5.1 V^{2}CG auction: an equivalent variant of VCG auction

We try to find a variant of VCG auction that can achieve the same outcome as the VCG auction. In V^{2}CG auction, as in the standard VCG auction, for each bunch $\mathcal{G}$, bidder i declares his bidding value $b_i(\mathcal{G})$. Note that the declared bidding value is not necessarily the same as the true evaluation value $v_i(\mathcal{G})$.

To simplify the description, we introduce the following notation. For a set of goods $\mathcal{G} \subseteq \mathcal{S}$ and a set of bidders $\mathcal{M}$, we define $B^*(\mathcal{G}, \mathcal{M})$ as the sum of the evaluation values of $\mathcal{M}$ when $\mathcal{G}$ is allocated optimally among $\mathcal{M}$. To be precise, let us represent the set of all feasible allocations of a set of goods $\mathcal{G}$ as $\mathcal{M}^{\mathcal{G}}$, where for each $\boldsymbol{\lambda} = (\lambda(1), \lambda(2), \ldots, \lambda(m)) \in \mathcal{M}^{\mathcal{G}}$, $\bigcup_{i\in\mathcal{M}} \lambda(i) \subseteq \mathcal{G}$ and for all $i \neq j$, $\lambda(i) \cap \lambda(j) = \emptyset$ holds. $B^*(\mathcal{G}, \mathcal{M})$ is defined as follows.

$$B^*(\mathcal{G}, \mathcal{M}) = \max_{\boldsymbol{\lambda}\in\mathcal{M}^{\mathcal{G}}} \sum_{j\in\mathcal{M}} b_j(\lambda(j)). \tag{6}$$

In V^{2}CG auction, instead of determining the allocation, we first determine the price of each bunch of bands $\mathcal{G}$ for each bidder i, defined as follows:

$$p_{i,\mathcal{G}} = B^*(\mathcal{S}, \mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\mathcal{G}, \mathcal{N}\backslash\{i\}). \tag{7}$$

Next, each bidder i chooses a bundle that maximizes his utility based on the prices, i.e., he chooses $\mathcal{G}^*$, where $\mathcal{G}^* = \text{argmax}_{\mathcal{G}\subseteq\mathcal{S}} v_i(\mathcal{G}) - p_{i,\mathcal{G}}$. Note that each bidder can choose a bunch of bands that maximizes his utility independently from the choices of other bidders. To be more precise, if there exist multiple bunches that maximize his utility, then some adjustment is performed so that the choices are consistent, but each bidder is still guaranteed to obtain one bunch that maximizes his utility.

It is obvious that this V^{2}CG auction satisfies incentive compatibility. For bidder i, his prices are determined independently of i's declaration. Also, he can choose the optimal bunch of spectrum bands regardless of the choices of other bidders. Therefore, bidder i has no incentive to manipulate the prices of other bidders (which are dependent on his declaration). Since V^{2}CG auction satisfies incentive compatibility, in the rest of this paper, we assume each bidder declares his true evaluation values $v_i(\mathcal{G})$.

The proposed V^{2}CG auction is equivalent to VCG auction which can be proved by the following theorems.

Theorem 1 *A bunch of spectrum bands $\mathcal{G}$ maximizes bidder i's utility if and only if for some $\boldsymbol{\lambda}^*$, $\lambda^*(i) = \mathcal{G}$ holds.*

Proof See the proof in Appendix 1. □

Theorem 2 *If $\mathcal{G}$ maximizes bidder i's utility, then $p_i = p_{i,\mathcal{G}}$ holds.*

Proof See the proof in Appendix 2. □

Example 2 For illustrative purposes, we compare VCG auction and the V^{2}CG auction via a simple example. Assume $\mathcal{S} = \{1, 2\}$ and $\mathcal{N} = \{1, 2, 3\}$ in the subnetwork. According to VCG auction, the bidding/evaluation values of the bidders for a bunch of bands are given as follows.

	{1},	{2},	{1,2}
bidder 1 =	5	0	5
bidder 2 =	0	0	7
bidder 3 =	1	4	5

Thus, in a Pareto efficient allocation, band 1 is allocated to bidder 1 and band 2 is allocated to bidder 3. Based on VCG auction, the payment of bidder 1 is calculated as follows. Without considering bidder 1's bidding values, the optimal allocation is to allocate both bands to bidder 2, and the sum of the evaluation values, i.e., $\sum_{i\neq 1} b_i\left(\lambda^*_{\sim 1}(i)\right)$, is equal to 7. When considering bidder 1, the sum of the evaluation values other than that of bidder 1, i.e., $\sum_{i\neq 1} b_i(\lambda^*(i))$, is 4. Therefore, $p_1 = 7 - 4 = 3$. Similarly, $p_3 = 7 - 5 = 2$.

By contrast, let us show how the V^{2}CG auction works in the identical setting. From (7), the price of each bunch of spectrum bands is calculated as follows.

	{1}	{2},	{1,2}
bidder 1 =	3	7	7
bidder 2 =	5	4	9
bidder 3 =	7	2	7

Therefore, bidder 1 obtains band 1 at price 3, and bidder 3 obtains band 2 at price 2, which are the same as the results of VCG auction.

5.2 Encrypted representation of bidding values

We use homomorphic additive cryptosystem [24, 25, 40] to mask the bidding values. Assuming k ($1 \leq k \leq q$) is the bidding value for a bunch of spectrum bands λ (i.e., $k = b(\lambda)$), k can be represented by a vector $\mathbf{e}(k)$ of ciphertexts

$$\mathbf{e}(k) = (e^1, \ldots, e^q) = (\underbrace{\mathscr{E}(x), \ldots, \mathscr{E}(x)}_{k}, \underbrace{\mathscr{E}(0), \ldots, \mathscr{E}(0)}_{q-k}), \tag{8}$$

where $\mathscr{E}(0)$ and $\mathscr{E}(x)$ account for the homomorphic encryption of 0 and the common public element x ($x \neq 0$), respectively. Here, q is a number large enough to cover all the possible bidding values for any bunch of available spectrum bands. For instance, assuming $q = 3$ and $k = 2$ for the given bunch of bands λ, $\mathbf{e}(k) = \mathbf{e}(2) = (\mathscr{E}(x), \mathscr{E}(x), \mathscr{E}(0))$.

Because of the self-blinding property of $\mathscr{E}$, k cannot be determined without decrypting each element in the vector $\mathbf{e}(k)$.

Maximum Bid Selection. The maximum of encrypted bidding value, $\mathbf{e}(k_i) = (e_i^1, \ldots, e_i^q)$, can be found without leaking information about any other bidding value, $\mathbf{e}(k_j) = (e_j^1, \ldots, e_j^q), j \neq i$, as follows. Let us consider the product of all the bidding vectors for certain spectrum allocation λ,

$$\prod_i \mathbf{e}(k_i) = \left(\prod_i e_i^1, \ldots, \prod_i e_i^q \right). \tag{9}$$

By the property of homomorphic addition, the j-th component of the vector above can be denoted as

$$y_j = \prod_i e_i^j = \mathscr{E}^{c(j)}(x) = \mathscr{E}(c(j)x), \tag{10}$$

where $c(j) = |\{i \mid j \leq k_i\}|$ indicates the number of values that are equal to or greater than j.

It is obvious that $c(j)$ monotonically decreases when j increases, which gives us some hints to solving the maximum value selection problem. To find the maximum of these bidding values, we decrypt y_j and check whether decryption $\mathscr{E}^{-1}(y_j)$ is equal to 0 or not from $j = q$ down to $j = 1$ until we find the largest j subject to $\mathscr{E}^{-1}(y_j) \neq 0$. This j is equal to $\max\{k_i\}$, i.e., the maximum of the bidding values for the bunch λ.

Bid Randomization. We can make the auctioneer randomize the elements in the bidding value vector or add constants to encrypted vector $\mathbf{e}(k) = (e^1, \ldots, e^q)$ without decrypting $\mathbf{e}(k)$ nor learning k. Shifting $\mathbf{e}(k)$ by a constant r and randomizing the rest of elements, we have

$$\mathbf{e}'(k+r) = \left(\underbrace{\mathscr{E}(x), \ldots, \mathscr{E}(x)}_{r}, e'_1, \ldots, e'_{q-r} \right), \tag{11}$$

where $e_j^{'}$ is a randomized version of ciphertext e_j. No information about the constant r can be obtained from $\mathbf{e}(k)$ as well as $\mathbf{e}'(k+r)$ w.r.t. the self-blinding property of homomorphic encryption. Moreover, it should be noted that during randomizing and constant shift operations, neither $\mathbf{e}(k)$ is decrypted nor k is exposed. That is to say, if we compare $\mathbf{e}(k)$ and $\mathbf{e}(k+r)$, we cannot figure out the amount of the shift without decrypting both of them.

5.3 Payment calculation via dynamic programming

In this subsection, we illustrate how to calculate the payment of bidder i in the V^{2}CG auction via dynamic programming. This approach is based on the solution for winner determination problems in a combinatorial auction as described in Suzuki and Yokoo [42, 43].

Let $\mathbf{e}[\cdot]$ represent the encrypted value. Based on the homomorphic encryption and formula of payment in (7), assume each bidder j (except i) declares his encrypted bidding value $\mathbf{e}[b_j(\mathcal{G})]$[8] for each bunch of bands $\mathcal{G}$ in which he is interested. If bidder j has substitutable choice of band-bunch, e.g., bidder j wants either $\mathcal{G}_1$ or $\mathcal{G}_2$ but not both at the same time, we introduce a dummy good d to solve the problem. Specifically, if bidder j is interested in both $\mathcal{G}_1 \cup \{d\}$ and $\mathcal{G}_2 \cup \{d\}$, it can be avoided that both $\mathcal{G}_1$ and $\mathcal{G}_2$ are allocated to bidder j at the same time since $[\mathcal{G}_1 \cup \{d\}] \bigcap [\mathcal{G}_2 \cup \{d\}] = \{d\}$.

Then, the auctioneer creates a virtual state $(\mathcal{G}, |\mathcal{G}|)$ for each bunch $\mathcal{G} \subseteq \mathcal{S}$, where $|\mathcal{G}|$ denotes the number of available spectrum bands included in $\mathcal{G}$. Meanwhile, the auctioneer creates the following directed and weighted links for each bunch of bands $\mathcal{G}$ which bidder j is interested in.

- For a link from state $(\mathcal{G}, |\mathcal{G}|)$ to state $(\{\},0)$, the weight $w((\mathcal{G}, |\mathcal{G}|), (\{\},0))$ is $\mathbf{e}[b_j(\mathcal{G})]$ (also equal to $\mathbf{e}[v_j(\mathcal{G})]$).
- - For any $\mathcal{G}', \mathcal{G}'' \subseteq \mathcal{S}$, where $\mathcal{G}'' \subset \mathcal{G}'$, $\mathcal{G}' \backslash \mathcal{G}'' = \mathcal{G}$, and $|\mathcal{G}''| \geq |\mathcal{G}'|/2$, the weight $w((\mathcal{G}', |\mathcal{G}'|), (\mathcal{G}'', |\mathcal{G}''|))$ for a link from state $(\mathcal{G}', |\mathcal{G}'|)$ to state $(\mathcal{G}'', |\mathcal{G}''|)$ is $\mathbf{e}[v_j(\mathcal{G})]$.

If there exists a band-bunch $\mathcal{G}$ in which nobody is interested, then the auctioneer assumes a dummy bidder is interested in $\mathcal{G}$, where the bidding value submitted by the dummy bidder is $\mathbf{e}$ [0].

We present a graph of state diagram and corresponding weighted links with $\mathcal{G} = \{1, 2\}$ in Fig. 4. In this figure, the length of the longest path from initial state $(\mathcal{G}, |\mathcal{G}|)$ to terminal state $(\{\},0)$ represents the sum of the encrypted bidding values when allocating a bunch of spectrum bands $\mathcal{G}$ optimally to bidders other than i, i.e., $\mathbf{e}[B^*(\mathcal{G}, \mathcal{N} \backslash \{i\})]$. Let $\Omega((\mathcal{G}, |\mathcal{G}|))$ denote the length of the longest path from $(\mathcal{G}, |\mathcal{G}|)$ to $(\{\},0)$. Then, $\mathbf{e}[\Omega((\mathcal{G}, |\mathcal{G}|))]$ can be calculated by the following recurrence process.

[8] Since V^{2}CG auction is the variant of VCG auction and keeps the property of incentive compatibility, each bidder bids truthfully and the bidding value for any bunch of spectrum bands is equal to the evaluation value.

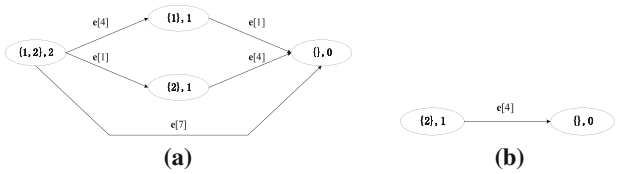


Fig. 4 An example of state diagram for dynamic programming in the case that bidder 1 is interested in $\mathcal{G} = \{1\}$. **a** The illustrative graph for $\Omega((\{1,2\},2))$ calculation. **b** The illustrative graph for $\Omega((\{2\},1))$ calculation

- $\mathbf{e}[\Omega((\{\},0))] = \mathbf{e}[0]$
- $\mathbf{e}[\Omega((\mathcal{G},|\mathcal{G}|))] = \max_{((\mathcal{G},|\mathcal{G}|),(\mathcal{G}',|\mathcal{G}'|))} \mathbf{e}[w((\mathcal{G},|\mathcal{G}|),(\mathcal{G}',|\mathcal{G}'|)) + \Omega((\mathcal{G}',|\mathcal{G}'|))]$.

Using this approach, we can obtain $\Omega((\mathcal{G},|\mathcal{G}|))$ by starting from a state that has a smaller bunch of spectrum bands.

From (7), the price of bidder i for bunch $\mathcal{G}$, i.e., $p_{i,\mathcal{G}}$, is given as $B^*(\mathcal{S},\mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\mathcal{G},\mathcal{N}\backslash\{i\})$. Therefore, $p_{i,\mathcal{G}}$ can be written as

$$p_{i,\mathcal{G}} = \Omega((\mathcal{S},|\mathcal{S}|)) - \Omega((\mathcal{S}\backslash\mathcal{G},|\mathcal{S}\backslash\mathcal{G}|)). \tag{12}$$

One special case of the subnetwork combinatorial spectrm auction is that multiple spectrum bands with identical quality are auctioned to bidding nodes. In this case, as described in Suzuki and Yokoo [42], the dynamic programming procedure requires only $\mathcal{O}(n \times m)$ states instead of 2^m states.

Example 3 With the identical setting in Ex. 2, the bidders use homomorphic encryption to mask their bidding values and the auctioneer calculates the payment of the bidders without learning the bidding values. For illustrative purposes, we take $i = 1$ and $\mathcal{G} = \{1\}$ for example and let r in the bid randomization be 0. The payment, i.e., $p_{i,\mathcal{G}}$, is calculated as follows.

From (12), the auctioneer first calculates $\mathbf{e}[\Omega((\{1,2\},2))]$. By the recurrence process, as shown in Fig. 4(a), the auctioneer finds that $\mathbf{e}[w((\{1,2\},2),(\{1\},1)) + \Omega((\{1\},1))] = \mathbf{e}[w((\{1,2\},2),(\{2\},1)) + \Omega((\{2\},1))] = \mathbf{e}(1+4)$. To find $\mathbf{e}[\Omega((\{1,2\},2))]$, the auctioneer compares $\mathbf{e}(5)$ with $w((\{1,2\},2),(\{\},0))$ by creating the product of them, i.e.,

$$\mathbf{e}(5) \cdot \mathbf{e}[w((\{1,2\},2),(\{\},0))] = \mathbf{e}(5) \cdot \mathbf{e}(7) = \left(\underbrace{\mathscr{E}(2x),\ldots,\mathscr{E}(2x)}_{5}, \mathscr{E}(x), \mathscr{E}(x), \underbrace{\mathscr{E}(0),\ldots,\mathscr{E}(0)}_{q-(5+2)} \right). \tag{13}$$

The auctioneer decrypts this vector to find $\Omega((\{1,2\},2)) = \max\{\mathbf{e}[w((\{1,2\},2),(\{\},0)),\mathbf{e}(5)\} = 7$. Similarly, as shown in Fig. 4(b), $\Omega((\{2\},1)) = 4$. As a result, $p_{1,\{1\}} = 3 = p_1$.

5.4 Procedure of the secure subnetwork spectrum auction

Similar to *THEMIS* in Pan et al. [23], *SCSA* employs plural servers $\mathcal{L} = \{1,2,\ldots,l\}$ to share the secret key $\mathscr{E}$, to calculate the charging price of bidders and to determine the winner of subnetwork spectrum auction in a distributed manner. The servers are implemented in the form of either the third party servers or even the bidders themselves. The task of calculating the price of bidder i can be distributed among other bidders because even if bidder j, which interferes with bidder i, manipulates bidder i's price, this manipulation does not affect the price of bidder j as illustrated in Sect. 5.1. Therefore, bidder j has no incentive to manipulate the price of bidder i and can participate in the procedure for calculating the prices of bidder i.

More specifically, the procedure of the proposed secure subnetwork auction is as follows.

- Each of the servers is entitled to have a share of a secret key for $\mathscr{E}$ so that if t servers[9] cooperate, they can decrypt $\mathscr{E}$. The secret and public keys are generated in a distributed way, and each server has only a share of the secret key [42, 45].
- Each bidder i submits an encrypted vector that represents his bidding/evaluation value $b_i(\mathcal{G})$ for each bunch of spectrum bands $\mathcal{G}$ in which he is interested to the auctioneer.
- For bidder $i \in \mathcal{N}$, the following process is conducted by the auctioneer.
  (1) Any t servers can be utilized to calculate the prices for bidder i. The randomly selected servers are regarded as payment-calculators for bidder i.
  (2) The auctioneer first exploits the payment-calculators to construct the state diagram using the encrypted bidding/evaluation values except that of i. Then, the auctioneer calculates $\Omega((\mathcal{G},|\mathcal{G}|))$ for each node using the approach described in the subsection above. Next, for each bunch of bands $\mathcal{G}$ that bidder i desires to have, the auctioneer calculates $p_{i,\mathcal{G}} = \Omega((\mathcal{S},|\mathcal{S}|)) - \Omega((\mathcal{S}\backslash\mathcal{G},|\mathcal{S}\backslash\mathcal{G}|))$.
  (3) The auctioneer sends this payment (i.e., $p_{i,\mathcal{G}}$) calculated by the t servers to bidder i.
  (4) Bidder i finds all bunch of bands that maximize his utility and informs the auctioneer the set of bunches that he wants to use.

[9] The keys for decrypting bidding values are shared by the plural servers by using secret sharing technique. A lot of secret sharing or group decryption mechanisms can be employed to effectively prevent the distributed servers from colluding with each other to reveal the bids. Please refer to Pedersen [44], Shamir [45] for the details about secret sharing algorithms.

– The auctioneer adjusts the allocation of spectrum bunches to ensure no conflicts among them.

6 Simulation and analysis

In this section, we compare the proposed *SCSA* with the existing spectrum auction designs, i.e., *VERITAS* in Zhou et al. [8], the Multi-Winner spectrum auction (*M-W*) in Wu et al. [11] and *THEMIS* in Pan et al. [23]. Since neither *VERITAS* nor *M-W* is resistant to the untrustworthy auctioneer, we first compare the performance of *SCSA* with that of *M-W*, *VERITAS* and *THEMIS* in a fraud and bid-rigging free environment in terms of spectrum utilization, auctioneer's revenue and bidders' satisfactory degree. Then, in security analysis, we demonstrate that the homomorphic encryption based *SCSA* can effectively purge the frauds and bid-riggings incurred by untrustworthy auctioneer. Finally, we show the cost of leveraging homomorphic encryption to secure combinatorial spectrum auction in the efficiency analysis part, and compare *SCSA* with *THEMIS* in terms of communication and computational complexity.

6.1 Performance comparison

6.1.1 Simulation setup

We assume the spectrum auction hosted by the auctioneer is deployed in a 1*1 square area, where nodes are uniformly distributed and connected [46, 47]. Suppose the wireless mutual interference is simply distance-based, and any two bidders within 0.1 distance conflict with each other and cannot be allocated with the same spectrum bands. The bidding values of different bidders over different bands are supposed to be i.i.d random variables uniformly distributed over (0,10]. To be simple, for every bidder, we let the bidding value for a bunch of bands be the sum of bidding values for the bands, which constitutes the value of the spectrum bunch. We use the following three performance metrics to compare *SCSA* with *M-W*, *VERITAS* and *THEMIS*.

- *Spectrum Utilization :* It is the sum of the allocated spectrum bands of all the winning bidders, which is the same as the definition in Zhou et al. [8].
- *Auctioneer's Revenue :* It is the sum of payments of all the winning bidders, as defined in Sect. 3.
- *Bidders' Satisfaction :* It is defined as the ratio of $\sum_{i\in\mathcal{W}} u_i$ to $\sum_{i\in\mathcal{N}} v_i$, which denotes the percentage of bidders' potential monetary gains realized.

6.1.2 Results and analysis

Figure 5 shows the performance of the spectrum utilization, auctioneer's revenue and bidder's satisfaction for the four auction designs with 200 and 300 bidders, respectively.

In Fig. 5(a), as the number of spectrum bands increases, the spectrum utilization also increases until it saturates (i.e., every bidder is allocated a band) in all these four auctions. It is not surprising that the performance results of *M-W*, *VERITAS*, *THEMIS* and *SCSA* are the same in terms of spectrum utilization, because they mainly differ in their price charging designs if the auctioneer can be trusted.

In Fig. 5(b), we find that *SCSA* is the same as *THEMIS* in terms of the auctioneer's revenue since the V^2CG auction is only a variant of the VCG auction and the payment of each bidder for the two auctions is equal as illustrated in Sect. 5.1. *SCSA* is slightly higher than *M-W* at only a few points. It makes sense because *SCSA* originates from the VCG auction and *M-W* is based on secondary price auction, while VCG is equivalent to secondary price auction provided that the good consists of only one single item [12]. The bump of *SCSA* over *M-W* is from the payments for the winning bidders located in the crossing area of subnetworks, where the highest price in the price-charged table is paid for the bunch of bands as illustrated in Sect. 4. Moreover, *VERITAS* is characterized by charging the winners with their *critical neighbor* prices [8], which makes it perform a little bit better than the other designs in the auctioneer's revenue. By contrast, in Fig. 5(c), *VERITAS* loses his advantages correspondingly, and *SCSA*, *M-W* and *THEMIS* outperform it in bidders' satisfactory degree. Actually, the auctioneer's revenue and bidders' satisfactory degree are just two complementary evaluation metrics.

Based on the comparison and analysis above, we observe that *SCSA* almost sacrifices nothing in performance from the view of mechanism designs.

6.2 Security analysis

Let us recap and clarify two properties of homomorphic encryption. First, due to the indistinguishability, no information about the value k can be leaked out from its representation $\mathbf{e}(k)$ without decrypting each element. Second, self-blinding property makes it impossible to find a mapping function from $\mathbf{e}(k)$ to $\mathbf{e}'(k + r)$, where r is a random number.

To prevent an untrustworthy auctioneer from learning the bids and manipulating the auction by frauds, in *SCSA*, the decryption to determine the maximum of truthful bidding values and the addition of random mask constant r are

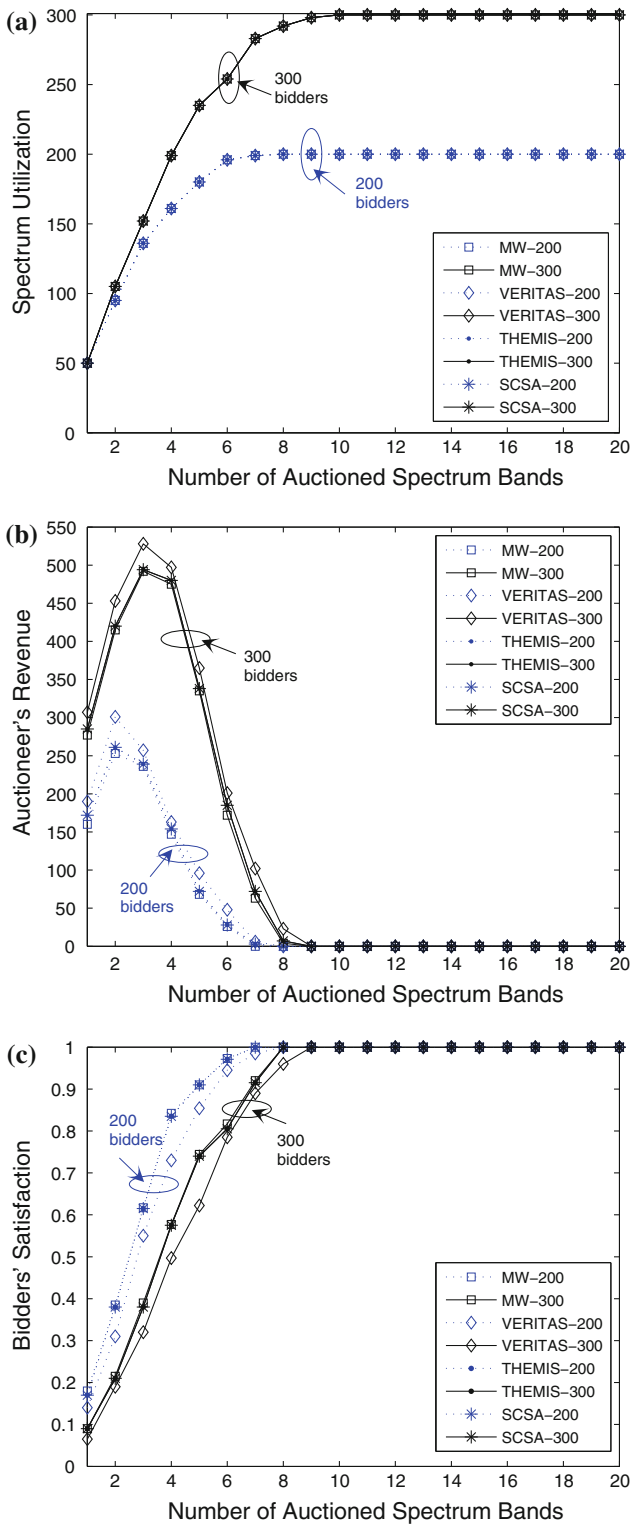


Fig. 5 Performance comparison of *M-W*, *VERITAS*, *THEMIS* and *SCSA*. **a** Spectrum utilization. **b** Revenue of the auctioneer. **c** Bidders' satisfaction

both performed in a distributed manner by the servers as mentioned in Sect. 5.4. By using *SCSA*, for bidder i, the payment-calculator consisting of t servers learns $B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})$ for each state $(\mathcal{G}, |\mathcal{G}|)$. However, note that $B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})$ is obtained by aggregating many truthful bidding values of bidders, so that it is difficult to estimate each bidding value or learn random mask constant r from $B^*(\mathcal{G}, \mathcal{N}\backslash\{i\})$. The auctioneer cannot decrypt vectors representing the bidding values of bidders, unless it colludes with at least t servers.

Asides from the frauds, the bid-rigging between the bidders and the auctioneer becomes meaningless because the individual server itself knows nothing more than the winners and their payments in *SCSA*. Even if a bidder could collude with the auctioneer as well as a number of servers, he is not able to find out any information about the bids if only the number of servers is less than t.

Furthermore, *SCSA* satisfies the fairness requirements of the spectrum auction because it treats all the bidders equally, selects the bidder with the highest bid to win a bunch of spectrum bands in each subnetwork, and makes the multiple winning bidders pay by predefined rule. Besides, *SCSA* also guarantees the anonymity of the spectrum auction in the sense that it leaks out no more information than the winning bidders and corresponding price charged during the opening phase.

Although homomorphic encryption is intrinsically malleable[10], which results in the loss of integrity guarantee of the bids, the malleability of this encryption perfectly matches with the secure spectrum design. Assuming the auctioneer only has the information about the winner and his payment, an insincere but not malicious auctioneer has no incentive to tamper with the charging price. The auctioneer would not risk overcharging the winner at a price even higher than the highest bid provided that the auctioneer knows nothing about the bidding values at all. On the other hand, the malleability[11] of homomorphic encryption is helpful to the selection of winners and the computation of the payment in *SCSA*.

[10] An encryption algorithm is malleable if it allows an adversary to modify the contents of the message, i.e., to transform the ciphertext into another ciphertext which can be decrypted to a related plaintext [48]. For example, given an encryption of a plaintext m, it is possible to generate another ciphertext which can be decrypted to $f(m)$, for a known function f, without necessarily knowing or learning m.

[11] Malleability may be exploited by outsiders (e.g., eavesdroppers, active attackers) to modify the bids on the fly. To further address this potential vulnerability, some integrity protection mechanisms (i.e., keyed-hash message authentication code (HMAC), digital signature) can be employed. Specifically, HMAC is infeasible since there is no shared secret between the bidders and the auctioneer. We can therefore use digital signatures by adopting the public key infrastructure such as identity-based cryptosystem [49], whose additional computation complexity should not be a concern for the bidders (e.g., cellular phones, PDAs, laptops, etc.).

Table 1 The comparison of different spectrum auction designs

Spec-auction designs	Spatial reuse	Truthful bidding	Risk-neutral attraction	Bid-rigging resistant	Frauds Resistant	Combinatorial Spec-Auction
VERITAS	✔	✔	×	×	×	×
M–W	✔	✔	✔	×	×	×
THEMIS	✔	✔	✔	✔	✔	×
SCSA	✔	✔	✔	✔	✔	✔

Table 2 The comparison of communication complexity between *THEMIS* and *SCSA*

Spectrum auction designs	*THEMIS*		*SCSA*	
Pattern	Round	Volume	Round	Volume
The bidders ↔ The auctioneer	$\mathcal{O}(n \log n)$	$\mathcal{O}(n \log n \times (\log n)^s \times q \log n)$	$\mathcal{O}(n \log n)$	$\mathcal{O}(n \log n \times 2^s \times q \log n)$
The bidder ↔ neighbor bidders	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$

Table 3 The comparison of computational complexity between *THEMIS* and *SCSA*

Spectrum auction designs Pattern	*THEMIS* Computational complexity	*SCSA* Computational complexity
The bidder	$\mathcal{O}(n \log n \times (\log n)^s \times q \log n)$	$\mathcal{O}(n \log n \times 2^s \times q \log n)$
The auctioneer	$\mathcal{O}(t \times n \log n \times (\log n)^s \times q \log n)$	$\mathcal{O}(t \times n \log n \times 2^s \times q \log n)$

6.3 Efficiency analysis

The communication and computational complexity of a secure spectrum auction against untrustworthy auctioneer are determined by several factors, namely, the number of bidders n, the number of available spectrum bands s, the number of possible bidding values q, and the number of servers t composing the payment-calculator. Here, we assume the network in the auction area is connected, which implies that the node density of the subnetworks is on the order of $\mathcal{O}(\log n)$ [47].

Table 2 shows the communication pattern, the order of communication rounds and the communication volume for bidders in both *THEMIS* and *SCSA*. In *THEMIS*, the bidder must declare his evaluation values over all $\mathcal{O}(\log n^s)$ possible allocations in the subnetwork auction. But in the subnetwork auction of *SCSA*, the bidder only declares his evaluation values for the spectrum bunch that he is interested in, where the number of states for those bunches is in the order of $\mathcal{O}(2^s)$. Compared with *THEMIS*, it effectively reduces the communication overhead, especially for the case that the network density is high. In addition, the communication complexity from the bidder to the auctioneer is linear in terms of the number of possible maximum bidding values q for homomorphic encryption, so it may incur a heavy cost for a large range of bidding values. However, this is inevitable cost for purging the frauds and bid-riggings. Meanwhile, the communication complexity is closely related to s. Since spectrum is scare resource and the available bands cannot be arbitrarily large, s will not impose much communication cost. Compared with conventional secure auction designs [29–31], there is also additional communication complexity incurred by the subnetwork decomposition. But this overhead is unavoidable when we take frequency reuse into consideration.

Table 3 shows the computational complexity for the auctioneer and a bidder in both *THEMIS* and *SCSA*. The computational complexity of bidders and the auctioneer is also related to the subnetwork composition, linear in terms of the number of possible bidding values q and exponential in terms of available spectrum bands s. Similar to the analysis of communication cost, we find that *SCSA* is much more efficient than *THEMIS* in terms of computational complexity as well.

7 Conclusion

To purge the frauds and bid-riggings caused by the untrustworthy auctioneer, in this paper, we have incorporated cryptographic technique into the spectrum auction design and proposed *SCSA*, a secure combinatorial spectrum auction scheme based on homomorphic encryption. Considering frequency reuse, we have divided the whole network into small subnetworks and allowed the bidders to maintain and update their conflict-tables, which facilitate

the spectrum allocation. *SCSA* masks the bidding values of a bidder with a vector of homomorphic ciphertexts. By effectively utilizing the properties of homomorphic encryption, *SCSA* enables the auctioneer to find the maximum bid and calculate the charging prices for a bunch of spectrum bands securely in the subnetwork auction, while keeping the actual bidding values confidential. In this case, frauds and bid-rigging become impossible, and insincere auctioneer's manipulation of the auction is implausible. Compared with our previously designed secure spectrum auction against the untrustworthy auctioneer, namely *THEMIS*, our *SCSA* is much more efficient in terms of communication and computational complexity. We also show that *SCSA* is as good as other spectrum auction designs with the trustworthy auctioneer in terms of spectrum utilization, the auctioneer's revenue and bidders' satisfaction.

Acknowledgments This work was partially supported by the U.S. National Science Foundation under grants CNS-1147813 and ECCS-1129062. The work of X. Zhu was partially supported by the National Natural Science Foundation of China under grant 61003300, the Fundamental Research Funds for the Central Universities under grant JY10000901021 and the China 111 Project under grant B08038.

Appendix

Proof of Theorems

Proof of Theorem 1

Proof From the definition in (6), the following formula holds:

$$\sum_{j\neq i} b_j\left(\lambda^*_{\sim i}(j)\right) = B^*(\mathcal{S},\mathcal{N}\backslash\{i\}). \tag{14}$$

Moreover, for $\boldsymbol{\lambda}^* = (\lambda^*(1),\lambda^*(2),\ldots,\lambda^*(n))$, the following formula holds:

$$\sum_{j\neq i} b_j(\lambda^*(j)) = B^*(\mathcal{S}\backslash\lambda^*(i),\mathcal{N}\backslash\{i\}). \tag{15}$$

The proof of Theorem 1 is conducted as follows. First, we show if for some $\boldsymbol{\lambda}^*$, $\lambda^*(i)=\mathcal{G}$, then $\mathcal{G}$ maximizes bidder i's utility. Specifically, we are going to derive a contradiction by assuming for some $\boldsymbol{\lambda}^*$, $\lambda^*(i)=\mathcal{G}$ but bundle $\mathcal{G}$ does not maximize bidder i's utility. In this case, there exists another bunch $\mathcal{G}'$ and $b_i(\mathcal{G}')-p_{i,\mathcal{G}'} > b_i(\mathcal{G})-p_{i,\mathcal{G}}$ holds, where $b_i(\mathcal{G}')=v_i(\mathcal{G}')$ and $b_i(\mathcal{G})=v_i(\mathcal{G})$ in the VCG auction.

$$p_{i,\mathcal{G}'} = B^*(\mathcal{S},\mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\mathcal{G}',\mathcal{N}\backslash\{i\}). \tag{16}$$

$$p_{i,\mathcal{G}} = B^*(\mathcal{S},\mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\mathcal{G},\mathcal{N}\backslash\{i\}). \tag{17}$$

By substituting $p_{i,\mathcal{G}'}$ and $p_{i,\mathcal{G}}$ into the inequality function, the following formula holds.

$$b_i(\mathcal{G}') + B^*(\mathcal{S}\backslash\mathcal{G}',\mathcal{N}\backslash\{i\}) > b_i(\mathcal{G}) + B^*(\mathcal{S}\backslash\mathcal{G},\mathcal{N}\backslash\{i\}). \tag{18}$$

However, the right side of the equation above can easily be transformed as follows.

$$\begin{aligned} b_i(\mathcal{G}) + B^*(\mathcal{S}\backslash\mathcal{G},\mathcal{N}\backslash\{i\}) &= b_i(\lambda^*(i)) + B^*(\mathcal{S}\backslash\lambda^*(i),\mathcal{N}\backslash\{i\}) \\ &= b_i(\lambda^*(i)) + \sum_{j\neq i} b_j(\lambda^*(j)) \\ &= \sum_i b_i(\lambda^*(i)). \end{aligned} \tag{19}$$

The right side of this equation represents the sum of evaluation values at Pareto efficient allocation $\boldsymbol{\lambda}^*$. However, from (18), the left side is less than $b_i(\mathcal{G}')+B^*(\mathcal{S}\backslash\mathcal{G}',\mathcal{N}\backslash\{i\})$, i.e., allocating $\mathcal{G}'$ to bidder i and allocating other bands optimally among bidders other than i. This contradicts the assumption that $\boldsymbol{\lambda}^*$ is Pareto efficient.

Then, we prove that if a bunch $\mathcal{G}$ maximizes bidder i's utility, then for some $\boldsymbol{\lambda}^*$, $\lambda^*=\mathcal{G}$ holds. Similarly, we are going to derive a contradiction by assuming a spectrum bunch $\mathcal{G}$ maximizes bidder i's utility but for any $\boldsymbol{\lambda}^*$, $\lambda^*\neq\mathcal{G}$. In this case, there exists a spectrum bunch $\mathcal{G}'$, where $\mathcal{G}'\neq\mathcal{G}$, $\mathcal{G}'=\lambda^*$, and $b_i(\mathcal{G})-p_{i,\mathcal{G}} > b_i(\mathcal{G}')-p_{i,\mathcal{G}'}$ hold. Thus, the following formula holds.

$$b_i(\mathcal{G}) + B^*(\mathcal{S}\backslash\mathcal{G},\mathcal{N}\backslash\{i\}) > b_i(\mathcal{G}') + B^*(\mathcal{S}\backslash\mathcal{G}',\mathcal{N}\backslash\{i\}). \tag{20}$$

However, the right side of this formula represents the sum of evaluation values at Pareto efficient allocation $\boldsymbol{\lambda}^*$, while the left side is the sum of evaluation values when allocating $\mathcal{G}$ to bidder i and allocating other bands optimally among bidders except i. This contradicts the assumption that $\boldsymbol{\lambda}^*$ is Pareto efficient. □

Proof of Theorem 2

Proof According to Theorem 1, when $\mathcal{G}$ maximizes bidder i's utility, then for some $\boldsymbol{\lambda}^*$, $\lambda^*=\mathcal{G}$ holds. Therefore,

$$\begin{aligned} p_i &= \sum_{j\neq i} b_i\left(\lambda^*_{\sim i}(j)\right) - \sum_{j\neq i} b_i(\lambda^*(j)) \\ &= B^*(\mathcal{S},\mathcal{N}\backslash\{i\}) - B^*(\mathcal{S}\backslash\lambda^*(i),\mathcal{N}\backslash\{i\}) \\ &= p_{i,\mathcal{G}}. \end{aligned} \tag{21}$$

If there exist multiple Pareto efficient allocations, then multiple bunches can simultaneously maximize the bidder's utility. In this case, the auctioneer needs to adjust allocations so that the choices of bidders are consistent, i.e., no spectrum band is allocated to different bidders simultaneously. Theorem 1 demonstrates that any

bunch of spectrum bands $\mathcal{G}$ that is allocated to bidder i in a Pareto efficient allocation would maximize bidder i's utility. Therefore, by choosing any Pareto efficient allocation, there is always a way to adjust the choices of bidders so that each bidder is guaranteed to obtain one of the optimal spectrum bunch. □

References

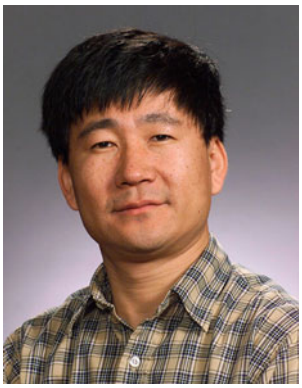
1. FCC (2002). *Spectrum policy task force report*. Report of Federal Communications Commission, Et docket No. 02-135, November 2002.
2. IEEE 802.22 Working Group on Wireless Regional Area Networks (2006). *IEEE P802.22/D0.1 Draft standard for wireless regional area networks part 22: Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands*, [Online]. Available: http://www.ieee802.org/22.
3. Mitola, J. (2000). Cognitive radio: An integrated agent architecture for software defined radio (Ph.D. Thesis, Royal Institute of Technology, Sweden, 2000).
4. Akyildiz, I., Lee, W., Vuran, M., & Shantidev, M. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(4), 2127–2159.
5. Sengupta, S., & Chatterjee, M. (2009). An economic framework for dynamic spectrum access and service pricing. *IEEE/ACM Transactions on Networking, 17*(4), 1200–1213.
6. Pan, M., Chen, F., Yin, X., & Fang, Y. (2009). Fair profit allocation in the spectrum auction using the shapley value. In *Proceedings of IEEE global telecommunications conference, Globecom '09*. Honolulu, HI, USA.
7. Zhang, J., & Zhang, Q. (2009). Stackelberg game for utility-based cooperative cognitive radio networks. In *Proceedings of ACM international symposium on mobile ad hoc networking and computing, ACM MobiHoc*. New Orleans, LA.
8. Zhou, X., Gandhi, S., Suri, S., & Zheng, H. (2008). eBay in the sky: Strategy-proof wireless spectrum auctions. In *Proceedimgs of mobile computing and networking, Mobicom '08*. San Francisco, CA.
9. Zhou, X., & Zheng, H. (2009). Trust: A general framework for truthful double spectrum auctions. In *Proceedings of IEEE conference on computer communications, INFOCOM 2009*. Rio de Janeiro, Brazil.
10. Jia, J., Zhang, Q., Zhang, Q., & Liu, M. (2009). Revenue generation for truthful spectrum auction in dynamic spectrum access. In *Proceedings of ACM international symposium on mobile ad hoc networking and computing, ACM MobiHoc, 2009*. New Orleans, LA.
11. Wu, Y., Wang, B., Liu, K. J., & Clancy, T. (2008). A multi-winner cognitive spectrum auction framework with collusion-resistant mechanisms. In *Proceedings of IEEE international symposium on new frontiers in dynamic spectrum access networks, DySPAN '08*. Chicago, IL.
12. Krishna, V. (2002). *Auction theory*. New York: Academic Press.
13. Vickrey, W. (1961). Counter speculation, auctions, and competitive sealed tenders. *The Journal of Finance, 16*(1), 8–37.
14. Vries, S., & Vohra, R. (2003). Combinatorial auctions: A survey. *INFORMS Journal on Computing, 15*(3), 284–309.
15. Cramton, P., Shoham, Y., & Steinberg, R. (2006). *Combinatorial auctions*. Cambridge: MIT Press.
16. Groves, T. (1973). Incentives in teams. *Econometrica, 41*, 617–631.
17. Wu, C.-C., Chang, C.-C., & Lin I.-C. (2008). New sealed-bid electronic auction with fairness, security and efficiency. *Journal of Computer Science and Technology, 23*(2), 253–264.
18. Peng, K., Boyd, C., & Dawson, E. (2006). Batch verification of validity of bids in homomorphic e-auction. *Computer Communications, 29*(15), 2798–2805.
19. Boyd, C., & Mao, W. (2003) Security issues for electronic auctions. In *Proceedings of the financial cryptography conference FC '03*. Guadeloupe, French West Indies.
20. Gandhi, S., Buragohain, C., Cao, L., Zheng, H., & Suri, S. (2007). A general framework for wireless spectrum auctions. In *Proceedings of IEEE international symposium on new frontiers in dynamic spectrum access networks, DySPAN '07*. Dublin, Ireland.
21. Jain, K., Padhye, J., Padmanabhan, V. N., & Qiu, L. (2003). Impact of interference on multi-hop wireless network performance. In *Proceedings of mobile computing and networking, Mobicom '03*. San Diego, CA.
22. Zhou, X., & Zheng, H. (2010). Breaking bidder collusion in large-scale spectrum auctions. In *Proceedings of ACM international symposium on mobile ad hoc networking and computing, ACM MobiHoc, 2010*. Chicago, IL.
23. Pan, M., Sun, J., & Fang, Y. (2011). Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem. *IEEE Journal on Selected Areas in Communications, 29*(4), 866–876.
24. Paillier, P. (1999). Cryptographie à clé publique basée sur la résiduosité de degré composite (Ph.D. Thesis, École Nationale Supérieure des Télécommunications, Paris, France).
25. Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of IEEE international conference on computational intelligence for modelling, control, and automation, EUROCRYPT '99*. Prague, Czech Republic.
26. Paillier, P., & Pointcheval, D. (1999). Efficient public-key cryptosystems provably secure against active adversaries. In *Proceedings of advances in cryptology, ASIACRYPT '99*. Singapore.
27. Sawa, S., Itoh, H., & Nakamura, K. (2006). An evolutionary basis for preference behavior in decision making under risk. In *Proceedings of IEEE international conference on computational intelligence for modelling, control, and automation, CIMCA '06*. Sydney, Australia.
28. Kikuchi, H. (2001). (m + 1)st-price auction protocol. In *Proceeings of financial cryptography, FC '01*. Grand Cayman, British West Indies.
29. Yokoo, M., & Suzuki, K. (2002). Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions. In *Proceedings of the first international joint conference on autonomous agents and multi-agent systems, AAMAS '02*. Bologna, Italy.
30. Suzuki, K., & Yokoo, M. (2003). Secure generalized vickrey auction using homomorphic encryption. In *Proceedings of the financial cryptography conference, FC '03*. Guadeloupe, French West Indies.
31. Yokoo, M., & Suzuki, K. (2004). Secure generalized vickrey auction without third-party servers. In *Proceedings of the financial cryptography conference, FC '04*. Key West, FL.
32. Xing, Y., Chandramouli, R., & Cordeiro, C. (2007). Price dynamics in competitive agile spectrum access markets. *IEEE Journal on Selected Areas in Communications, 25*(3), 613–621.
33. Niyato, D., & Hossain, E. (2008). Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion. *IEEE Journal on Selected Areas in Communications, 26*(1), 192–202.
34. Pan, M., Song, Y., Li, P., & Fang, Y. (2010). Reward and risk for opportunistic spectrum accessing in cognitive radio networks. In *Proceedings of IEEE global telecommunications conference, Globecom 2010*, Miami, FL.
35. Chen, C.-C., & Lee, D.-S. (2006). A joint design of distributed qos scheduling and power control for wireless networks. In *Proceedings of IEEE conference on computer communications, INFOCOM '06*. Barcelona, Catalunya, Spain.

36. Gupta, P., & Kumar, P. R. (2000). The capacity of wireless networks. *IEEE Transactions on Information Theory, 46*(2), 388–404.
37. Giupponi, L., Agusti, R., Perez-Romero, J., & Roig, O. S. (2008). A novel approach for joint radio resource management based on fuzzy neural methodology. *IEEE Transactions on Vehicular Technology, 57*(3), 1789–1805.
38. Perez-Romero, J., Salient, O., Agusti, R., & Giupponi, L. (2007). A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation. In *Proceedings of IEEE international symposium on new frontiers in dynamic spectrum access networks, DySPAN '07*. Dublin, Ireland.
39. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. on Information Theory, 31*(4), 469–472.
40. Benaloh, J. (1994). Dense probabilistic encryption. In *Proceedings of the workshop on selected areas in cryptography*. Kingston, ON, Canada.
41. Goh, E. (2007). Encryption schemes from bilinear maps (Ph.D. Thesis, Stanford University, USA).
42. Suzuki, K., & Yokoo, M. (2002). Secure combinatorial auctions by dynamic programming with polynomial secret sharing. In *Proceedings of the financial cryptography conference FC '02*. Southampton, Bermuda.
43. Bellman, R. (1957). *Dynamic programming*. Princeton, NJ: Princeton University Press.
44. Pedersen, T. P. (1991). Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of advances in cryptology CRYPTO '91*. Santa Barbara, CA, USA.
45. Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612–613.
46. Bettstetter, C. (2002). On the minimum node degree and connectivity of a wireless multihop network. In *Proceedings of ACM international symposium on mobile ad hoc networking and computing, Mobihoc '02*. Lausanne, Switzerland.
47. Xue, F., & Kumar, P. (2004). The number of neighbors needed for connectivity of wireless networks. *Wireless Networks, 10*(2), 169–181.
48. Danny, D., Cynthia, D., & Moni, N. (2000). Nonmalleable cryptography. *SIAM Journal of Computing, 30*(2), 391–437.
49. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the weil pairings. *Advances in Cryptology-Asiacrypt*, 514–532.

Author Biographies

Miao Pan received his BSc degree in Electrical Engineering from Dalian University of Technology, China, in 2004 and MASc degree in electrical and computer engineering from Beijing University of Posts and Telecommunications, China, in 2007. He has been working towards the Ph.D. degree in the Department of Electrical and Computer Engineering at University of Florida, Gainesville since August 2007. His research interests include cognitive radio networks, spectrum auction, game theory, radio resource allocation and cross-layer optimization.

Xiaoyan Zhu received her BE in Information Engineering and ME in Information and Communications Engineering, a Ph.D. from the School of Telecommunications Engineering, all at Xidian University, Xi'an, China, in 2000, 2004 and 2009 respectively. She was a visiting research scholar in the Department of Electrical and Computer Engineering at University of Florida, Gainesville, USA from 2008 to 2010. She is currently an Associate Professor in the School of Telecommunications Engineering, at Xidian University. Her research interests include wireless networks and network security.



Yuguang Fang received a Ph.D. degree in Systems Engineering from Case Western Reserve University in January 1994 and a Ph.D. degree in Electrical Engineering from Boston University in May 1997. He was an assistant professor in the Department of Electrical and Computer Engineering at New Jersey Institute of Technology from July 1998 to May 2000. He then joined the Department of Electrical and Computer Engineering at University of Florida in May 2000 as an assistant professor, got an early promotion to an associate professor with tenure in August 2003 and to a full professor in August 2005. He holds a University of Florida Research Foundation (UFRF) Professorship from 2006 to 2009, a Changjiang Scholar Chair Professorship with Xidian University, Xi'an, China, from 2008 to 2011, and a Guest Chair Professorship with Tsinghua University, China, from 2009 to 2012. He has published over 300 papers in refereed professional journals and conferences. Dr. Fang received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002, and is the recipient of the Best Paper Award in IEEE International Conference on Network Protocols (ICNP) in 2006 and the recipient of the IEEE TCGN Best Paper Award in the IEEE High-Speed Networks Symposium, IEEE Globecom in 2002. He has also received a 2010-2011 UF Doctoral Dissertation Advisor/Mentoring Award and the 2009 UF College of Engineering Faculty Mentoring Award. Dr. Fang is also active in professional activities. He is a Fellow of IEEE and a member of ACM. He is currently serving as the Editor-in-Chief for IEEE Wireless Communications (2009-present) and serves/served on several editorial boards of technical journals including IEEE Transactions on Mobile Computing (2003-2008, 2011-present), IEEE Transactions on Communications (2000-present), IEEE Transactions on Wireless Communications (2002-2009), IEEE Journal on Selected Areas in Communications (1999-2001), IEEE Wireless Communications Magazine (2003-2009) and ACM Wireless Networks (2001-present). He served on the Steering Committee for IEEE Transactions on Mobile Computing (2008-2010). He has been actively participating in professional conference organizations such as serving as the Technical Program Co-Chair

for IEEE INOFOCOM'2014, the Steering Committee Co-Chair for QShine (2004-2008), the Technical Program Vice-Chair for IEEE INFOCOM'2005, the Technical Program Area Chair for IEEE INFOCOM (2009-2012), Technical Program Symposium Co-Chair for IEEE Globecom'2004, and a member of Technical Program Committee for IEEE INFOCOM (1998, 2000, 2003-2008).