Secure Power Scheduling Auction for Smart Grids Using Homomorphic Encryption

Haya Shajaiah, *Student Member, IEEE,* Ahmed Abdelhadi, *Senior Member, IEEE,* and Charles Clancy, *Senior Member, IEEE*

***Abstract*—In this paper, we introduce a secure energy trading auction approach to schedule the power plant limited resources during peak hours time slots. In the proposed auction model, the power plant serving a power grid shares with the smart meters its available amount of resources that is expected during the next future peak time slot; smart meters expecting a demand for additional power during future peak hours participate in the power auction by submitting bids of their offered price for their requested amount of power. In order to secure the power auction and protect smart meters' privacy, homomorphic encryption is used to secure the bidding values and ensure avoiding possible insincere behaviors of smart meters or the grid operator (i.e. the auctioneer) to manipulate the auction for their own benefits. We propose an efficient power scheduling mechanism to distribute the operator's limited resources among smart meters participating in the power auction. Finally, we present simulation results for the performance of our secure power scheduling auction mechanism.**

***Index Terms*—Power Scheduling Auction, Homomorphic Encryption, Smart Grid**

I. Introduction

Many power grids experience a faster grow in the consumption of electric power compared to the expansion rates of generation units. Therefore, maintaining a sufficient reliability of power grids during peak time periods has been given significant attention recently [1]. Demand response in smart grids is one of the promising approaches to improve power grids' reliability. It controls the consumption of electric power by users during peak time periods and usually provides lower overall costs. Price based demand response is the most commonly used approach which controls and manages users' consumption of electric power by adopting a day ahead [2], [3] or real time [4], [5] designs for electricity prices. In this paper we introduce a new secure electric power management and pricing approach by designing a secure power scheduling auction to schedule the power grid's limited resources for future peak time periods.

We have focused on designing a power auction that has the following auction's favorable economic properties: incentive compatible, Pareto efficient and individual rational. An efficient auction design needs to make sure that all bidders submit their true evaluation bidding values in order to ensure truthfulness in the power auction. The proposed power auction uses a payment method that is based on Vickrey-Clarke-Groves (VCG) auction since VCG is the only auction that has proved to satisfy the above economic properties while maximizing the auctioneer's revenue [6], [7]. Even though VCG auction has the aforementioned good properties, it is vulnerable to back-room dealing between an insincere auctioneer and greedy bidders who collude with each other to manipulate the auction for their own benefits. For example, the auctioneer may carry out frauds when he overcharges the winning bidder if that bidder cannot verify the actual submitted bids from other bidders. On the other hand, bid rigging occurs when the auctioneer shares the value of the winning bid with certain bidder (a greedy bidder) so that the greedy bidder bids more than his true evaluation value to enable the auctioneer to increase his revenue and share the spoils with the greedy bidder. Therefore, VCG auction cannot be directly used in the power auction and providing a secure power auction design is becoming necessary. In order to ensure bidders' privacy and avoid possible back room dealings, a successful secure auction design needs to enable the auctioneer to decide the winners and their charging price without knowing the bidders' actual bids.

In this paper, we design a secure power scheduling auction mechanism to schedule the power plant's limited electric power resources during peak hours time slots. The proposed mechanism allows the power grid operator to schedule his expected future available resources to the smart grids and charge them for the scheduled resources. It provides a framework for the power plant's operator, who plays the role of an auctioneer, to manage his limited resources efficiently and securely. It uses homomorphic encryption to ensure users' privacy and secure the power auction which is vulnerable to fraud of an insincere auctioneer and bid rigging.

II. System Model and Design Assumptions

We consider a power grid consisting of K smart meters (SM)s, denoted in the set $\mathcal{K} = \{1, 2, ..., K\}$, that purchases electric power from a power plant operator (grid operator). We consider the situation where a set of smart meters $\mathcal{N} = \{1, 2, ..., N\}$, $\mathcal{N} \subseteq \mathcal{K}$, are interested in purchasing additional amount of electric power (in addition to its regularly scheduled power) from the power plant operator to satisfy the demands of their commercial or industrial users during the next peak hours time slot. We express the power trading mechanism by designing a secure power auction. The grid operator plays the role of an auctioneer that auctions its spare resources to bidders (i.e. smart grids in $\mathcal{N}$). We assume that the grid operator is able to determine its expected amount of spare resources (electric power) denoted by R in KW that will be available during the next peak time slot. The amount of resources R is divided into M electric power units (EPU)s. Let $\mathcal{M} = \{1, 2, ..., M\}$ denotes the set of available EPUs to be auctioned by the grid operator to the N smart meters in the power grid. We assume

H. Shajaiah, A. Abdelhadi, and C. Clancy are with the Hume Center for National Security and Technology, Virginia Tech, Arlington, VA, 22203 USA e-mail: {hayajs, aabdelhadi, tcc}@vt.edu.

This research is based upon work supported by the National Science Foundation under Grant No. 1134843.

that the grid operator runs the power scheduling auction for future peak hours time slot during which a contingency will occur. Each smart meter can bid for a single or multiple EPUs from the set $\mathcal{M}$ based on its demand.

In the proposed power auction model, we consider a secure gateway that plays the role of a middleman between the auctioneer and the bidders. Figure 1 shows a power grid that consists of SMs, power plant and secure gateway. The secure gateway announces to the SMs the number of bidders as well as the number of auctioned EPUs. Once the smart meters receive these information, the interested smart meters submit their bids (price) to the auctioneer.

Let $\mathcal{A} = \{\beta^1, \beta^2, ..., \beta^|\mathcal{A}|\}$ be the set of all possible allocations for the M EPUs that each SM bids for and $|\mathcal{A}|$ is the number of all possible allocations. For example, in the case of $\mathcal{M} = \{\text{EPU1}, \text{EPU2}\}$ and $\mathcal{N} = \{1, 2, 3\}$, then we have $\mathcal{A} = \{\beta^1 = (2,0,0), \beta^2 = (0,2,0), \beta^3 = (0,0,2), \beta^4 = (1,1,0), \beta^5 = (1,0,1), \beta^6 = (0,1,1)\}$, e.g., $\beta^1 = (2,0,0)$ denotes an allocation where EPU1 and EPU2 are scheduled for bidder 1 and nothing is scheduled for bidder 2 and bidder 3. Each SM submits an encrypted bid for each allocations in $\mathcal{A}$ where $\mathbf{w_i} = [w_i(\beta^1), w_i(\beta^2), ...]$ represents the encrypted bids that bidder i in $\mathcal{N}$ submits for the allocations in $\mathcal{A}$, e.g. $\mathbf{w_2} = [0,2,0,1,0,1]$ indicates that SM 2 bids 0 for allocation β^1, 2 for allocation β^2, 0 for allocation β^3, 1 for allocation β^4, 0 for allocation β^5 and 1 for allocation β^6. It is assumed that each SM submits same bids for different allocations in $\mathcal{A}$ if the number of EPUs that corresponds to that SM in these allocations is the same. The bidding values of each SM represent the price of the EPUs that the SM is bidding for. This price is traffic dependant [8]; i.e. increases when the demand for more EPUs is high. Let $v_i(\beta)$ denotes the true evaluation value (bidding price) of SM i for allocation β and $\mathbf{v_i} = [v_i(\beta^1), v_i(\beta^2), ...]$ be the true evaluation vector for SM i.

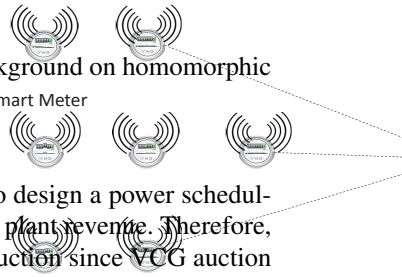
Let p_i denotes the charging price of the auctioneer (grid operator) to SM i for the scheduled EPUs. Then the utility of SM i is given by $u_i = v_i(\beta) - p_i$; i.e. the difference between the true evaluation value and the actual price that the SM pays to the auctioneer for allocation β. Furthermore, let $Rev = \sum_{i=1}^{i=N} p_i$ represents the power plant's revenue from selling the auctioned electric power R.

Providing an efficient contingency management using a secure power auction provides a fair scheduling mechanism and helps the grid operator improve its profit. It is important to take into consideration that the grid operator (auctioneer) is prone to fraud. Therefore, an ideal power auction should prevent possible back room dealing by allowing the auctioneer to determine the winners and their payments while the actual bidding values are kept secret from the auctioneer.

III. Design Considerations

In this section, we discuss some desired properties that are taken into consideration in the proposed power scheduling auction. First, we discuss the payment rule that the auctioneer adopts to determine the charging price that the SMs pay for the scheduled EPUs. Then we discuss the security and privacy challenges that need to be addressed in the auction design. Finally, we provide some background on homomorphic encryption.

Fig. 1. Power grid that consists of smart meters, power plant and secure gateway.



A. VCG Based Payment Rule

As mentioned before, our goal is to design a power scheduling auction that maximizes the power plant revenue. Therefore, we adopt the payment rule of VCG auction since VCG auction is proven to be Pareto efficient [9]. In order for a SM to maximize its utility, it has to bid with its true evaluation value regardless of the bidding strategies of other bidders [10]. In the proposed power auction design, we use a payment rule that is based on VCG auction mechanism [11] where each bidder is charged a price that is equivalent to the difference between the social welfare with and without that bidder's participation in the auction. Each SM i submits its encrypted bidding vector $\mathbf{w_i}$ for the allocation set $\mathcal{A}$. Let $\beta^* \in \mathcal{A}$ be a Pareto efficient allocation that the auctioneer selects where β^* is defined as

$$\beta^* = \arg\max_{\beta \in \mathcal{A}} \sum_i w_i(\beta). \tag{1}$$

The auctioneer schedules the EPUs in $\mathcal{M}$ to the SMs in $\mathcal{N}$ based on allocation β^*. Furthermore, when SM i is not participating in the auction then the corresponding allocation $\beta^*_{-i} \in \mathcal{A}$ is defined as

$$\beta^*_{-i} = \arg\max_{\beta \in \mathcal{A}} \sum_{j \neq i} w_j(\beta). \tag{2}$$

The price that SM i is charged by the auctioneer for allocation β^* is equivalent to

$$p_i = \sum_{j \neq i} w_j(\beta^*_{-i}) - \sum_{j \neq i} w_j(\beta^*). \tag{3}$$

Then the utility of SM i is $u_i = v_i(\beta^*) - p_i$. By using the payment method expressed in equation 3, the auction has no positive transfers (i.e. $p_i \geq 0 \forall i \in \mathcal{N}$ and other desired economic properties can be satisfied as mentioned before.

B. Security and Privacy Considerations

One of the most important features of the proposed power scheduling auction is providing a sufficient level of security in order to enable a reliable and efficient scheduling of the auctioneer's resources. On the other hand, it is important to provide the SMs with a sufficient level of privacy by using a cryptosystem that allows bidders to submit their encrypted bidding values while keeping the actual values unknown to

the auctioneer and other bidders in order to thwart back-room dealing such as bid-rigging between the bidders and the auctioneer and possible fraud of an insincere auctioneer. Bid-rigging can occur if the insincere auctioneer that is aware of the bidders actual bidding values colludes with certain bidder, for the benefit of both, by sharing with him the bidding values of other bidders and manipulate the auction. On the other hand, frauds of the insincere auctioneer occurs if the auctioneer manipulates the charging price and overcharges the winners in order to increase its revenue which results in a bad utilities for the winners. Therefore, it is important for a power scheduling auction to use a mechanism that allows the auctioneer to determine the maximum bid without knowing the actual bidding values.

C. Homomorphic Encryption

As mentioned before, homomorphic encryption is adopted in our auction design. Homomorphic encryption is used when there is a requirement to perform certain operations while the inputs are not disclosed. There are many schemes for homomorphic encryption. In the proposed auction design we adopt Paillier cryptosystem [12], [13]. By using Paillier cryptosystem, the encryption function $E(.)$ of plaintexts x_1 and x_2 is additively homomorphic, i.e. $E(x_1 + x_2) = E(x_1)E(x_2)$. With the indistinguishability property of Paillier cryptosystem, if a plaintext x is encrypted twice the resulting two cyphertexts are different from each other making it not possible for anyone to distinguish their original plaintexts unless decrypting the two ciphertexts. In addition, with the self blinding property of Paillier cryptosystem, it is possible to compute different ciphertext $E^{'}(x)$ from the ciphertext $E(x)$ without knowing the decryption key of the plaintext.

IV. Secure Power Scheduling Auction Mechanism

Given that the grid operator who plays the role of an auctioneer could be a private entity, the auction is prone to fraud from an insincere auctioneer. Therefore, preventing possible insincere behavior from the auctioneer is essential. In order to enable an efficient secure scheduling process of the power plant's resources, it is important to design a secure power auction that enables the power plant's operator to determine the winners and the resource price without knowing the original bids. By making the auctioneer only able to exploit the winners and their payments, it is then not possible for him to conduct bid-rigging or fraud. Once the power auction is performed, the power plant's operator schedules each of the winning SMs for the corresponding EPUs and charges it for the scheduled resources. The proposed power auction leverages homomorphic encryption through Paillier cryptosystem to provide a secure and honest auction mechanism by avoiding possible frauds and bid-rigging. The procedure of the proposed secure power auction is presented in the following steps:

1. The auctioneer generates a private and public keys of Paillier cryptosystem and shares his public key x (i.e. $x \neq 0$) with the SMs in the power grid.

2. Each SM i in $\mathcal{N}$ submits its true evaluation bidding values in $\mathbf{w_i} = \mathbf{v_i}$ to a buffer that encrypts these values using Paillier cryptosystem and creates ciphertexts. Let the bidding value $w(\beta)$ of allocation β be equivalent to m such that $1 \leq m \leq s$ where s is any number that is large enough to cover all possible bidding values for the allocation of the EPUs. Let $E(x)$ be the Paillier encryption of the public key $x \neq 0$, the buffer creates a vector of ciphertexts $\mathbf{e}(m)$ for bidding value m where $\mathbf{e}(m)$ is given by

$$\begin{aligned}\mathbf{e}(m) &= (e^1, ..., e^s) \\ &= (\underbrace{E(x), ..., E(x)}_{m}, \underbrace{E(0), ..., E(0)}_{s-m}).\end{aligned} \tag{4}$$

Furthermore, the auctioneer creates $N+1$ representing vectors $\mathbf{E}_T = \mathbf{E}(O)$, $\mathbf{E}_1 = \mathbf{E}(O)$,...,$\mathbf{E}_N = \mathbf{E}(O)$ (i.e. N is the number of bidders). The size of $\mathbf{E}$ equals $|\mathcal{A}|$ and the initial $O(\beta)$ equals 0; i.e. $\mathbf{E}(O) = \{e(0), e(0), .., e(0)\}$. Each SM; i.e. the j^{th} SM in $\mathcal{N}$ keeps its encrypted bidding vector $\mathbf{w_j}$ secret by adding it to all representing vectors except $\mathbf{E}_j$. Once performing this addition process by each SM in $\mathcal{N}$, the auctioneer obtains

$$\mathbf{E}_T = (\prod_i \mathbf{e}(w_i(\beta_1)), ..., \prod_i \mathbf{e}(w_i(\beta_{|\mathcal{A}|}))). \tag{5}$$

By applying the homomorphic addition property, $\mathbf{E}_T$ can be expressed as

$$\mathbf{E}_T = (\mathbf{e}(\sum_i w_i(\beta_1)), ..., \mathbf{e}(\sum_i w_i(\beta_{|\mathcal{A}|}))) = \mathbf{E}(\sum_i w_i), \tag{6}$$

and the auctioneer also has $\mathbf{E}_j = \mathbf{E}(\sum_{i \neq j} w_i)$ for $(1 \leq j \leq N)$.

3. The secure gateway adds a random constant $\theta(\beta) = r$ to each of $\mathbf{E}_T, \mathbf{E}_1, ..., \mathbf{E}_N$ to obtain $\mathbf{E}(\sum_i w_i + \theta)$ and $\mathbf{E}(\sum_{i \neq j} w_i + \theta) \forall j$ and sends them to the auctioneer.

4. The auctioneer determines the maximum sum value of the masked bids according to the following equation:

$$\begin{aligned}k &= \max_{\beta \in \mathcal{A}} (\sum_i w_i(\beta) + \theta(\beta)) \\ &= \max_{\beta \in \mathcal{A}} (\sum_i w_i(\beta)) + r,\end{aligned} \tag{7}$$

where k can be determined by the auctioneer by taking the product of the encrypted values in $\mathbf{E}_T$, which is equivalent to $\prod_{n=1}^{|\mathcal{A}|} \mathbf{e}(\sum_{i=1}^{N} w_i(\beta_n) + r)$, and finding the maximum element in that product.

5. The auctioneer decrypts the k^{th} element of each vector $\mathbf{e}(\sum_i w_i(\beta) + \theta(\beta))$ in $\mathbf{E}_T$ for all the allocations in $\mathcal{A}$. Its decrypted value will be equivalent to zero or x. The allocation that has a decryption value equivalent to x, i.e. β^*, is the one that maximizes $\sum_i w_i$. The auctioneer considers β^* to be the winning allocation and schedules its resources to the corresponding SMs according to β^*.

6. In order for the auctioneer to find its charging price for each winning SM, the auctioneer decrypts $\mathbf{e}(\sum_{i \neq z} w_i(\beta^*) + \theta)$ of $\mathbf{E}_z$ (i.e. SM z is a winning one) and finds the value $(\sum_{i \neq z} w_i(\beta^*) + \theta)$. The auctioneer then finds the maximum value of the product of the encrypted elements $\max_{\beta \in \mathcal{A}} (\sum_{i \neq z} w_i(\beta) + r) = (\sum_{i \neq z} w_i(\alpha^*_{-z}) + r)$.

The auctioneer calculates the charging price that each of the winning SMs needs to pay for the scheduled EPUs according to the following equation

$$p_z = (\sum_{i \neq z} w_i(\beta^*_{-z}) + r) - (\sum_{i \neq z} w_i(\beta^*) + r). \quad (8)$$

where SM z is a winning bidder that pays a price p_z for its scheduled EPUs.

Figure 2 shows the procedure of the proposed secure power

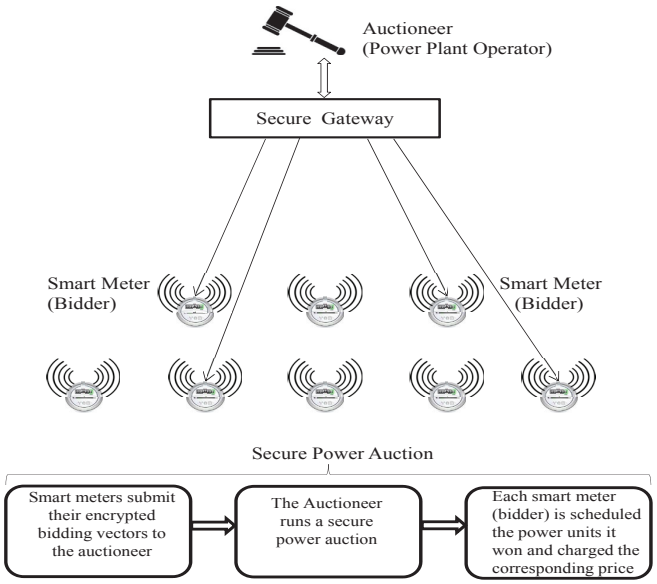


Fig. 2. Procedure of the proposed secure power scheduling auction.

V. Simulation Results

In this section, we present the performance of the proposed power scheduling auction. Two performance metrics are considered: power plant's revenue and SMs' satisfaction. Let $\mathcal{W}$ denotes the set of all winning SMs. The power plant's revenue is given by $Rev = \sum_{i \in \mathcal{W}} p_i$ (i.e. the sum of all winning SMs' charging prices) and the SMs' satisfaction is represented by the sum of all winning SMs' utilities divided by the sum of all SMs' evaluation values that is given by $\sum_{i \in \mathcal{W}} u_i / \sum_{i \in \mathcal{N}} v_i$. We ran Monte Carlo Simulation for different number of SMs that are bidding for the auctioneer's resources and the results are averaged over the independent runs in which the bidding values of the SMs are generated randomly and the two performance metrics are evaluated. Simulation results are represented for each of the four cases: $N = 2$ SMs (bidders), $N = 3$ SMs, $N = 4$ SMs and $N = 5$ SMs.

Figure 3 shows that the auctioneer's revenue increases when the number of SMs (bidders) increases. This is expected as the auctioneer's revenue increases with more bidders requesting more resources. In Figure 4, we show that the bidders' satisfaction increases as the number of EPUs increases until the bidders' satisfaction saturates when each SM is assigned the number of EPUs it bids for. Figure 4 also shows that for the same amount of the auctioneer's available resources R, the bidders satisfaction is higher when there are less number of bidders participating in the power auction.

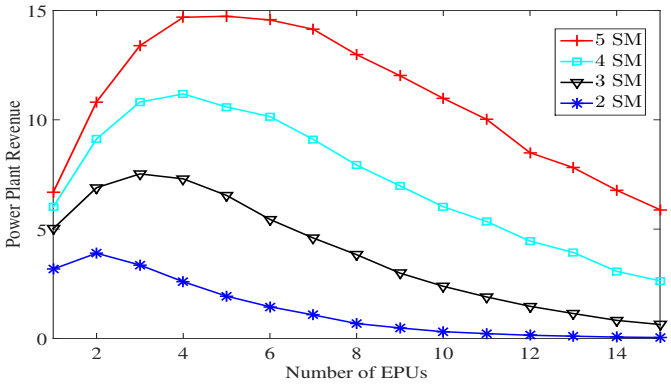


Fig. 3. The auctioneer's revenue for different number of bidders with the auctioned EPUs changing from 1 to 15.

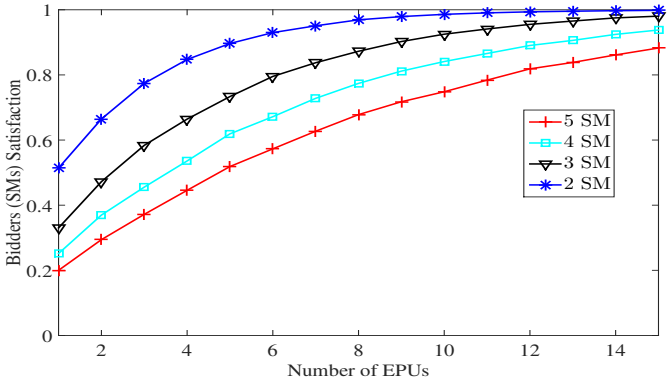


Fig. 4. Bidders' satisfaction with the auctioned EPUs changing from 1 to 15.

VI. Conclusion

In this paper, we have proposed a secure power scheduling auction that enables an efficient power scheduling mechanism to schedule the power plant's limited resources during peak hours time slots. We have taken into consideration possible insincere behavior of the auctioneer and designed a power auction that prevents possible frauds and bid-rigging between an insincere auctioneer and greedy bidders. The proposed power auction leverages homomorphic encryption through Paillier cryptosystem to keep the SMs' bidding values unknown to the auctioneer while the auctioneer is still able to find the winning SMs. We showed through simulations that the proposed power auction provides sufficient revenue for the power plant and satisfactory utilities for the SMs while providing a secure power scheduling auction against possible back room dealings.

References

[1] P. Yi, X. Dong, A. Iwayemi, C. Zhou, and S. Li, "Real-time opportunistic scheduling for residential demand response," *Smart Grid, IEEE Transactions on*, vol. 4, pp. 227–234, March 2013.

[2] A.-H. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, pp. 320–331, Dec 2010.

[3] C. Joe-Wong, S. Sen, S. Ha, and M. Chiang, "Optimized day-ahead pricing for smart grids with device-specific scheduling flexibility," *Selected Areas in Communications, IEEE Journal on*, vol. 30, pp. 1075–1085, July 2012.

[4] J. H. Yoon, R. Baldick, and A. Novoselac, "Dynamic demand response controller based on real-time retail price for residential buildings," *Smart Grid, IEEE Transactions on*, vol. 5, pp. 121–129, Jan 2014.

[5] S. Li, D. Zhang, A. Roget, and Z. O'Neill, "Integrating home energy simulation and dynamic electricity price for demand response study," *Smart Grid, IEEE Transactions on*, vol. 5, pp. 779–788, March 2014.
[6] R. Weber, "Auction Theory: By Vijay Krishna. Academic Press, 2002," *Games and Economic Behavior*, vol. 45, no. 2, pp. 488–497, 2003.
[7] T. Groves, "Incentives in teams," *Econometrica*, vol. 41, p. 617631, 1973.
[8] A. Abdel-Hadi and C. Clancy, "A Robust Optimal Rate Allocation Algorithm and Pricing Policy for Hybrid Traffic in 4G-LTE," in *PIMRC*, 2013.
[9] W. Vickrey, "Counterspeculation, Auctions and Competitive Sealed Tenders," *Journal of Finance*, pp. 8–37, 1961.
[10] A. Abdelhadi, H. Shajaiah, and C. Clancy, "A multitier wireless spectrum sharing system leveraging secure spectrum auctions," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, pp. 217–229, June 2015.
[11] N. Nisan, T. Roughgarden, É. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.
[12] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'99, (Berlin, Heidelberg), pp. 223–238, Springer-Verlag, 1999.
[13] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems provably secure against active adversaries," in *Advances in Cryptology - ASIACRYPT99* (K.-Y. Lam, E. Okamoto, and C. Xing, eds.), vol. 1716 of *Lecture Notes in Computer Science*, pp. 165–179, Springer Berlin Heidelberg, 1999.