Purging the Back-Room Dealing: Secure Spectrum Auction Leveraging Paillier Cryptosystem

Miao Pan, *Student Member, IEEE,* Jinyuan Sun, *Member, IEEE*, and Yuguang Fang, *Fellow, IEEE*

***Abstract*—Microeconomics-inspired spectrum auctions can dramatically improve the spectrum utilization for wireless networks to satisfy the ever increasing service demands. However, the back-room dealing (i.e., the frauds of the insincere auctioneer and the bid-rigging between the greedy bidders and the auctioneer) poses significant security challenges, and fails all existing secure auction designs to allocate spectrum bands when considering the frequency reuse in wireless networks. In this paper, we propose *THEMIS*, a secure spectrum auction leveraging the Paillier cryptosystem to prevent the frauds of the insincere auctioneer as well as the bid-rigging between the bidders and the auctioneer. *THEMIS* incorporates cryptographic technique into spectrum auction to address the challenges of back-room dealing. It computes and reveals the results of spectrum auction while the actual bidding values of bidders are kept confidential. *THEMIS* also provides a novel procedure for implementing secure spectrum auction under interference constraints. It has been shown that *THEMIS* can effectively purge the back-room dealing with limited communication and computational complexity, and achieve similar performance compared with existing insecure spectrum auction designs in terms of spectrum utilization, revenue of the auctioneer, and bidders' satisfaction.**

***Index Terms*—Secure Spectrum Auctions, Paillier Cryptosystem, Auction Procedure, Homomorphic Addition**

I. Introduction

DURING the last decade, the dilemma between the rapid growth of wireless services and the limited radio spectrum has shoved the fixed spectrum allocation of Federal Communications Commission (FCC) off the edge, and resulted in 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], [13], i.e., open or sealed auction according to the bidding manner, first price auction, secondary price auction, Vickery auction [14], or Vickrey-Clarke-Groves (VCG) auction (also known as Generalized Vickrey Auction, i.e., GVA) according to the pricing manner, and single item or combinatorial auction according to the number of auctioned goods [15], [16]. According to the requirements, these auction mechanisms can be applied to different scenarios. For instance, the most widely used auctioneer-favored auction, English auction [12], [13], is an open first price auction, where 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 the sense that each bidder has to strategize delicately to win, which inevitably leads to great complexity and a long auction time. On the contrary, the sealed secondary price auction can make sure the bidders submit their bids with true evaluation values and save 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 [17]. With respect to the security issues, there has been considerable work on designing electronic auction with different features, such as fairness [18], [19], confidentiality, anonymity and so on [20].

Despite the desirable characteristics, traditional auction cannot be hammered into the spectrum auction design directly. Unlike common goods in conventional auctions, spectrum is reusable among bidders subject to the spatial interference constraints, i.e., bidders geographically far apart can use the same frequency simultaneously while bidders in close proximity cannot. Even though interference is only a local effect, the spatial reuse of frequency makes the problem of finding the optimal spectrum allocation NP-complete [21], [22], which fails all the optimal allocation based conventional auction mechanisms [8]. Besides, these unique properties of spectrum *butterfly* 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, the task of designing a secure spectrum auction is highly challenging but imperative.

To deal with the mutual interference between neighboring bidders, Gandhi et al. [21] has proposed the conflict graph and a general framework for wireless spectrum auctions. Based on these concepts, a truthfully bidding spectrum auction, *VERITAS*, is proposed by Zhou et al. in [8]. The notion of critical neighbor/value is proposed and employed to guarantee the auction strategy-proof. However, the bidders in *VERITAS* must be risk-seeking. Otherwise, if the bidders are only greedy, but

Manuscript received 1 December 2009; revised 1 May 2010. This work was partially supported by the U.S. National Science Foundation under grants CNS-0721744 and CNS-0916391. The work of Y. Fang was also partially supported by the National Natural Science Foundation of China under grant 61003300 and the 111 Project under grant B08038.

M. Pan and Y. Fang are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: miaopan@ufl.edu; fang@ece.ufl.edu).

J. Sun is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996 USA (e-mail: jysun@utk.edu).

Digital Object Identifier 10.1109/JSAC.2011.110417.

still rational and risk neutral, bidders do not have incentive to bid arbitrarily high or low with the concern of overpayment or losing in an auction [17]. 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 values [12], [23]. 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 [11], which shows that it is not always right 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 [11]. As a possible solution, they group the nodes with negligible interference together as virtual bidders, trim the multi-winner spectrum auction [11] into a traditional single-winner auction, and then split the payment or revenue among the participating bidders using game theory. However, it should be noted that the issue of group partition itself is NP-complete in terms of the spatial reuse [22].

Aside from truthfully bidding and collusion among the bidders, a secure spectrum auction design should also consider the frauds of the insincere auctioneer (i.e., the auctioneer overcharges the winning bidders with the forged price) and the bid-rigging between the bidders and the auctioneer (i.e., the auctioneer colludes with greedy bidders to manipulate the auction)[1]. A combination of interference consideration and cryptographic techniques allows us to provide a novel secure spectrum auction scheme, *THEMIS*[2], to purge these possible back-room dealing. The major contributions of the proposed auction are listed as follows:

1) *THEMIS* supports spectrum bands with diverse characteristics other than the bands only with uniform characteristics in previous works [8], [11], [21].
2) *THEMIS* provides an effective procedure to auction the spectrum bands with consideration of the interference constraints. To counter the NP-completeness of spectrum allocation in view of the frequency reuse, *THEMIS* divides 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, and a bidder is able to update his conflict-table and broadcast the spectrum occupancy information to his neighbors when detecting changes of the environment.
3) *THEMIS* leverages Paillier cryptosystem [24], [25] 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. In this way, the auctioneer could compute and reveal the results of spectrum auction, while the actual bidding values of the bidders are kept secret from the other bidders and even from the auctioneer himself.
4) *THEMIS* secures the spectrum auction effectively against the back-room dealing with limited communication and computational complexity. Our simulation results show that *THEMIS* achieves similar performance compared with existing insecure auction designs in terms of spectrum utilization, the revenue of the auctioneer, and bidders' satisfactory degree.

[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. In addition, the fraud and big-rigging are formally defined in Sec. II-B.

[2]*THEMIS* is an ancient Greek goddess who is a blind-folded lady holding a sword and a set of scales as shown in Fig. 1. *THEMIS* is world-widely referred as the symbol of truth and justice.

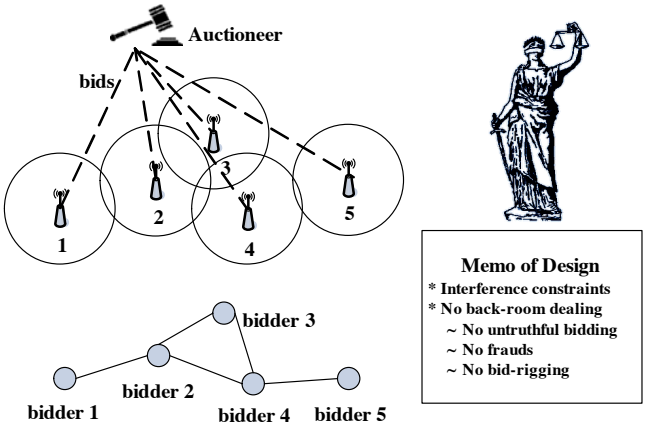


Fig. 1. System architecture, conflict graph, and secure spectrum auction memo.

The remainder of the paper is organized as follows. In Section II, system model is outlined and design challenges are described. VCG auction and Paillier cryptosystem are introduced as the fundamentals in Section III. In Section IV, the procedure and encryption design of *THEMIS* are illustrated. The performance analysis is presented in Section V. Finally, concluding remarks are drawn in Section VI.

II. System Model

A. Overview

We consider a typical spectrum auction setting, where one auctioneer auctions his unutilized spectrum bands $\mathcal{S} = \{1, 2, ..., s\}$ to $\mathcal{N} = \{1, 2, ..., n\}$ nodes/bidders located in the geographic region. The available $\mathcal{S}$ spectrum bands are supposed to have different characteristics to different nodes (in the sequel, we use the words nodes and bidders interchangeably) in terms of the frequency of the available band, the segment type of the band (i.e., contiguous segment or discontinuous one), the location of the bidders, etc. [26]–[28], so that bidders may submit different bids for different combinations of the spectrum bands. Considering the frequency reuse [21], [22], 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 [29] or protocol model [30] as described in [8], [9], [11], [21]. As shown in Fig. 1, the edges stand for mutual interference between corresponding nodes. Moreover, we assume

that spectrum auctions take place periodically[3], the bidders are static in each period, and there is a common channel[4] for necessary information exchanges between the auctioneer and bidders.

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

- *Bidder Set* ($\mathcal{N}$) – $\mathcal{N} = \{1, 2, ..., n\}$ represents the set of n bidders.
- *Spectrum Band Set* ($\mathcal{S}$) – $\mathcal{S} = \{1, 2, ..., s\}$ is the set of s available spectrum bands.
- *Allocation Set* ($\mathcal{N}^{\mathcal{S}}$) – $\mathcal{N}^{\mathcal{S}} = \{\lambda : \mathcal{S} \rightarrow \mathcal{N}\}$ denotes the set of allocations of spectrum bands $\mathcal{S}$ to bidders $\mathcal{N}$. For instance, for $\mathcal{N} = \{1, 2\}$ and $\mathcal{S} = \{1\}$, $\mathcal{N}^{\mathcal{S}} = \{\lambda_1 = (\{1\}, \{\}), \lambda_2 = (\{\}, \{1\})\}$, e.g., $(\{1\}, \{\})$ denotes that spectrum band 1 is allocated to bidder 1 and nothing to bidder 2.
- *Bidding Values* (b_i) – b_i indicates the bidding values of node i for certain allocation set, e.g., for $\mathcal{N}^{\mathcal{S}} = \{\lambda_1 = (\{1\}, \{\}), \lambda_2 = (\{\}, \{1\})\}$, $b_1 = (1, 0)$ and $b_2 = (0, 2)$ indicate that node 1 bids 1 for the allocation λ_1 and 0 for λ_2, and node 2 bids 2 for the allocation λ_2 and 0 for λ_1.
- *Evaluation Values* (v_i) – v_i represents the true evaluation values of node i for certain allocation set. In case that the auction is incentive compatible, v_i equals to b_i.
- *Charging Price* (p_i) – p_i is the price charged by the auctioneer for allocating the spectrum bands to winning bidder i. This charging price might be different among bidders, and the charging mechanisms are different over various allocations as well.
- *Bidder's Utility* (u_i) – u_i stands for the budget balance of bidder i. It is defined as $u_i(\lambda) = v_i(\lambda) - p_i$ for the specific allocation λ.
- *Auctioneer's Revenue* (R) – R denotes the monetary gains of the auctioneer. It is simply expressed as $R = \sum_1^n p_i$.

B. Design Challenges

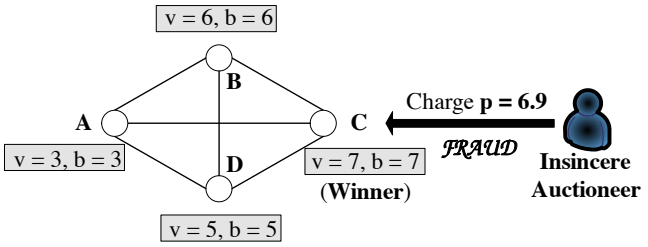
To preclude the threats from untruthful spectrum auction bidders, sealed secondary price auction or VCG auction seems to be the most favorite choice, as mentioned in the introduction. However, based on trusted auctioneer, this type of auction is vulnerable to the frauds of the auctioneer and not bid-rigging resistant.

***Definition** 1: A fraud is a deception made by the insincere auctioneer. The auctioneer commits frauds by overcharging the winning bidders with the forged price for his personal monetary gain, which damages the utility of the corresponding winners in the spectrum auction.*

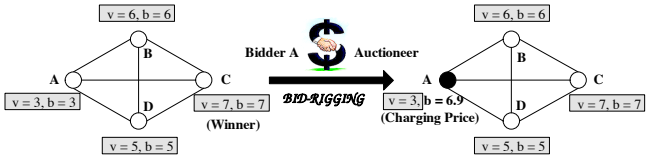
***Definition** 2: Bid-rigging in the spectrum auction is a form of collusion between the auctioneer and the bidders, where insincere auctioneer conspires with greedy bidders to illegally fix the price, share the spoils, and manipulate the auctions.*

[3]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 [31]. 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.

[4]It is like the common control channel (CCC) proposed in [2], or the common pilot channel (CPC) in [32].



(a) Frauds of the insincere auctioneer



(b) Bid-rigging between the auctioneer and the bidders

Fig. 2. Challenges to secure spectrum auction design

To be specific, we take the scenario shown in Fig. 2 for example, where only one spectrum band is available for auction[5]. In Fig. 2(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. 2(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.

Therefore, to purge these potential back-room dealing, an ideal spectrum auction should allow the auctioneer to make the appropriate decision of allocating spectrum bands and publish only the results of the auction, i.e., winners and their payments, while the bidding values must be kept secret even from the auctioneer.

III. Preliminaries

A. VCG Auction

As one of the most widely used auction schemes, VCG auction is proved to be individual rational, Pareto efficient, and incentive compatible [14]. 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. Details of VCG auction are as follows.

[5]VCG is equivalent to the sealed secondary price auction for the single spectrum band auction.

To distinguish from the notations in *THEMIS*, we substitute $\mathcal{S} = \{1, 2, 3, ..., s\}$ with $\mathcal{G} = \{1, 2, 3, ..., g\}$ for illustrative purposes in this subsection.

Bidding: Each bidder i submits his sealed bidding vector b_i for all the possible allocations $\lambda \in \mathcal{N}^{\mathcal{G}}$.

Allocation: The auctioneer selects a Pareto efficient allocation $\lambda^* \in \mathcal{N}^{\mathcal{G}}$ based on the truthful bidding values. That is

$$\lambda^* = \underset{\lambda \in \mathcal{N}^{\mathcal{G}}}{\operatorname{argmax}} \Big(\sum_i b_i(\lambda) \Big). \tag{1}$$

Then, the goods are assigned according to λ^*.

Charging: Assume $\lambda^*_{\sim i}$ is an allocation without node i satisfying the following inequality

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

Then, the payment of bidder i is defined as

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

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

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

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

$$\sum_i b_i(\lambda^*) \geq \sum_i b_i(\lambda), \quad \forall \lambda \in \mathcal{N}^{\mathcal{G}}, \tag{5}$$

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

Even though VCG auction has several good properties, it cannot be directly extended to spectrum auction because of the following two issues:

1) VCG requires the solution to the optimal allocation, which is NP-complete in spectrum auction w.r.t. the spatial reuse.
2) VCG is vulnerable to the frauds of the insincere auctioneer and the bid-rigging between the bidders and the auctioneer.

B. Paillier Cryptosystem

In order to thwart the back-room dealing and allocate the spectrum bands, bidding values should be kept secret. On the other hand, the auctioneer has to find the maximum bid and charge the corresponding bidder. Therefore, a cryptosystem is needed for spectrum auction, which enables the auctioneer to properly execute the auction and reveal nothing more than the resultant payments and allocation of spectrum bands.

Paillier cryptosystem is such a probabilistic[6] asymmetric public key encryption system that satisfies these requirements. The special features of Paillier cryptosystem includes homomorphic addition, indistinguishability, and self-blinding [24], [25], [33]:

- **Homomorphic addition.** Given $\mathscr{E}$ is the Paillier's encryption of a message M, $\mathscr{E}(\cdot)$ is additive homomorphic, i.e., $\mathscr{E}(M_1 + M_2) = \mathscr{E}(M_1)\mathscr{E}(M_2)$.
- **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.

These desired properties of Paillier cryptosystem are essential for our secure spectrum auction design as described in Section IV-B.

IV. Auction Design of THEMIS

Since spatial reuse of spectrum bands makes finding the optimal spectrum allocation NP-complete [8], [22], researchers resort to greedy algorithms for possible solutions [8], [11]. In order to sort the bidders for the allocation of spectrum bands, the auctioneer has to know the global information of bids in these schemes, rendering them vulnerable to frauds and bid-rigging.

In order to deal with the back-room dealing, the proposed *THEMIS* leverages Paillier cryptosystem to encrypt the bidding values and enable the auctioneer to charge the winners without leaking any information about the bidding values. In parallel with the encryption design, *THEMIS* also provides a supporting conflict-table-driven auction procedure to implement the spectrum auction. Thus, in this section, we first describe the implementation procedure of *THEMIS* to give an overall impression. Then, we dwell on the encryption design details of the proposed auction.

A. THEMIS: Spectrum Auction Procedure

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 [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, the whole network is divided into small subnetworks based on the interference range and the location of the bidders, i.e., 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. 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 (especially for the nodes in the crossing

[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.

area of different subnetworks) when taking the interference constraints into account.

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

Step 1. Preparation:

Let $\mathcal{N} = \{1, 2, \cdots, i, \cdots, n\}$ be the set of n bidders, $\mathcal{S} = \{1, 2, \cdots, j, \cdots, s\}$ be the set of s spectrum bands, and $\mathcal{N}^{\mathcal{S}} = \{\lambda : \mathcal{S} \rightarrow \mathcal{N}\}$ be the set of possible allocations of spectrum bands to bidders. Each bidder sets up two tables, a conflict-table for storing the nodes causing mutual interference and a price-charged table for storing 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, he encloses his identity, location information and his own bidding values b_i for $\mathcal{N}^{\mathcal{S}}$ allocations into his bid, where 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 encrypted using Paillier cryptosystem (How to encrypt b_i is elaborated in the next subsection). Then, bidders submit their bids to the auctioneer.

Step 2. Start-up:

Due to the NP-completeness of spectrum allocation, there is no 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.

Step 3. 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 j-th node away from the center i in terms of distance.

Step 4. Subnetwork Auction:

After indexing the bidders, the auctioneer collects the bids and carries out the secure spectrum auction within the subnetwork using Paillier cryptosystem. The results of the subnetwork auction, i.e., the set of winners and the set of corresponding charging prices, are published. Details of encryption design for the secure subnetwork spectrum auction are elaborated in Section IV-B.

Step 5. Allocation & Payment:

Depending on both subnetwork auction results and location of the winners, the allocation of spectrum bands and the payment vary 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 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 allocation λ, he will compare the current charging price p_i with the previous charging prices, $\mathcal{P}_\lambda$, stored in his price-charged table and pay the highest one of all the prices for the allocation λ. That is to say, the payment for the center node i is $\max(\mathcal{P}_\lambda)$[7]. Then, the center node updates 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 due to computational efficiency.

Algorithm 1 THEMIS - *Spectrum Allocation Procedure*

```
i = randomch(N)
while N! = φ do
    set up the subnetwork centered at i
    D = sorted N by distance to i
    auction S securely within the subnetwork
    if i ∉ W then
        N = N \ {i}
        i = min(D)
        continue
    else
        allocate(i, λ, max(P_λ))
        N = N \ {i}
        W = W \ {i}
        if W == φ then
            i = min(D)
            continue
        else
            i = min(D ∩ W)
        end if
    end if
end while
```

The overall spectrum auction procedure of *THEMIS* is summarized in Alg. 1.

B. THEMIS : Secure Spectrum Auction Design

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. Assuming the only information that the auctioneer can exploit is the subnetwork auction winners and their corresponding payments, there is no way for him to conduct any frauds or bid-rigging to manipulate the market. So, in the encryption design part of *THEMIS*, we

[7]Paying $\max(\mathcal{P}_\lambda)$ is to guarantee the center, bidder i, to beat other competitors in the previous subnetwork auctions, where i is not the center.

elaborate on how to represent the bidding values, how to entitle the auctioneer to select the maximum from the encrypted bids, how to reveal the charging prices for the winners, and how to establish the subnetwork auction resistant to back-room dealing.

1) Representation of Bidding Values:

Bidding Value Encryption.

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

$$\mathbf{e}(k) = (e^1, \cdots, e^q) = (\underbrace{\mathscr{E}(x), \cdots, \mathscr{E}(x)}_{k}, \underbrace{\mathscr{E}(0), \cdots, \mathscr{E}(0)}_{q-k}), \quad (6)$$

where $\mathscr{E}(0)$ and $\mathscr{E}(x)$ account for the Paillier 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 the allocation of available spectrum bands. For instance, assuming $q = 3$ and $k = 2$ for given spectrum allocation λ, $\mathbf{e}(k) = \mathbf{e}(2) = \big(\mathscr{E}(x), \mathscr{E}(x), \mathscr{E}(0)\big)$.

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

$$\prod_i \mathbf{e}(k_i) = (\prod_i e_i^1, \cdots, \prod_i e_i^q). \quad (7)$$

Due to the homomorphic addition of Paillier cryptosystem, the j-th component of the vector above can be denoted as

$$y_j = \prod_i e_i^j = \mathscr{E}^{c(j)}(x) = \mathscr{E}(c(j)x), \quad (8)$$

where $c(j) = |\{i | j \leq k_i\}|$ 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 value for the spectrum allocation λ.

Bid Randomization.

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

$$\mathbf{e}'(k + r) = (\underbrace{\mathscr{E}(x), \cdots, \mathscr{E}(x)}_{r}, e_1', \cdots, e_{q-r}'), \quad (9)$$

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. self-blinding property of Paillier cryptosystem. Moreover, it should be noted that during randomizing and constant adding 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.

2) Secure Subnetwork Spectrum Auction: Representing bids by encrypted vectors based on Paillier cryptosystem, we can easily find the maximum of the given bids and randomize the bidding values without knowing these values themselves, which paves the way to the secure computation of the VCG based spectrum auction in the subnetwork.

For the simplicity of description, we use $\mathbf{E}(f)$ to denote the encrypted vector of bidding values, where f is a function from $\mathcal{N}^{\mathcal{S}}$ to the vector of bidding values. The proposed secure subnetwork spectrum auction is as follows.

Initial Phase:

The auctioneer[8] generates his private and public key of Paillier cryptosystem, and publishes the public key and public element $x (x \neq 0)$ over the common channel.

Bidding Phase:

Step 1: Each bidder z decides his vector of bidding values b_z for $\mathcal{N}^{\mathcal{S}}$. Since the subnetwork spectrum auction is VCG based, $b_z(\lambda)$, $\forall \lambda \in \mathcal{N}^{\mathcal{S}}$, is also the true evaluation value of bidder z for the allocation λ.

Step 2: The auctioneer creates $(n+1)$ representing vectors $\mathbf{E}_\xi = \mathbf{E}(O), \mathbf{E}_1 = \mathbf{E}(O), \cdots, \mathbf{E}_n = \mathbf{E}(O)$, where the size of vector $\mathbf{E}$ is equal to $|\mathcal{N}^{\mathcal{S}}|$, and the initial $O(\lambda)$ is always equal to 0.

Step 3: Each bidder z adds his encrypted bidding value vector b_z to the representing vectors $\mathbf{E}_\xi, \mathbf{E}_1, \cdots, \mathbf{E}_{z-1}$, $\mathbf{E}_{z+1}, \cdots, \mathbf{E}_n$ except the z-th representing vector $\mathbf{E}_z$ to keep b_z secret. When all bidders have finished this process, the auctioneer obtains

$$\mathbf{E}_\xi = \Big(\prod_i \mathbf{e}\big(b_i(\lambda_1)\big), \prod_i \mathbf{e}\big(b_i(\lambda_2)\big), \cdots, \prod_i \mathbf{e}\big(b_i(\lambda_{|\mathcal{N}^{\mathcal{S}}|})\big)\Big). \quad (10)$$

According to the homomorphic addition property of Paillier cryptosystem, the equation above can be rewritten as

$$\begin{aligned}\mathbf{E}_\xi &= \Big(\mathbf{e}\big(\sum_i b_i(\lambda_1)\big), \mathbf{e}\big(\sum_i b_i(\lambda_2)\big), \cdots, \mathbf{e}\big(\sum_i b_i(\lambda_{|\mathcal{N}^{\mathcal{S}}|})\big)\Big) \\ &= \mathbf{E}(\sum_i b_i). \end{aligned} \quad (11)$$

Similarly, the auctioneer also has

$$\mathbf{E}_z = \mathbf{E}(\sum_{i \neq z} b_i) \quad z = 1, 2, \cdots, n. \quad (12)$$

Opening Phase:

The 5-step opening phase of subnetwork auction consists of two parts: allocation selection and charging price calculation.

I. Allocation Selection

Step 1: The auctioneer derives $\mathbf{E}(\sum_i b_i + R)$ from $\mathbf{E}_\xi$ by adding a random constant function $R(\lambda) = r$ to mask the

[8]In fact, the auctioneer should be implemented by plural servers to prevent the auctioneer from learning the bidding values. Indeed, the decryption to find the maximum combination of the bids and the addition of random mask constant r in the following design are performed in a distributed manner by these servers. 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 [34]–[36] for the details about secret sharing designs.

values. With $\mathbf{E}(\sum_i b_i + R)$, the auctioneer can find masked maximum sum value of the bids

$$m = \max_{\lambda \in \mathcal{N}^{\mathcal{S}}} (\sum_i b_i(\lambda) + R(\lambda)) = \max_{\lambda \in \mathcal{N}^{\mathcal{S}}} (\sum_i b_i(\lambda)) + r. \quad (13)$$

To be more specific, the auctioneer takes the product of the encrypted elements in $\mathbf{E}_\xi$ to obtain $\prod_{j=1}^{|\mathcal{N}^{\mathcal{S}}|} \mathbf{e}(\sum_{i=1}^{n} b_i(\lambda_j)+r)$, and makes use of **Maximum Bid Selection** to determine the maximum element of $\prod_{j=1}^{|\mathcal{N}^{\mathcal{S}}|} \mathbf{e}(\sum_{i=1}^{n} b_i(\lambda_j)+r)$, whose value is $m = \max_{\lambda \in \mathcal{N}^{\mathcal{S}}} (\sum_i b_i(\lambda) + R(\lambda))$.

Step 2: The auctioneer then decrypts the m-th element of every vector $\mathbf{e}(\sum_i b_i(\lambda)+R(\lambda))$ in $\mathbf{E}_\xi$, i.e., for any allocation $\lambda \in \mathcal{N}^{\mathcal{S}}$, and finds out whether the decryption is equal to x or equal to 0. If it is equal to x at allocation $\lambda^* \in \mathcal{N}^{\mathcal{S}}$, the auctioneer regards λ^* as the allocation that maximizes $\sum_i b_i$, the sum of all bidding values. The allocation λ^* is the result of the subnetwork auction. Correspondingly, the winner set is determined by λ^*.

II. Charging Price Calculation

The auctioneer then computes the charging price p_z of bidder z as shown in Step 3 to Step 5.

Step 3: The auctioneer derives $\mathbf{e}(\sum_{i \neq z} b_i(\lambda^*)+r')$ from the element $\mathbf{e}(\sum_{i \neq z} b_i(\lambda^*))$ of $\mathbf{E}_z$ by adding a random constant r' to mask the value. Then, the auctioneer decrypts and finds out the masked value of $(\sum_{i \neq z} b_i(\lambda^*) + r')$.

Step 4: The auctioneer derives $\mathbf{E}(\sum_{i \neq z} b_i + R')$ from $\mathbf{E}_z$ by adding random constant function $R'(\lambda) = r'$ to mask the values. Similar to ***Step 1***, the auctioneer takes the product of the Paillier encrypted elements in $\mathbf{E}(\sum_{i \neq z} b_i + R')$, and employs **Maximum Bid Selection** to find out the masked maximum, $\max_{\lambda \in \mathcal{N}^{\mathcal{S}}} (\sum_{i \neq z} b_i(\lambda) + r')$. By the definition of $\lambda^*_{\sim x}$, $\max_{\lambda \in \mathcal{N}^{\mathcal{S}}} (\sum_{i \neq z} b_i(\lambda)+r')$ is equal to $(\sum_{i \neq z} b_i(\lambda^*_{\sim z})+ r')$.

Step 5: After that, the auctioneer calculates the charging price by subtracting these masked values.

$$p_z = \Big(\sum_{i \neq z} b_i(\lambda^*_{\sim z}) + r'\Big) - \Big(\sum_{i \neq z} b_i(\lambda^*) + r'\Big). \quad (14)$$

In consistent with the allocation λ^*, bidder z should be charged with p_z for spectrum bands he won in this subnetwork auction.

C. THEMIS: An Example

To make better understanding of the proposed *THEMIS*, we illustrate it with an example, where $\mathcal{S} = \{1, 2\}$ and $\mathcal{N} = \{1, 2, 3, 4\}$, in a simplified topology reflecting the typical interference constraints as depicted in Fig. 3(a).

In *THEMIS*, the overall network in Fig. 3(a) can be substituted with four subnetworks based on the number of the nodes and their mutual interference. Since Subnetwork $\underline{3}$ and Subnetwork $\underline{4}$ are symmetric with the same bidding nodes and available spectrum resource, they can be combined into one subnetwork. Hence, the network can be decomposed into three subnetworks and the spectrum auction is executed in these subnetworks consecutively like the abstract state machine as shown in Fig. 3(b).

As for Subnetwork $\underline{1}$, node 1 has no conflicts with node 3 and 4 but node 2. The competition for spectrum bands is between node 1 and 2. Therefore, the set of bidders is $\mathcal{N} = \{1, 2\}$, and the set of available spectrum bands is $\mathcal{S} = \{1, 2\}$. So,

$$\mathcal{N}^{\mathcal{S}}_{\underline{1}} = \{\lambda_1 = (\{1, 2\}, \{\}), \lambda_2 = (\{1\}, \{2\}), \lambda_3 = (\{2\}, \{1\}), \lambda_4 = (\{\}, \{1, 2\})\},$$

where, e.g., $\lambda_2 = (\{1\}, \{2\})$ indicates that spectrum band 1 is allocated to bidder 1 and band 2 to bidder 2. Assume the truthful bidding values b_1 and b_2 of bidder 1 and 2 are $b_1 = (3, 2, 2, 0)$ and $b_2 = (0, 0, 2, 3)$, respectively. Then, we obtain

$$b_1 + b_2 = (3, 2, 4, 3).$$

The auctioneer creates $\mathbf{E}_\xi$, $\mathbf{E}_1$, and $\mathbf{E}_2 = \mathbf{E}(O) = (\mathbf{e}(0), \mathbf{e}(0), \mathbf{e}(0), \mathbf{e}(0))$. Then, bidders use Paillier cryptosystem to encrypt their bids. Bidder 1 adds his bidding values to $\mathbf{E}_\xi$, $\mathbf{E}_2$ and bidder 2 adds his values to $\mathbf{E}_\xi$, $\mathbf{E}_1$, i.e.,

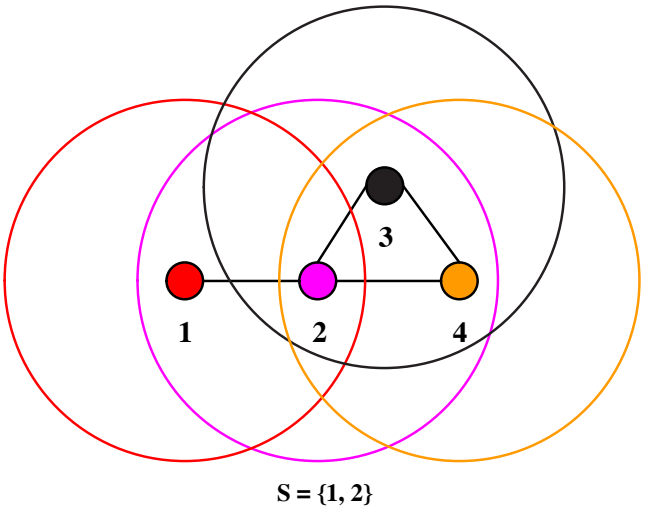
$$\mathbf{E}_\xi = (\mathbf{e}(3), \mathbf{e}(2), \mathbf{e}(4), \mathbf{e}(3)),$$
$$\mathbf{E}_1 = (\mathbf{e}(0), \mathbf{e}(0), \mathbf{e}(2), \mathbf{e}(3)),$$
$$\mathbf{E}_2 = (\mathbf{e}(3), \mathbf{e}(2), \mathbf{e}(2), \mathbf{e}(0)).$$

First, the auctioneer should find the allocation of spectrum bands in Subnetwork $\underline{1}$.

The auctioneer adds random constant function $R(\lambda) = r = 2$ to $\mathbf{E}_\xi$, which leads to

$$\mathbf{E}(\sum_i b_i + R) = (\mathbf{e}(3+2), \mathbf{e}(2+2), \mathbf{e}(4+2), \mathbf{e}(3+2)).$$

The auctioneer takes the product of all elements in $\mathbf{E}(\sum_i b_i + R)$, $\big(\mathbf{e}(3+2) \cdot \mathbf{e}(4+2) \cdot \mathbf{e}(2+2) \cdot \mathbf{e}(3+2)\big)$, which can also



(a) The topology of the example.

(b) Subnetwork decomposition for spectrum auctions.

Fig. 3. An illustrative example for THEMIS.

be interpreted as

$$\big(\mathscr{E}(4x),\mathscr{E}(4x),\mathscr{E}(4x),\mathscr{E}(4x),\mathscr{E}(3x),\mathscr{E}(x),\underbrace{\mathscr{E}(0),\cdots,\mathscr{E}(0)}_{q-(4+2)}\big).$$

Then, the auctioneer decrypts this vector to find $\max_{\lambda\in\mathcal{N}_{\underline{1}}^{\mathcal{S}}}(\sum_{i=1,2} b_i(\lambda)+r) = 4+2$. After that, the auctioneer decrypts the $(4+2)$-th element of $\mathbf{e}(3+2), \mathbf{e}(2+2), \mathbf{e}(4+2), \mathbf{e}(3+2)$ to determine $\lambda^* = \lambda_3$.

Next, the auctioneer should calculate the charging prices for the winners in Subnetwork $\underline{1}$.

The auctioneer adds random constant $r^{'} = 1$ to the 3-rd element $\mathbf{e}(2)$ of $\mathbf{E}_1$ to yield

$$\mathbf{e}(\sum_{i\neq 1} b_i(\lambda^*) + r^{'}) = \mathbf{e}(2+1),$$

and decrypts $\mathbf{e}(2+1)$ to find $\big(\sum_{i\neq 1} b_i(\lambda^*) + r^{'}\big) = b_2(\lambda_3) + r^{'} = 2+1$.

Then, the auctioneer adds random constant function $R^{'}(\lambda) = r^{'} = 1$ to $\mathbf{E}_1$ to yield

$$\mathbf{E}(\sum_{i\neq 1}(b_i) + R^{'}) = (\mathbf{e}(0+1), \mathbf{e}(0+1), \mathbf{e}(2+1), \mathbf{e}(3+1)),$$

takes the product of $\big(\mathbf{e}(0+1)\cdot\mathbf{e}(2+1)\cdot\mathbf{e}(0+1)\cdot\mathbf{e}(3+1)\big)$, and then decrypts this to find $\max\big(\sum_{i\neq 1}(b_i) + R^{'}\big) = \big(\sum_{i\neq 1} b_i(\lambda^*_{\sim 1}) + r^{'}\big) = b_2(\lambda_4) + r^{'} = 3+1$.

According to ***Step 5*** in opening phase of the subnetwork spectrum auction, $p_1 = b_2(\lambda_4) - b_2(\lambda_3)$. Thus, the auctioneer calculates $p_1 = (b_2(\lambda_4)+r^{'}) - (b_2(\lambda_3)+r^{'}) = (3+1)-(2+1) = 3-2 = 1$. The auctioneer can also compute $p_2 = 3-2 = 1$ in the same way. Consequently, in terms of spectrum auction in Subnetwork $\underline{1}$, spectrum band 2 is allocated to bidder 1 at the price of 1, and spectrum band 1 is allocated to bidder 2 at the price of 1.

However, the spectrum allocation of bidder 2 is determined not only by the interference between node 2 and 1, but also by the interference between node 2 and node 3, as well as node 4. So, whether available spectrum band 1 should be allocated to bidder 2 and how much the charging price is cannot be determined until the auctioneer finishes the auction in Subnetwork $\underline{2}$ centered at node 2. Before the auction in Subnetwork $\underline{2}$ starts, bidder 1 should update his bid information, i.e., broadcasting his spectrum occupancy and location information to his neighbors to notify them which bands are taken within his interference range.

As a result, the nodes within Subnetwork $\underline{2}$ are only able to bid for the left spectrum band 1 subject to the interference constraints. In this way, bidder 1 and his interference to bidder 2 can be ignored, so that node 1 can be deleted both from the conflict-table of bidder 2 and from the bidder list of auction in Subnetwork $\underline{2}$ as shown in Fig. 3(b).

Meanwhile, nodes in Subnetwork $\underline{2}$ have to renew their bids for the available spectrum band 1. Hence, the set of the bidders in Subnetwork $\underline{2}$ is $\mathcal{N} = \{2,3,4\}$, the spectrum band set is $\mathcal{S} = \{1\}$, and the allocation set can be represented as

$$\mathcal{N}_{\underline{2}}^{\mathcal{S}} = \{\lambda_1 = (\{1\},\{\},\{\}), \lambda_2 = (\{\},\{1\},\{\}), \lambda_3 = (\{\},\{\},\{1\})\}.$$

Similar to auction in Subnetwork $\underline{1}$, e.g., $\lambda_2 = (\{\},\{1\},\{\})$ stands for allocating available spectrum band 1 to bidder 3 and no spectrum bands to bidder 2 or bidder 4. Suppose the bidding values b_2, b_3 and b_4 of bidder 2, 3, and 4 are $b_2 = (3,0,0)$, $b_3 = (0,2,0)$, and $b_4 = (0,0,1)$, respectively. The sum of the bidders is $(b_2+b_3+b_4) = (3,2,1)$.

First, the auctioneer makes $\mathbf{E}_\xi$, $\mathbf{E}_2$, $\mathbf{E}_3$, and $\mathbf{E}_4 = (\mathbf{e}(0),\mathbf{e}(0),$
$\mathbf{e}(0))$. Bidder 2 adds his bids to $\mathbf{E}_\xi$, $\mathbf{E}_3$, and $\mathbf{E}_4$, bidder 3 adds his bid to $\mathbf{E}_\xi$, $\mathbf{E}_2$, and $\mathbf{E}_4$, and bidder 4 adds his bid to $\mathbf{E}_\xi$, $\mathbf{E}_2$ and $\mathbf{E}_3$, which leads to

$$\begin{aligned}\mathbf{E}_\xi &= (\mathbf{e}(3),\mathbf{e}(2),\mathbf{e}(1)),\\ \mathbf{E}_2 &= (\mathbf{e}(0),\mathbf{e}(2),\mathbf{e}(1)),\\ \mathbf{E}_3 &= (\mathbf{e}(3),\mathbf{e}(0),\mathbf{e}(1)),\\ \mathbf{E}_4 &= (\mathbf{e}(3),\mathbf{e}(2),\mathbf{e}(0)).\end{aligned}$$

Then, the auctioneer adds random constant function $R(\lambda)$ to $\mathbf{E}_\xi$, takes the product of elements in $\mathbf{E}_\xi$ and decrypts this to find $\max_{\lambda\in\mathcal{N}_{\underline{2}}^{\mathcal{S}}}(\sum_{i=2,3,4} b_i(\lambda) + R(\lambda))$. After that, the auctioneer decrypts the corresponding max-th element of $\big(\mathbf{e}(3+R(\lambda)),\mathbf{e}(2+R(\lambda)),\mathbf{e}(1+R(\lambda))\big)$ to find $\lambda^* = \lambda_1$.

Then, the auctioneer adds random constant $R^{''}(\lambda) = r^{''} = 2$ to the 1-st component $\mathbf{e}(0)$ of $\mathbf{E}_2$ to obtain $\mathbf{e}(\sum_{i=3,4} b_i(\lambda^*) + r^{''}) = \mathbf{e}(0+2)$, and decrypts $\mathbf{e}(0+2)$ to find $\big(\sum_{i=3,4} b_i(\lambda^*) + r^{''}\big) = b_3(\lambda_1) + b_4(\lambda_1) + r^{''} = 0+2$.

The auctioneer adds random constant function $R^{''}(\lambda) = r^{''} = 2$ to $\mathbf{E}_2$ to yield

$$\mathbf{E}(\sum_{i=3,4} b_i + R^{''}) = (\mathbf{e}(0+2),\mathbf{e}(2+2),\mathbf{e}(1+2)).$$

The auctioneer takes the product of $\big(\mathbf{e}(0+2)\cdot\mathbf{e}(2+2)\cdot\mathbf{e}(1+2)\big)$, and decrypts this vector to find $\max(\sum_{i=3,4} b_i + R^{''}) = \sum_{i\neq 2} b_i(\lambda^*_{\sim 2}) + r^{''} = b_3(\lambda_2) + b_4(\lambda_2) + r^{''} = 2+2$.

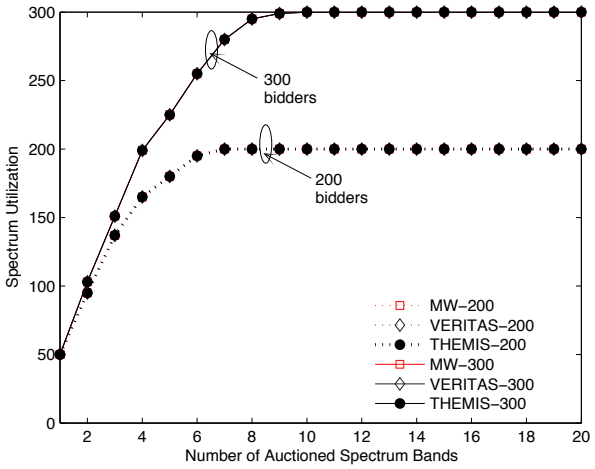
Finally, the auctioneer calculates $p_2 = [b_3(\lambda_2) + b_4(\lambda_2) + r^{''}] - [b_3(\lambda_1) + b_4(\lambda_1) + r^{''}] = (2+2) - (0+2) = 2-0 = 2$. For Subnetwork $\underline{2}$, spectrum band 1 is allocated to bidder 2, and spectrum band 2 is not vacant. Furthermore, since node 2 lies in the crossing area of Subnetwork $\underline{1}$ and Subnetwork $\underline{2}$, his payment for the spectrum band 1 should be $p_2 = \max\{p_{(2,\underline{1})}, p_{(2,\underline{2})}\} = \max\{1,2\} = 2$.

In Subnetwork $\underline{3}$, all these processes are repeated, and node 3 and 4 are charged in the same manners.

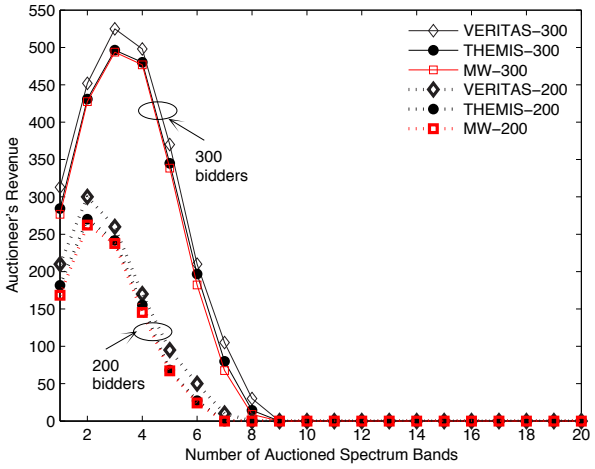
V. Simulation and Analysis

Compared with two existing spectrum auction schemes, *VERITAS* [8] and the Multi-Winner spectrum auction (*M-W*) [11], *THEMIS* beats two unsolved challenges of secure spectrum auction design, i.e., the frauds of the insincere auctioneer and the bid-rigging between bidders and auctioneer. Leveraging subnetwork division and Paillier cryptosystem encrypted subnetwork auction, the proposed *THEMIS* is resistant to these two back-room dealing, while it supports spatial reuse, attracts risk neutral bidders, and guarantees strategy-proof bidding.

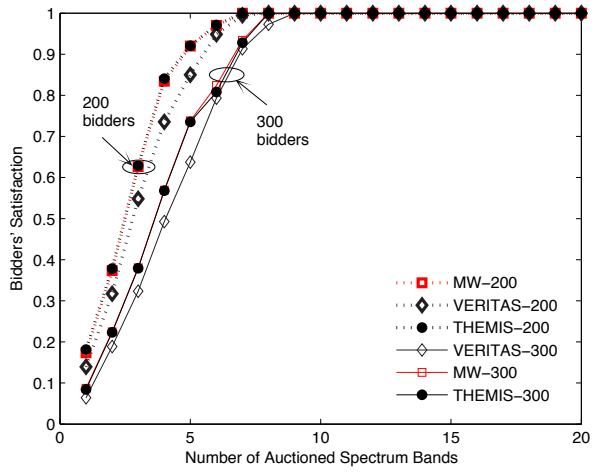
In this section, we also show that *THEMIS* achieves similar performance to *VERITAS* and *M-W* in terms of spectrum utilization, auctioneer's revenue, and bidders' satisfactory degree. Besides, we carry out the security analysis of *THEMIS* and demonstrate the efficiency of the proposed spectrum auction by evaluating its communication and computational complexity.



(a) Spectrum Utilization



(b) Revenue of the Auctioneer



(c) Bidders' Satisfaction

Fig. 4. Performance comparison of *THEMIS*, *VERITAS* and *M-W*

A. Performance Comparison

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 [37], [38]. 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, we let each bidder request only one spectrum band.

We use the following three performance metrics to compare *THEMIS* with *VERITAS* and *M-W*.

- *Spectrum Utilization:* It is the sum of allocated spectrum bands of all the winning bidders, which is the same as the definition in [8].
- *Auctioneer's Revenue:* It is the sum of payments of all the winning bidders, as defined in Section II.
- *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.

2) Results and Analysis: When we compare the performance of *THEMIS* with that of *VERITAS* or *M-W*, we assume all the auctions are collusion-free, and there are not any frauds or bid-rigging. In Fig. 4, we plot the spectrum utilization, auctioneer's revenue, and bidder's satisfaction of the three auction designs with 200 bidders and 300 bidders, respectively.

In Fig. 4(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 three auctions. It is not surprising that the performance results of *THEMIS*, *VERITAS* and *M-W* are the same in terms of spectrum utilization, because they mainly differ in their price charging designs if all the possible back-room dealing could be neglected.

In Fig. 4(b), we find that *THEMIS* and *M-W* are almost the same in terms of the auctioneer's revenue, and *THEMIS* is slightly higher than *M-W* at only a few points. It makes sense because *THEMIS* 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 is a single item [12]. Therefore, the performance results of *THEMIS* and *M-W* are quite similar in our simulations. The bump of *THEMIS* over *M-W* is from the payments for the winning bidders located in the crossing area, as we illustrated in Section IV-A. In addition, *VERITAS* is characterized by charging the winners with their *critical neighbor* prices [8], which make it perform a little bit better than the other two schemes in the auctioneer's revenue.

On the other hand, in Fig. 4(c), *VERITAS* loses his advantages correspondingly, and *THEMIS* and *M-W* outperform it in bidders' satisfactory degree. Actually, the auctioneer's revenue and bidders' satisfactory degree are just two complementary evaluation metrics.

From the comparison and analysis above, we show that *THEMIS* sacrifices nothing in performance when guaranteeing the spectrum auction secure.

B. Security Analysis

Before presenting our security analysis of *THEMIS*, we must re-emphasize and clarify two properties of Paillier cryptosystem. First, due to the indistinguishability of this encryption, no information about the value k can be leaked out

TABLE I
THE COMMUNICATION COMPLEXITY OF *THEMIS*

pattern	round	volume
the bidder $\leftrightarrow$ the auctioneer	$\mathcal{O}(n \log n)$	$\mathcal{O}\big(n \log n \times (\log n)^s \times q \log n\big)$
the bidder $\leftrightarrow$ neighbor bidders	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$

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 insincere auctioneer from learning the bids and manipulating the auction by frauds, we embodies the auctioneer by multiple servers in *THEMIS*. The decryption to determine the maximum of truthful bidding values and the addition of random mask constant r are both performed in a distributed manner by these servers, so that no insincere auctioneer can decrypt to learn about the bids or learn random mask constant r illegally. Hence, *THEMIS* can keep bids confidential except the results of the auction, i.e., the winners and their corresponding payments.

Asides from the frauds, the bid-rigging between the bidders and the auctioneer becomes meaningless because the auctioneer himself knows nothing more than the winners and their payments in *THEMIS*. Even if a certain bidder colludes with each of servers composing the auctioneer, he is not able to find out any information about the bids if the auction is carried out in a distributed manner by these servers.

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

C. Efficiency Analysis

The communication and computational complexity of *THEMIS* 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 a composing the auctioneer. 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 $\mathcal{O}(\log n)$ [38].

Table I shows the communication pattern, the order of communication rounds and the communication volume for bidders in *THEMIS*. The communication complexity from the bidder to the auctioneer is linear in terms of the number of possible bidding values q, so it may incur a heavy cost for a large range of bidding values. However, this is inevitable cost for purging the back-room dealing. Meanwhile, the communication complexity are closely related to s. Since spectrum is scare resource and the available bands cannot be arbitrarily large, s may only impose limited communication cost. Compared with conventional secure auction designs [39], [40], there is also additional communication complexity incurred by the subnetwork decomposition. But this overhead is unavoidable when we take frequency reuse into consideration in spectrum auctions.

TABLE II
THE COMPUTATIONAL COMPLEXITY OF *THEMIS*

	computational complexity
the bidder	$\mathcal{O}\big(n \log n \times (\log n)^s \times q \log n\big)$
the auctioneer	$\mathcal{O}\big(a \times n \log n \times (\log n)^s \times q \log n\big)$

Table II shows the computational complexity for the auctioneer and a bidder in *THEMIS*. Similar to the communication cost, the complexity of each bidder and the auctioneer is 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, which are inevitable but limited.

VI. CONCLUSION

In this paper, we have incorporated cryptographic technique into the spectrum auction design and proposed *THEMIS*, a secure spectrum auction scheme leveraging Paillier cryptosystem to purge the back-room dealing. Considering spectrum 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. *THEMIS* masks the bidding values of a bidder with a vector of Paillier ciphertexts, whose additive homomorphic property enables the auctioneer to find the maximum bid and calculate the charging prices securely in the subnetwork auction, while the actual bidding values are kept secret. In this case, frauds and bid-rigging becomes impossible, and manipulation of the auction is implausible. We have also shown that *THEMIS* is a secure spectrum auction with limited communication and computational complexity, and is as good as other insecure spectrum auction schemes in terms of spectrum utilization, the auctioneer's revenue, and bidders' satisfaction.

REFERENCES

[1] FCC, "Spectrum policy task force report," Report of Federal Communications Commission, Et docket No. 02-135, Nov. 2002.
[2] IEEE 802.22 Working Group on Wireless Regional Area Networks, "IEEE P802.22/D0.1 Draft Standard for Wireless Regional Area Networks: policies and procedures for operation in the TV Bands," May 2006. [Online]. Available: http://www.ieee802.org/22/
[3] J. Mitola, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D. Thesis, Royal Institute of Technology, Sweden, May 2000.
[4] I. Akyildiz, W. Lee, M. Vuran, and M. Shantidev, "Next generation/ dynamic spectrum access/ cognitive radio wireless networks: a survey," *Computer Networks (Elsevier) Journal*, vol. 50, no. 4, pp. 2127–2159, Sep. 2006.
[5] S. Sengupta and M. Chatterjee, "An economic framework for dynamic spectrum access and service pricing," *IEEE/ACM Trans. Netw.*, vol. 17, no. 4, pp. 1200–1213, Aug. 2009.
[6] M. Pan, F. Chen, X. Yin, and Y. Fang, "Fair profit allocation in the spectrum auction using the shapley value," in *Proc. IEEE Global telecommunications conference, Globecom '09*, Honolulu, HI, USA, Dec. 2009.

[7] J. Zhang and Q. Zhang, "Stackelberg game for utility-based cooperative cognitive radio networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM MobiHoc, 2009*, New Orleans, LA, May 2009.

[8] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "ebay in the sky: strategy-proof wireless spectrum auctions," in *Proc. Mobile Computing and Networking, Mobicom '08*, San Francisco, CA, Sep. 2008.

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

[10] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, "Revenue generation for truthful spectrum auction in dynamic spectrum access," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM MobiHoc, 2009*, New Orleans, LA, May 2009.

[11] Y. Wu, B. Wang, K. J. Liu, and T. Clancy, "A multi-winner cognitive spectrum auction framework with collusion-resistant mechanisms," in *Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN '08*, Chicago, IL, Oct. 2008.

[12] V. Krishna, *Auction Theory*. Academic Press, 2002.

[13] P. Klemperer, "Auction theory: a guide to the literature," *Economics Surveys*, vol. 13, no. 3, pp. 227–286, 1999.

[14] W. Vickrey, "Counter speculation, auctions, and competitive sealed tenders," *The Journal of Finance*, vol. 16, no. 1, pp. 8–37, 1961.

[15] S. Vries and R. Vohra, "Combinatorial auctions: A survey," *INFORMS Journal on Computing*, vol. 15, no. 3, pp. 284–309, 2003.

[16] P. Cramton, Y. Shoham, and R. Steinberg, *Combinatorial auctions*. MIT Press, 2006.

[17] T. Groves, "Incentives in teams," *Econometrica*, vol. 41, pp. 617–631, 1973.

[18] C.-C. Wu, C.-C. Chang, and I.-C. Lin, "New sealed-bid electronic auction with fairness, security and efficiency," *J. Computer Science and Technology*, vol. 23, no. 2, pp. 253–264, Apr. 2008.

[19] K. Peng, C. Boyd, and E. Dawson, "Batch verification of validity of bids in homomorphic e-auction," *Computer Communications*, vol. 29, no. 15, pp. 2798–2805, Sep. 2006.

[20] C. Boyd and W. Mao, "Security issues for electronic auctions," in *Proc. of the Financial Cryptography Conference FC '03*, Guadeloupe, French West Indies, Jan. 2003.

[21] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, "A general framework for wireless spectrum auctions," in *Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN '07*, Dublin, Ireland, Apr. 2007.

[22] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, "Impact of interference on multi-hop wireless network performance," in *Proc. Mobile Computing and Networking, Mobicom '03*, San Diego, CA, Sep. 2003.

[23] H. Kikuchi, "(m+1)st-price auction protocol," in *Proc. Financial Cryptography, FC '01*, Grand Cayman, British West Indies, Feb. 2001.

[24] P. Paillier, "Cryptographie à clé publique basée sur la résiduosité de degré composite," Ph.D. Thesis, École Nationale Supérieure des Télécommunications, Paris, France, Sep. 1999.

[25] ——, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. IEEE International Conference on Computational Intelligence for Modelling, Control, and Automation, EUROCRYPT '99*, Prague, Czech Republic, May 1999.

[26] Y. Xing, R. Chandramouli, and C. Cordeiro, "Price dynamics in competitive agile spectrum access markets," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 613–621, April 2007.

[27] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 192–202, Jan. 2008.

[28] D. Niyato, E. Hossain, and Z. Han, "Dynamics of multiple-seller and multiple-buyer spectrum trading in cognitive radio networks: A game theoretic modeling approach," *IEEE Trans. Mobile Comput.*, vol. 8, no. 8, pp. 1009–1022, Aug. 2009.

[29] C.-C. Chen and D.-S. Lee, "A joint design of distributed qos scheduling and power control for wireless networks," in *Proc. IEEE Conference on Computer Communications, INFOCOM '06*, Barcelona, Catalunya, Spain, April 2006.

[30] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, March 2000.

[31] L. Giupponi, R. Agusti, J. Perez-Romero, and O. S. Roig, "A novel approach for joint radio resource management based on fuzzy neural methodology," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1789–1805, May 2008.

[32] J. Perez-Romero, O. Salient, R. Agusti, and L. Giupponi, "A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation," in *Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN '07*, Dublin, Ireland, Apr. 2007.

[33] E. Goh, "Encryption schemes from bilinear maps," Ph.D. Thesis, Stanford University, USA, Sep. 2007.

[34] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Advances in Cryptology CRYPTO '91*, Santa Barbara, CA, US, Aug. 1991.

[35] A. Yao, "Protocols for secure computations," in *Proc. the 23rd Annual Symposium on Foundations of Computer Science, SFCS '82*, Washington, DC, US, 1982.

[36] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[37] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proc. ACM international symposium on Mobile ad hoc networking and computing, Mobihoc '02*, Lausanne, Switzerland, Jun. 2002.

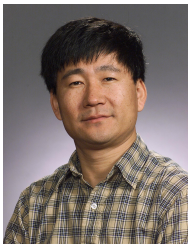
[38] F. Xue and P. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wireless Networks*, vol. 10, no. 2, pp. 169–181, 2004.

[39] M. Yokoo and K. Suzuki, "Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions," in *Proc. the first international joint conference on Autonomous agents and multiagent systems, AAMAS '02*, Bologna, Italy, Jul. 2002.

[40] ——, "Secure generalized vickrey auction without third-party servers," in *Proc. the Financial Cryptography Conference, FC '04*, Key West, FL, Feb. 2004.

Miao Pan (S'07) 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.

Jinyuan Sun (S'06) received the BSc degree in computer information systems from Beijing Information Technology Institute, China, in 2003, the MASc degree in computer networks from Ryerson University, Canada, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Florida, in 2010. She was a Network Test Developer at RuggedCom Inc., Ontario, Canada, 2005-2006. She has been an assistant professor in the Department of Electrical Engineering and Computer Science at University of Tennessee Knoxville since August 2010. Her research interests include the security protocol and architecture design of wireless networks.



Yuguang "Michael" Fang (S'92-M'97-SM'99-F'08) is a professor with University of Florida since 2005 and holds a University of Florida Research Foundation (UFRF) Professorship from 2006 to 2009. He received the NSF Career Award and ONR Young Investigator Award. He is the Editor-in-Chief for IEEE Wireless Communications and also serves/served on several editorial boards of technical journals including IEEE Transactions on Mobile Computing, IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Wireless Communications and ACM Wireless Networks.