IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 26, 2020, accepted February 10, 2020, date of publication February 17, 2020, date of current version February 27, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2974227*

# An Efficient Privacy Preserving Spectrum Sharing Framework for Internet of Things

**XIAOYAN WANG[1], (Member, IEEE), MASAHIRO UMEHIRA[1], (Member, IEEE), BIAO HAN[2], (Member, IEEE), HAO ZHOU[3], (Member, IEEE), PENG LI[4], (Member, IEEE), AND CELIMUGE WU[5], (Senior Member, IEEE)**

[1]Graduate School of Science and Engineering, Ibaraki University, Ibaraki 316-8511, Japan
[2]School of Computer, National University of Defense Technology, Changsha 410073, China
[3]School of Computer Science, University of Science and Technology of China, Hefei 230026, China
[4]School of Computer Science and Engineering, University of Aizu, Aizuwakamatsu 965-8580, Japan
[5]Graduate School of Informatics and Engineering, The University of Electro-Communications, Chofu 182-8585, Japan

Corresponding author: Biao Han (nudtbill@nudt.edu.cn)

This work was supported in part by the Japan Society for the Promotion of Science Grant-in-Aid (JSPS) Grant-in-Aid for Young Scientists (B) under Grant 17K12670, and in part by the National Key Research and Development Program of China under Grant 2018YFB0204301.

**ABSTRACT** Internet of Things (IoT) devices are forecasted to increase to 20 billion by the year 2020. Questions are arising as where the bandwidth and radio channels come from to make it all work. It is a common belief that the spectrum under 6GHz is easy to use for various IoT applications. However, currently it has been almost fully allocated to different kinds of systems, some of which suffer from an extremely low spectrum utilization ratio. To this end, spectrum sharing approach has been proposed recently, which dynamically redistributes the incumbents' underutilized spectrum to secondary users and exchanges for profit. To incentivize the incumbent to share the spectrum in efficient and profitable ways, auction based mechanisms are extensively discussed. Most of the existing researches propose to share the spectrum by utilizing truthful auction mechanism, in which the secondary users' dominant strategies are to bid their true valuations. However in reality, exposing true valuation is very risky and thus keeping user's bidding value confidential is of great importance. In this paper, we propose an efficient privacy preserving spectrum sharing framework for IoT by utilizing ElGamal cyptosystem. The proposed scheme hides the user's bid from both the auctioneer and other users. By extensive evaluation results, we show that the proposed framework could achieve good spectrum utilization efficiency and user satisfactory ratio, at the cost of acceptable communication and computation overheads.

**INDEX TERMS** Auction theory, privacy preservation, spectrum sharing.

## I. INTRODUCTION

The number of Internet of Things (IoT) devices is projected to amount to 20 billion worldwide by 2020, and 75.44 billion by 2025. Correspondingly, the data traffic skyrockets due to the tremendous increasing of IoT devices and spectrum-hungry applications [1]–[4]. Since data is more and more wirelessly transferred, spectrum is expected to become the scarcest resource which hinders the development of IoT. To deal with the spectrum crunch problem, two kinds of solutions are investigated from different aspects. One solution is to exploit the usage of spectrum in higher frequency bands (6 GHz above) to scale up the network capacity. But high frequency band use-case is limited due to its propagation characteristics and therefore extensive real-world tests are required. Another solution is to enable more efficient and flexible usage of spectrum below 6 GHz. Based on the actual spectrum usage measurement results, there is a common belief that the capacity of the radio spectrum under 6 GHz has not been fully approached. For instance, the utilization ratio of TV broadcasting spectrum is less than 6% in most developed countries by considering different time and locations. These results encourage us for developing more dynamic and efficient spectrum management policies for future IoT systems.

The researches on spectrum sharing have emerged recently [5]–[9]. A paradigm shift from static spectrum allocation towards dynamic spectrum sharing has been widely

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenyu Zhou.

discussed. In the spectrum sharing framework, secondary users could access the spectrum that is underutilized by primary system, i.e., incumbent. In the context of IoT, the secondary users could be various IoT devices, and the incumbent could be the TV broadcasting, satellite, radar systems. To incentivize the primary system to lease the access right to secondary users, researches on secondary spectrum market have attracted intensive interests. The basic idea is that the primary users sell the temporarily or spatially unused spectrum, i.e., whitespace, to secondary users, in exchanging for profit which could be money, credit or resource. Meanwhile, the secondary users reuse the whitespace by paying the spectrum access right, and thus ease their starvation for transmission opportunities. The collaboration between primary and secondary users will lead to a win-win result finally.

To efficiently and fairly allocate the spectrum resource, market-based auction mechanism [10] is considered to be one of the most promising solutions. In the context of auction-based spectrum sharing, there are two fundamental requirements. The first one is *spatial reusability*. In traditional auction, there is only one winner for each auctioned goods, since the auctioned goods cannot be shared. However, the spectrum resource could be shared by multiple users who are out of the interference ranges with each other. These non-interference users could form a group and bid for the spectrum resource as one entity. The second one is *truthfulness*. A truthful auction implies that every bidder's dominant strategy is to bid at his true valuation for the selling goods. Bidding truthfully yields the highest utilities for all the bidders, regardless of the strategies of others. Truthfulness is considered to be the most important property for an auction, since it guarantees that all the bidders would not be interested in strategically manipulating their bids to pursue higher reward.

Bidders reveal their true valuations, however, might be very risky in reality. When the auctioneer or other bidders cannot be completely trusted, they may take malicious actions to maximize their own profits. For instance, by exploiting the bidders' true valuation information, the auctioneer might forge the auction process to maximize her profit in the future auctions [11]. We give a simple example to facilitate better understanding. Consider the case that Alice participates an online second-price auction [12], in which the bidder with the highest bid wins the auction but only needs to pay the second-highest bid. Assume Alice values the goods at \$5000. Since the second-price auction is proven to be a truthful one, Alice will bid her true valuation as her dominant strategy. Assume that Alice wins the auction and pays the second highest price, say \$4000. After a period of time, the same goods is put for auction again. And Alice bids her true valuation \$5000 again since she is still interested. Assume that Alice wins the auction again, however, this time she is charged with \$4999. Certainly, it is reasonable to suspect that the auctioneer forges the second highest price by learning from bidders' previous bids. Therefore, protecting the bidders' private valuation against exposure is of great importance. For an ideal privacy preserving auction [11], all the parties in the auction, including auctioneer and all bidders, can only be aware of the identities of winners and their respective charges, but the bids of individual users should be kept confidential as a private information.

In this paper, we propose an auction-based efficient privacy preserving spectrum sharing framework for IoT, by taking into consideration both the spatial spectrum reusage and truthfulness. The proposed framework intends to only reveal the winners' identities and the group bids, but keeps the individual user's bid confidential. To this end, the proposed spectrum sharing framework consists of three parties, i.e., an auctioneer, multiple bidders and a Cryptographic Authority (CA). Here, CA is a third party to generate public keys. Regarding the bidding processes, firstly the bidders send their homomorphic encrypted sealed bidding vectors (e.g., using ElGamal encryption) to the auctioneer by using the ElGamal public key generated by the CA. Then, the auctioneer constructs a mixed sealed group matrix and sends it to CA, who will decrypt the group bids by using her ElGamal private key. Finally, the auctioneer derives the winning groups and their charges. In our assumptions, either the auctioneer or CA could be untrusted, but they would not collude. The proposed framework guarantees that no bidder's bidding price would be exposed, as long as the auctioneer and CA do not collude with each other. We have performed extensive evaluations to show that the proposed framework achieves good spectrum utilization efficiency and user satisfactory ratio, at the cost of acceptable communication and computation overheads.

The rest of the paper is organized as follows. Section II introduces the preliminary for homomorphic encryption and related researches. Section III addresses the proposed efficient privacy preserving spectrum sharing framework in details. Section IV provides performance evaluations. And finally Section V draws the conclusions.

## II. PRELIMINARIES AND RELATED WORK

### A. HOMOMORPHIC ENCRYPTION: ELGAMAL ENCRYPTION SCHEME

The proposed auction-based privacy preserving spectrum sharing framework is built based on a widely known public key homomorphic encryption scheme: ElGamal cryptosystem [13]. In this subsection, to facilitate better understanding, we briefly introduce the ElGamal encryption function. Similar to the well known RSA (Rivest-Shamir-Adleman) scheme, ElGamal encryption scheme is a public key cryptosystem, i.e., the encryption key is published, and the decryption key is kept private. The mathematical relationship between the encryption and decryption keys lies upon the discrete log problem.

- *Key generation*. First, the first party chooses a very large prime number $p$, and a primitive root modulo $p$, say $\alpha$. Then, an integer $a$ is chosen and $\beta = \alpha^a \pmod p$ is computed. The encryption key is the ordered triple $(p, \alpha, \beta)$, which is made public. However, the integer $a$ is kept secret, which is the decryption key.

- *Encryption*. To use ElGamal to encrypt a plaintext $m$, the second party first chooses a secret integer $k$ and computes $r = \alpha^k \pmod p$ and $t = \beta^k m \pmod p$. The pair $(r, t)$ is second party's ciphertext, and $k$ is known only by the second party itself.
- *Decryption*. Once the encrypted message has been transmitted to the first party, he could compute the plaintext $m$ as $m = tr^{-a} \pmod p$ by using $a$. An eavesdropper knows $p, \alpha, \beta, r, t$ but is unaware of $k, a$. Knowledge of either $a$ or $k$ would be enough to decrypt the plaintext $m$, as $m = tr^{-a} = t\beta^{-k} \pmod p$.

In the following part, we use $El(\cdot)$ to denote the ElGamal encryption. The ElGamal encryption scheme has the following very important properties, which are the keys to realize our efficient private preserving spectrum sharing framework.

*Property 1: Homomorphic property. Homomorphic refers to homomorphism in algebra: the encryption and decryption functions can be thought as homomorphisms between plaintext and ciphertext spaces. Specifically, the encryption function $El(\cdot)$ allows computations to be carried out directly on ciphertext. When the generated encrypted result is decrypted, it will match the result of operations performed on the plaintext. I.e., $El(m) \cdot El(m') = El(m \cdot m')$, where $m$ and $m'$ are different plaintexts.*

*Property 2: Indistinguishability. The ciphertext $El(m)$ is considered indistinguishable if the same plaintext $m$ is encrypted twice. Specifically, given two cipertexts $El(m)$ and $El(m')$, a polynomial Turing machine is unable to distinguish whether or not the plaintexts are the same, i.e., $m = m'$.*

*Property 3: Randomizability. One can compute a randomized ciphertext $El'(m)$ directly from the original ciphertext $El(m)$, without either the decryption or knowing the plaintext $m$.*

We omit the detailed calculations and security analysis of ElGamal encryption/decryption functions in this article, which could be found in [13].

### B. RELATED WORK

#### 1) SPECTRUM SHARING IN IOT

In the context of spectrum sharing in IoT, it is of great importance to construct an accurate radio environment map (REM). REM provides the spectrum availability information for the primary systems at any locations, by using which the IoT devices could access the whitespace without causing harmful interference to primary users. In recent years, extensive researches have been done to improve the quality of REM. A basic approach is to deploy dedicated sensors uniformly over the region of interest [14]. To solve the high cost issue, crowdsourced based approaches have been proposed [15]–[17], in which mobile users with spectrum sensors are recruited to provide measurements. Besides REM, exclusion zone determination is also very important for spectrum sharing, inside which the secondary spectrum reuse is prohibited. Ullah *et al.* [18] have proposed a multitiered exclusion zone framework by exploiting point-to-point mode terrain profile. And Bhattarai *et al.* [19] have proposed an on-the-fly exclusion zone refinement approach to ensure a probabilistic guarantee of the interference from secondary user to primary user.

#### 2) AUCTION-BASED SPECTRUM SHARING

In the secondary spectrum market, utilizing auction-based schemes to fairly and efficiently redistribute the spectrum resource have been extensively investigated. To our limited knowledge, the first work in this topic is done by Zhou and Zheng [5], who have proposed a double spectrum auction framework which takes any reusability-driven spectrum allocation algorithm as the input, and applies a novel winner determination and pricing mechanism to achieve truthfulness, budget balance and individual rationality. Based on that, Feng *et al.* [6] have considered heterogeneous spectrum sharing problem and proposed a truthful double auction scheme, which allows buyers to explicitly express their personalized preferences and also addresses the problem of interference graph variation. Yi and Cai [7] have proposed a recall-based combinational spectrum auction mechanism which could deal with multiple heterogeneous secondary users with various quality-of-service requirements. Wang *et al.* [8], [20] have investigated the secure information transfer issue under spectrum sharing scenario by using both monetary-based and barter-like spectrum auction schemes. Moreover, fine-grained auction based incentive mechanisms for crowdsourced REM construction have been proposed in [21]–[23]. However, these researches do not consider the privacy preservation issue for the individual bidder.

#### 3) PRIVACY PRESERVING AUCTION

Extensive researches have been done on the privacy preserving auction mechanisms for conventional goods. Naor *et al.* [11] have proposed a privacy preserving auction mechanism by utilizing Yao's secure computation [24] and oblivious transfer functions. Abe and Suzuki [25] have proposed an $M+1$-st price sealed-bid auction scheme that offers bidding price secrecy and public verifiability. Sako [26] have proposed an auction protocol in which a bid will not be successfully decrypted unless it is the highest bid. To the best of our knowledge, Pan *et al.*'s research [27], [28] is the first work that addresses the privacy preservation problem for spectrum auctions. They have proposed a secure spectrum auction leveraging the Paillier cryptosystem to prevent the frauds of the auctioneer as well as the bid-rigging between the bidders and the auctioneer. Furthermore, Wu *et al.* [29] have proposed a truthful spectrum auction mechanism for both single channel request and multichannel request. They have employed order-preserving encryption as the cryptographic tools to guarantee the k-anonymity.

## III. PROPOSED EFFICIENT PRIVACY PRESERVING SPECTRUM SHARING FRAMEWORK

### A. AUCTION BASED SPECTRUM SHARING FRAMEWORK WITHOUT PRIVACY PRESERVATION

In this subsection, we first present an auction-based spectrum sharing framework without privacy protection. Here,

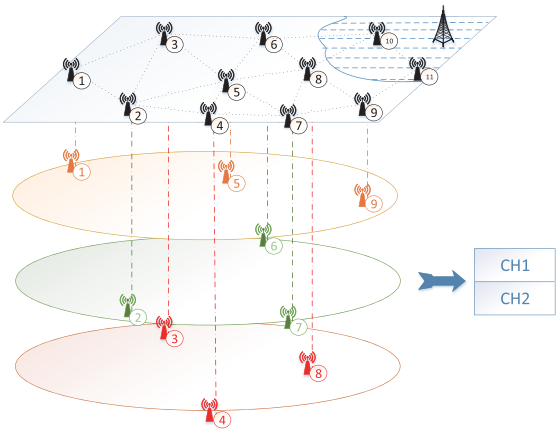



**FIGURE 1.** An example of grouped spectrum auction.

the primary system is the auctioneer, e.g., TV broadcast or naval shipborne radar system, who tends to lease $M$ channels in exchange for proper profit. The secondary users are the bidders, e.g., IoT devices, who tend to utilize the primary spectrum to perform their own transmission. Considering the example that illustrated in Fig. 1, where the primary system tends to lease the access right of 2 channels. The secondary spectrum sharing are only allowed in particular geographic regions, i.e., outside the exclusion zones. Generally, the exclusion zones are determined by an interference threshold. The signal strength of the primary system at a given location could be provided by REM, which is either calculated by path-loss model or monitored by dedicated spectrum sensors. All the secondary users locate outside the exclusion zones, e.g., IoT devices No. $1 \sim 9$ in Fig. 1, have the opportunities to access the primary system's spectrum by participating the spectrum auction.

The main difference between spectrum auction and conventional-goods auction is spatial reusability. In spectrum auction, multiple wireless users that locate outside each others' interference ranges can share the same channel simultaneously. Exploiting spatial reusability is extremely important when we design a spectrum auction, without which huge amount of spectrum resources will be wasted. Generally, we could model the interference relationship for wireless devices as a conflict graph. As illustrated in Fig. 1, two devices that connected by an edge denotes that they are interfering with each other. Similar to [30], we calculate the interference range based on Signal to Interference plus Noise Ratio (SINR) and a threshold. Considering a scenario with totally $N'$ users[1] as $\mathbb{N}' = \{1, \cdots, n, \cdots, N'\}$. We focus on the users that are outside the exclusion zones, which are denoted by $\mathbb{N} = \{1, \cdots, n, \cdots, N\}$, where $N \leq N'$. By using graph coloring algorithms [31], the $N$ users could be split into multiple nonconflicting groups $\mathbb{G} = \{1, \cdots, g, \cdots, G\}$. For instance, the users in Fig. 1 are divided into 3 nonconflicting groups, and users No.1, 5, 9 within the same group, are able to access the same channel simultaneously without interfering with each other. We use $\mathbb{N}_g$ to denote the set of users in group $g$, and have $\mathbb{N}_g \cap \mathbb{N}_{g'} = \emptyset, \forall g, g' \in \mathbb{G}$, and $\bigcup_{g\in\mathbb{G}} \mathbb{N}_g = \mathbb{N}$.

Each user outside the exclusion zones could bid one channel based on its *valuation* $v_n$ per channel[2]. The valuation also is known as *type*, which is related to its possible reward gained by accomplishing its transmission. The valuation is a private information to the user, and should be kept confidential. The user requests a channel by submitting a *bid* $b_n$, which is based on its valuation $v_n$. Based on the lowest bid in group $g$ and the number of bidders $|\mathbb{N}_g|$ in that group, the group bid $\beta_g$ is calculated as

$$\beta_g = |\mathbb{N}_g| \times \min_{n\in\mathbb{N}_g} b_n. \tag{1}$$

Upon receiving all the group bids, the auctioneer sorts them in non-increasing order, i.e., $\beta'_1 \geq \beta'_2 \geq \cdots \geq \beta'_G$, and announces the top $w = \min(M, G)$ groups as the winning groups, which is denoted by $\mathbb{W}$. Certainly, the corresponding users in those groups are the winning users. All the selected winning groups are equally charged, the charge price is decided by the $(w+1)$-th highest group bid $\beta'_{w+1}$ to guarantee the truthfulness. Finally, this group charge is evenly shared by all the users in that winning group, therefore each winner $n \in g$ is charged with $p_n = \beta'_{w+1}/\mathbb{N}_g$. Then, the utility $u_n$ of bidder $n$ can be represented by

$$u_n = \begin{cases} v_n - p_n, & n \in \mathbb{W} \\ 0, & \text{otherwise}, \end{cases} \tag{2}$$

For auction mechanism design, truthfulness is one of the most important desirable properties. Without truthfulness, the auction is vulnerable to market manipulation and leads to very poor outcomes. An auction is truthful, if for every participating user, revealing its true valuation is its dominant strategy regardless of other users' strategies.

*Theorem 1: Grouped $w+1$ price spectrum auction is truthful.*

*Proof:* We will show that the bidder cannot improve its utility by bidding a value other than its true valuation. We first consider bidder $n$ is in a winning group. When the bidder bids a higher value than her true valuation, the utility $u_n = v_n - p_n$ will not change since the $(w+1)$th highest bid maintains. When the bidder bids a lower value $b_n$ than her true valuation, if $b_n \geq \beta'_{w+1}$, still the utility will not change; otherwise if $b_n < \beta'_{w+1}$, bidder $n$'s group will lose the auction and her utility will decrease to 0. Next, we consider the case that $n$ is not in a winning group. Obviously, reporting a lower bid than her true valuation will not change her utility which is 0. When bidder $n$ bids a higher value than her true valuation, but $n$'s bid is not the lowest bid in her group, her group bid will not change and thus her utility will still be 0. When bidder $n$ bids a higher value than her true valuation and $n$ holds the lowest bid in her group $g$, she can make her group win. In this case, her utility is $u'_n = v_n - p'_n \leq v_n - \beta'_{w+1}/\mathbb{N}_g \leq v_n - b_n = u_n = 0$.

[1]We will use terms user and device interchangably in the following articles.

[2]In this paper, we only consider the scenario that each device is interested in a single channel. The combinatorial auction that allows user bids more than one channel will be our future work.

**TABLE 1. Notations.**

| Notations | Descriptions |
|---|---|
| $\mathbb{N}$, $\mathbb{G}$, $\mathbb{W}$ | set of users, set of groups, set of winning groups |
| $\mathbb{N}_g$ | set of users in group $g$ |
| $b_n$, $\beta_g$ | bid of user $n$, bid of group $g$ |
| $v_n$, $u_n$ | per channel valuation of user $n$, utility of user $n$ |
| $p_n$ | payment of user $n$ |
| $\mathbb{E}$, $e_j$ | set of possible prices, $j$-th possible price |
| $El(v)$, $El(1)$ | ElGamal encryption on value $v$ and 1 |
| $\vec{a_n}$ | sealed bidding vector of user $n$ |
| $\vec{c_g}$ | element-wise product vector of group $g$ |
| $\phi_g(j)$ | number of elements that equals $v$ in $\vec{a_n}[j]$ |
| $\boldsymbol{M}_g$ | sealed group matrix of group $g$ |
| $\boldsymbol{M}'_g$ | mixed sealed group matrix of group $g$ |
| $e^*$ | clearing price |

To summarize, bidder $n$'s utility would not increase when she offers a bid other than her true valuation. □

Table 1 lists frequently used notations.

### B. EFFICIENT PRIVACY PRESERVING SPECTRUM AUCTION

As we mentioned previously, preserving the users' true valuation is critical, since the auctioneer or malicious bidder may use this information to maximize their own profits and thus harm the interest of normal bidders. However, if there is only one authority carries out the auction, it is extremely hard to keep the users' bid confidential. To this end, besides the auctioneer and bidders, we introduce a third party into the spectrum auction, i.e., CA, who is responsible for generating the public keys. By decrypting the sealed information that received from the auctioneer, CA will determine the winners of the auction and decide their charges. In our considered scenario, *both auctioneer and CA could be untrusted, but we assume that they would not collude.*

Similar to the network model we addressed in the previous subsection, the primary system tries to lease $M$ available channels in exchange for profit. And a secondary user candidate set $\mathbb{N} = \{1, \cdots, n, \cdots, N\}$, (which consists of the users locate outside primary system's exclusion zones) is interested in bidding for the channels. We assume that bidders could not bid at arbitrary prices, and they have to pick a bid from a predefined possible price set $\mathbb{E} = \{e_1, \cdots, e_j, \cdots, e_J\}$, where $e_1 < \cdots < e_j < \cdots < e_J$. We define a binary variable $\chi_{n,j} \in \{0, 1\}$ to denote bidder $n$'s choice on price $e_j$. Therefore, the bid $b_n$ of bidder $n$ is represented by

$$b_n = e_j, \qquad if\ \chi_{n,j} = 1. \tag{3}$$

Since one bidder could not bid at multiple prices, we have $\sum_{j=1}^{J} \chi_{n,j} = 1$.

Inspired by the previous researches [25], [27], [29], we propose an efficient privacy preserving spectrum sharing framework for future IoT system in this paper, which is built upon ElGamal cryptosystem.[3] Fig. 2 illustrates the procedure of the proposed bidding process, and the details are presented in the following parts.

[3]Part of this work was published in our previous work [32].

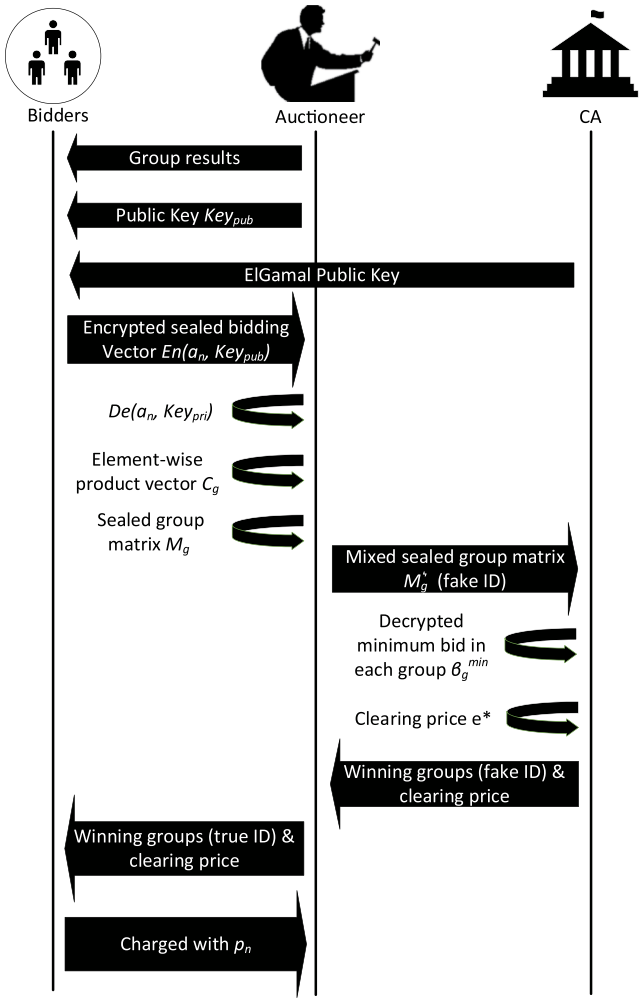



**FIGURE 2. The proposed privacy preserving spectrum auction procedure.**

#### 1) GROUPING (AUCTIONEER ⇒ USERS)

The first step is the auctioneer groups the users that locate outside the exclusion zones to $G$ groups. To guarantee the truthfulness, this grouping process is performed independently with the bidding process, therefore there is no connection between the grouping results and bidding values. As introduced previously, we construct conflict graphs by SINR calculations, and divide groups by graph coloring algorithm. The auctioneer will broadcast the grouping results to all the users in the network. The group set is denoted as $\mathbb{G} = \{1, \cdots, g, \cdots, G\}$, and the set of bidders in group $g$ is denoted as $\mathbb{N}_g$. Regarding the scenario that multiple primary systems with different channels, the exclusion zones could be different, and therefore the group algorithm becomes much more complicated. In this case, since every user's biding channel set is different, directly using graph coloring algorithm is not applicable. To divide the group in this scenario, we could firstly, for every channel, calculate the possible group set by using graph coloring algorithm, and then based on the possible group sets for all the channels, determine the final group result by using greedy algorithm.

#### 2) ENCRYPTED SEALED BIDDING VECTOR (USERS ⇒ AUCTIONEER)

Upon receiving the grouping results, each candidate constructs an *encrypted sealed bidding vector* and submits it to the auctioneer. To construct this vector, two keys are needed, i.e., the key of a public-key cryptography scheme $Key_{pub}$ that is generated by the auctioneer and the public key of ElGamal encryption that is generated by the CA. In order to keep user's bid confidential, every user $n$ firstly constructs a *sealed bidding vector* $\vec{a}_n$ instead of her bidding plaintext $b_n$ as

$$\begin{aligned}\vec{a}_n &= \{\vec{a}_n[1], \cdots, \vec{a}_n[j], \cdots, \vec{a}_n[J]\} \\ &= \left\{ \underbrace{El(v), \cdots, El(v)}_{j}, \underbrace{El(1), \cdots, El(1)}_{J-j} \right\}, \ if \ \chi_{n,j} = 1.\end{aligned} \tag{4}$$

where $El(v)$ and $El(1)$ denote the ElGamal encrypted ciphertexts of public values $v$ ($v \neq 1$) and 1, respectively. Since the ElGamal encryption key is generated by the CA, the auctioneer is unaware of the real bidding value. The only party in the framework that could decrypt the sealed bidding vector is CA, since he has the ElGamal private key. Notice that even for the same value $v$ (or 1), the generated ciphertext $El(v)$ (or $El(1)$) in different time is different, thanks to the randomizability of ElGamal cryptosystem. Therefore, *all the elements in the constructed sealed bidding vector* $\vec{a}_n$ *are indistinguishable*. In other words, to obtain $j$, i.e., the number of $El(v)$ elements in $\vec{a}_n$, it is a must to decrypt the sealed bidding vector by using ElGamal private key.

To prevent that the CA overhears and decrypts the original bid $b_n$, all the bidders further encrypt their sealed bidding vectors by using the public key that broadcasted by the auctioneer and send it to the auctioneer. The message is denoted as $Encrypt(\vec{a}_n, Key_{pub})$, namely the encrypted sealed bidding vector.

#### 3) MIXED SEALED GROUP MATRIX (AUCTIONEER ⇒ CA)

As long as the auctioneer receives the encrypted sealed bidding vectors from bidders, it firstly decrypts $\vec{a}_n$ by using its private key, i.e., $Decrypt(\vec{a}_n, Key_{pri})$. Then based on the already announced grouping result, she constructs an *element-wise product vector* $\vec{c}_g$ for each group $g$ as follows.

$$\begin{aligned}\vec{c}_g &= \left\{\vec{c}_g[1], \cdots, \vec{c}_g[j], \cdots, \vec{c}_g[J]\right\} \\ &= \left\{ \prod_{n\in\mathbb{N}_g} \vec{a}_n[1], \cdots, \prod_{n\in\mathbb{N}_g} \vec{a}_n[j], \cdots, \prod_{n\in\mathbb{N}_g} \vec{a}_n[J] \right\}.\end{aligned} \tag{5}$$

Notice that according to the homomorphic property of the ElGamal cryptosystem, we could derive the following relations.

$$\vec{c}_g[j] = \prod_{n\in\mathbb{N}_g} \vec{a}_n[j] = El(v)^{\phi_g(j)} = El(v^{\phi_g(j)}), \tag{6}$$

where $\phi_g(j)$ indicates that how many $\vec{a}_n[j]$'s plaintext is $v$ for all $n \in \mathbb{N}_g$. Next, based on the vector $\vec{c}_g$, the auctioneer constructs a *sealed group matrix* $\boldsymbol{M}_g$ for group $g$ as follows.

$$\begin{aligned}&\boldsymbol{M}_g \\ &= \left\{\boldsymbol{m}_{g,1}, \cdots, \boldsymbol{m}_{g,j}, \cdots, \boldsymbol{m}_{g,J}\right\} \\ &= \begin{Bmatrix} \left(\vec{c}_g[1]/El(1)\right)^{r_{1,1}} & \cdot & \left(\vec{c}_g[J]/El(1)\right)^{r_{1,J}} \\ \left(\vec{c}_g[1]/El(v)\right)^{r_{2,1}} & \cdot & \left(\vec{c}_g[J]/El(v)\right)^{r_{2,J}} \\ \vdots & & \vdots \\ \left(\vec{c}_g[1]/El(v^{|\mathbb{N}_g|-1})\right)^{r_{|\mathbb{N}_g|,1}} & \cdot & \left(\vec{c}_g[J]/El(v^{|\mathbb{N}_g|-1})\right)^{r_{|\mathbb{N}_g|,J}} \end{Bmatrix}\end{aligned} \tag{7}$$

where $r_{i,j}$ is a random generated number.

Finally, to break the correspondence between $\boldsymbol{M}_g[i,j]$ and $\left(\vec{c}_g[j]/El(v^{(i-1)})\right)^{r_{i-1,j}}$, we create a *mixed sealed group matrix* $\boldsymbol{M'}_g = \{\boldsymbol{m'}_{g,1}, \cdots, \boldsymbol{m'}_{g,j}, \cdots, \boldsymbol{m'}_{g,J}\}$. Here, $\boldsymbol{m'}_{g,j}$ is constructed by permutating the elements in each $\boldsymbol{m}_{g,j}$ randomly. The mixed sealed group matrix $\boldsymbol{M'}_g$, with fake group IDs[4] will be transferred from the auctioneer to the CA.

#### 4) WINNERS & CLEARING PRICE (CA ⇒ AUCTIONEER)

Based on the received mixed sealed group matrix $\boldsymbol{M'}_g$, CA could only decrypt the minimum bid in group $g$, i.e., $\beta_g^{min}$ without gaining any information regarding the other bids in group $g$. Specifically, CA uses her ElGamal private key to decrypt the elements in $\boldsymbol{m'}_{g,j}$. We have $\beta_g^{min} \leq e_{j-1}$, if $\exists\ 0 \leq i \leq |\mathbb{N}_g| - 1$ let $Decrypt\left(\left(\vec{c}_g[j]/E(v^{(i-1)})\right)^{r_{i-1,j}}\right) = 1$, otherwise $\beta_g^{min} > e_{j-1}$. Therefore, we can obtain $\beta_g^{min} = e_{j^*-1}$ by finding a $\boldsymbol{m'}_{g,j^*}$ with the smallest $j^*$ that has the element with plaintext equal to 1. This searching process could be speed up by using binary search tree algorithm.

Based on Eqn. (1), the group $g$'s bid $\beta_g$ is

$$\beta_g = \beta_g^{min} \cdot |\mathbb{N}_g| = e_{j^*-1} \cdot |\mathbb{N}_g|. \tag{8}$$

Notice that during this whole decryption process, CA can only obtain the information of $\beta_g^{min}$. Other bidding values in the group are kept confidential.

Based on the decrypted group bids $\{\beta_1, \beta_2, \cdots, \beta_g, \cdots, \beta_G\}$, all the groups could be sorted in non-increasing order with random tie-breaking. The *clearing price* $e*$ is set with the $(w+1)-$th group bid $\beta'_{w+1}$ on this ordered list. Based on this price, we have the *winning group set* $\mathbb{W}$ as

$$\mathbb{W} = \left\{g \mid 1 \leq g \leq G,\ \beta_g > e*\right\}, \tag{9}$$

Notice that the auction may fail when the first $w+1$ groups on the ordered list all have the same group bid. In that rare case, the auctioneer could initiate a new round auction by using a different grouping result. Finally, the information about winning group set $\mathbb{W}$ (with fake IDs) and clearing price $e*$ will be transferred from the CA to the auctioneer.

[4]Whether or not to use fake group IDs are optional. Here we simply consider that the auctioneer is the only authorized party in the framework that could announce the auction results.

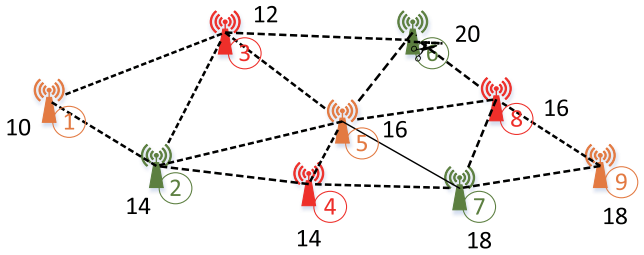



**FIGURE 3.** A scenario consisting of 9 users.

#### 5) PUBLICATIONS AND CHARGES (USERS ⇔ AUCTIONEER)

For the last step, the auctioneer converts the fake group IDs into the true IDs. The winning group, clearing price, and the mapping of winning group to the access channel number, will be published to all the bidders. The bidders in the winning groups evenly share the charge $e^*$, i.e., pays the following amount of money, and start to use the shared channel.

$$p_n = \frac{e^*}{|\mathbb{N}_g|}. \tag{10}$$

In practice, this auction process would be performed periodically in a relatively long interval, e.g., every several minutes, and we assume that during that period the interference condition will not change.

### C. AN ILLUSTRATIVE EXAMPLE

We use the scenario shown in Fig. 1 to illustrate how the proposed framework works. We consider a simple example with 9 users that locate outside the exclusion zone compete for 2 channels. Firstly, we construct a conflict graph by SINR calculation, and the users could be split into 3 groups. One grouping result is shown in Fig. 3, and the users with the same color belong to the same group. Specifically, group *orange*: users $\{1, 5, 9\}$, group *green*: users $\{2, 6, 7\}$, and group *red*: users $\{3, 4, 8\}$. In this example, we assume that there are only 6 possible prices that the users could bid, and the price set $\mathbb{P}$ is $\{10, 12, 14, 16, 18, 20\}$. In Fig. 3, the values besides the users denote their bids, and all the bids must be selected from the price set $\mathbb{P}$. To keep the users' bid confidential, user $n$ encrypts her bid to a sealed bidding vector $\vec{a}_n$ according to Eqn. (4). For instance, the users $\{1, 5, 9\}$ (group *orange*) have the bids 10, 16, 18, respectively, and they are converted to the following sealed bidding vectors.

$$\begin{aligned}
\vec{a}_1 &= \{El(v), El(1), El(1), El(1), El(1), El(1)\},\\
\vec{a}_5 &= \{El(v), El(v), El(v), El(v), El(1), El(1)\},\\
\vec{a}_9 &= \{El(v), El(v), El(v), El(v), El(v), El(1)\}.
\end{aligned}$$

Recall that thanks to the randomizability of the ElGamal cryptosystem, all the ciphertexts $El(v)$ and $El(1)$ are encrypted independently. Therefore, without ElGamal private key, there is no way to tell how many $El(v)$ (or $El(1)$) are in $\vec{a}_n$. To prevent the CA overhears and decrypts the sealed bidding vector, an encrypted version of $\vec{a}_n$ is sent by using another public key generated by the auctioneer, i.e., $Encrypt(\vec{a}_n, Key_{pub})$. After the transfering, the auctioneer decrypts $\vec{a}_n$ by using her private key as $Decrypt(\vec{a}_n, Key_{pri})$.

Next, based on Eqn. (5), the auctioneer calculates the element-wise product vector $\vec{c}_g$ for each group $g$ by using $\vec{a}_n$. For instance, the element-wise product vector for the group *orange* would be

$$\vec{c}_{orange} = \{El(v^3), El(v^2), El(v^2), El(v^2), El(v), El(1)\}.$$

Then, based on Eqn. (7), the auctioneer further converts it to a sealed group matrix $\boldsymbol{M}_g$ for group $g$. For instance, the sealed group matrix for group *orange* would be $\boldsymbol{M}_{orange}$, as shown at the bottom of this page. Finally, the auctioneer sends the mixed sealed group matrix $\boldsymbol{M'}_g$ to the CA, which is converted from $\boldsymbol{M}_g$ by permuating the elements in each column vector.

Finally, CA decrypts $\boldsymbol{M'}_g$ by using her ElGamal private key. By using the binary search tree algorithm, CA could find the minimum $p^*$ that $\boldsymbol{m'}_{g,j^*}$ has the element with plaintext 1. Based on the obtained $p^*$, the minimum bid in group $g$ as $\beta_g^{min} = e_{j^*-1}$ could be easily calculated. For instance, we could decrypt the minimum bid in group *orange* as

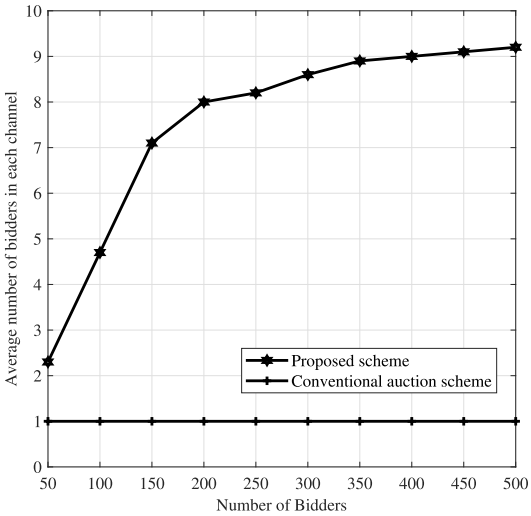
$$\beta_{orange}^{min} = e_1 = 10,$$

by using decryption $Decrypt\left(\left(\frac{El(v^2)}{El(v^2)}\right)^{r_{3,2}}\right) = 1$, and finding the minimum $j$ is 2. Based on Eqn. (8), CA calculates the group bids, e.g., $\beta_{orange} = 10 \times 3 = 30$, $\beta_{green} = 14 \times 3 = 42$ and $\beta_{red} = 12 \times 3 = 36$. Since in this example, $w = \min(M, G) = \min(2, 3) = 2$, the clearing price is set to $e^* = 30$, and the winning group set $\mathbb{W}$ consists of groups *green* and *red*. This clearing price will be shared by the users in the winning group. For instance, users $\{2, 6, 7\}$ in winning group *green* and the users $\{3, 4, 8\}$ in winning group *red* pay for the charges with $e^*/3 = 10$.

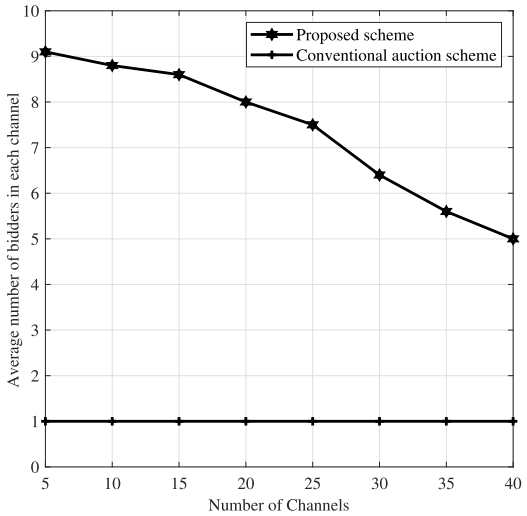
## IV. PERFORMANCE EVALUATIONS

In this section, we evaluate the proposed efficient privacy preserving spectrum sharing framework by simulations. The evaluation metrics include spectrum utilization efficiency, user satisfactory ratio, computation overhead and communication overhead. The considered scenario is

$$\boldsymbol{M}_{orange} = \left\{ \begin{array}{cccccc}
\frac{El(v^3)^{r_{11}}}{El(1)}, & \frac{El(v^2)^{r_{12}}}{El(1)}, & \frac{El(v^2)^{r_{13}}}{El(1)}, & \frac{El(v^2)^{r_{14}}}{El(1)}, & \frac{El(v)^{r_{15}}}{El(1)}, & \frac{El(1)^{r_{16}}}{El(1)} \\
\frac{El(v^3)^{r_{21}}}{El(v)}, & \frac{El(v^2)^{r_{22}}}{El(v)}, & \frac{El(v^2)^{r_{23}}}{El(v)}, & \frac{El(v^2)^{r_{24}}}{El(v)}, & \frac{El(v)^{r_{25}}}{El(v)}, & \frac{El(1)^{r_{26}}}{El(v)} \\
\frac{El(v^3)^{r_{31}}}{El(v^2)}, & \frac{El(v^2)^{r_{32}}}{El(v^2)}, & \frac{El(v^2)^{r_{33}}}{El(v^2)}, & \frac{El(v^2)^{r_{34}}}{El(v^2)}, & \frac{El(v)^{r_{35}}}{El(v^2)}, & \frac{El(1)^{r_{36}}}{El(v^2)}
\end{array} \right\}$$




(a) Impact of number of bidders. (number of channels = 20)




(b) Impact of number of channels. (number of bidders = 200)

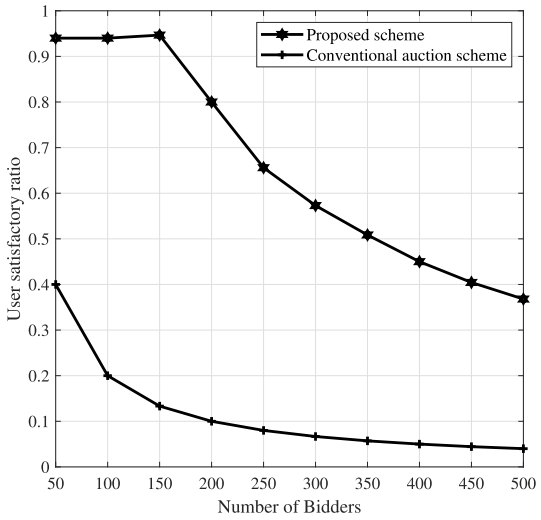
**FIGURE 4. Channel utilization efficiency. (a) Impact of number of bidders. (number of channels = 20). (b) Impact of number of channels. (number of bidders = 200).**

a $1500m \times 1500m$ square area, with multiple users randomly distributed. We assume the primary transmitter locates in the top right corner, and thus the surrounding $350m \times 350m$ area is considered as the exclusion zone. The number of primary system's channels, number of possible prices, number of bidders are set to 20, 1000 and 500, respectively, unless explicitly stated otherwise. Similar to the setting in [33], we set the interference range to 1.7 times of the outdoor transmission range of IEEE 802.11n which is $425m$. We average the simulation results by 100 trials with randomly generated user locations and bidding values.

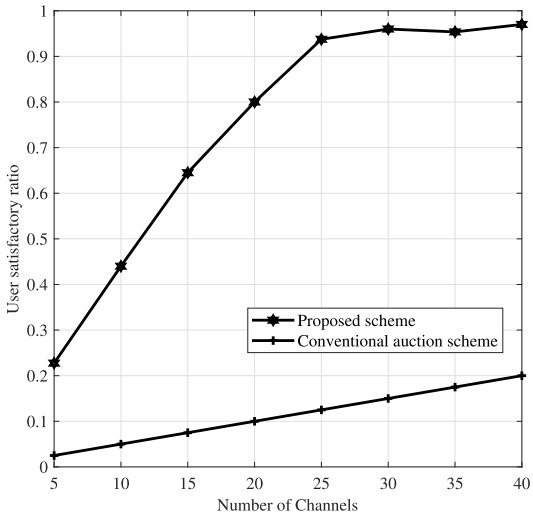
Firstly, in Fig. 4, we compare the proposed scheme with the privacy preserving conventional goods auction scheme [25] in terms of channel utilization efficiency. Here, the channel utilization efficiency is defined as the average number of users that share the same channel. In Fig. 4a, the number of channels is set to 20, and the number of bidders are varied from 50 to 500. As expected, for the proposed framework, the channel utilization efficiency increases when the number of bidders raises. Based on our scenario and inference range settings, we can infer that one group could consist of roughly 9 users without interference at most. Therefore, when the number of bidders increases, the channel utilization efficiency will approximate to this value. And regarding the cases that there is only small number of bidders, the channel is oversupplied obviously. In Fig. 4b, the number of bidders are set to 200, and the number of channels are varied from 5 to 40. We could observe that when the number of channel is small, e.g., 5 channels, the competition among the bidders becomes intense, and it would be easier to construct a group with more users. It is clear that the channel utilization efficiency of the proposed framework outperforms the one of the conventional privacy preserving auction scheme [25].

Secondly, we evaluate the proposed scheme on users' satisfactory ratio and show the results in Fig. 5. Here, the satisfactory ratio indicates the ratio of bidders who win the auction and thus could access the primary system's spectrum. Fig. 5a illustrates the satisfactory ratio varies with the number of bidders, when the number of channel is fixed to 20. We can see that when the number of bidders is less than 150, over 90% user satisfactory ratio could be achieved. This result is expected due to competitions among bidders are not very intense in that setting, and the 10% unsatisfied users are mainly locate inside the exclusion zones. When the number of bidders increases, the satisfactory ratio of both the proposed scheme and conventional auction scheme decrease, which means more and more bidders cannot win the auction. In Fig. 5b, we fix the number of bidders to 200, and change the number of channels from 5 to 40. We could observe that 25 channels or more could satisfy almost all 200 bidders. Finally, compared to conventional auction scheme, the proposed scheme could greatly improve the users' satisfactory ratio by taking into consideration the spectrum reusability.

Next, we illustrate the proposed scheme's computation overhead in Fig. 6. The prime number used in ElGamal encryption function is set to 128 bits. We adopt an evaluation environment with Intel Core i7-3770 CPU at 3.4 GHz. We compare the computation overhead for different parties, i.e., auctioneer, CA and bidder. From the results shown in Figs. 6a and 6b, we can observe that the auctioneer and CA's computation overheads increase linearly. It is confirmed that the ElGamal encryption and decryption processes contribute to this overhead mostly. We observe that the computation overhead at auctioneer is the heaviest, e.g., 21.2 seconds in the scenario with 500 bidders and 1000 possible prices. For each group $g$, the encryption overhead is proportional with $|\mathbb{N}_g| \times P$ times. The computation overhead at CA is much lower than that of auctioneer, e.g., 6.1 seconds in the same scenario. The reason is that the ElGamal decryption times is much smaller than the ElGamal encryption times, since we

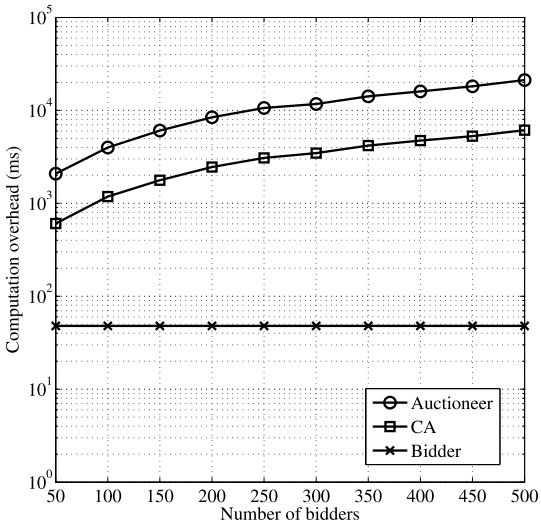



(a) Imapct of number of bidders. (number of channels = 20)

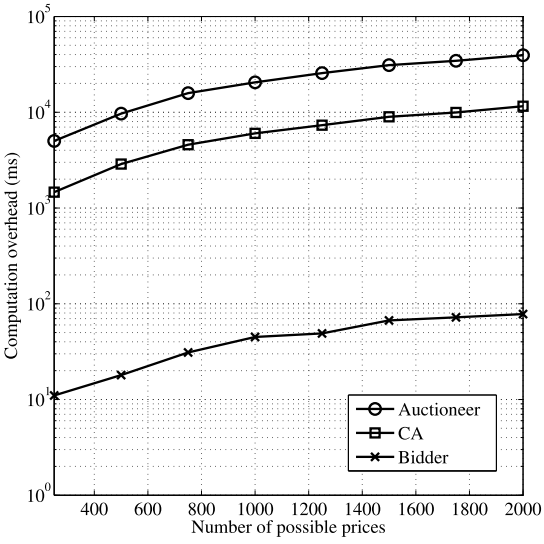



(b) Impact of number of channels. (number of bidders = 200)

**FIGURE 5.** Users' satisfactory ratio.




(a) Impact of number of bidders. (number of possible prices = 1000)

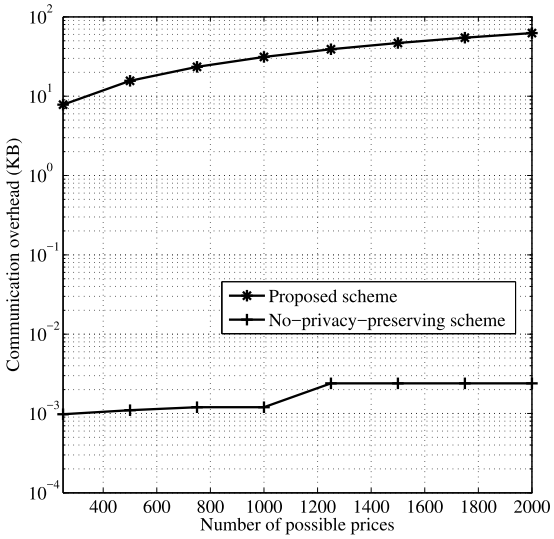



(b) Impact of number of possible prices. (number of bidders = 500)

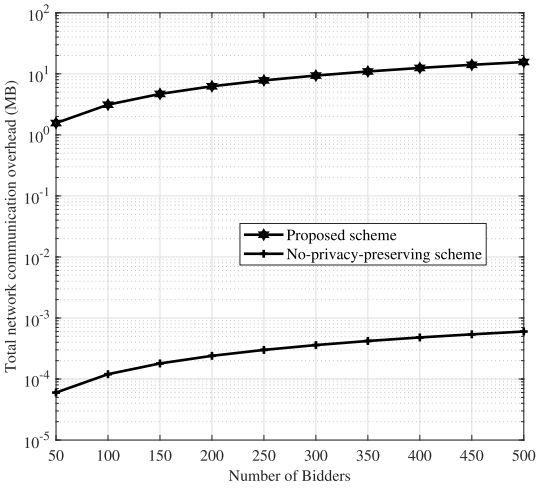
**FIGURE 6.** Computation overhead.

use binary search tree algorithm to find the minimum bid in each group instead of decrypting all the elements. At last, we can see that the computation time in individual bidder is comparatively small, e.g., 0.05 seconds in the same scenario. Therefore, we can conclude that the proposed framework is feasible for the low-cost IoT devices. Notice that in our simulation, we do not use any multithreading functions, which could speed up the computation time. Based on our simulation results, the proposed efficient spectrum sharing framework is totally feasible for IoT scenario, since the heavy computation tasks are carried on powerful auctioneer and CA. And because the computation time is at the scale of dozens of seconds, we could expect the proposed framework works well if the spectrum auction is performed in comparatively long-term scale, e.g., every 30 minutes.

Finally, Fig. 7 illustrates the evaluation results in terms of communication overhead by comparing the proposed scheme with no-privacy-preserving spectrum auction scheme [5]. Since the data transfer between auctioneer and CA could be wired, we only focus on the bidder's communication overhead. For the no-privacy-preserving scheme, the payload for the bidding information is extremely low. For instance, when the number of possible prices $P = 1000$, the no-privacy-preserving scheme only needs to transmit a packet with 10 bits. Notice that here we do not consider the control header overhead for both schemes. From the single user communication overhead result shown in Fig. 7a, the communication overhead of the proposed framework reaches 62.5 KB when $P = 2000$. The majority of this overhead comes from the ElGamal ciphertext for every possible price.




(a) Single user communication overhead.




(b) Network total communication overhead. (1000 possible price)

**FIGURE 7.** **Communication overhead.**

However, it is considered that this amount of communication overhead is acceptable even for low-cost IoT devices, since the bidding process is carried out in a comparatively long period. Furthermore, Fig. 7b illustrates the network total communication overhead. The communication overhead for the whole wireless network of the proposed scheme reaches 15.625 Mb, but that of the no-privacy-preserving scheme is still lower than 1 Kb.

## V. CONCLUSION

In this paper, we have proposed an auction-based efficient privacy preserving spectrum sharing framework for IoT systems. The proposed auction framework enables an efficient and profitable allocation of underutilized spectral resources by taking into consideration the spectrum reusability. The truthfulness of the proposed spectrum auction scheme has been proved, therefore revealing the true valuation is every bidder's dominant strategy. The proposed framework utilizes the ElGamal cryptosystem to only reveal the groups' bid but keep the bidders' bids confidential. The evaluation results validate that the proposed framework could achieve high spectrum utilization efficiency and user satisfactory ratio, at acceptable communication and computation costs.

## REFERENCES

[1] L. Zhang, Y.-C. Liang, and M. Xiao, "Spectrum sharing for Internet of Things: A survey," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 132–139, Jun. 2019.
[2] Z. Zhou, J. Feng, L. Tan, Y. He, and J. Gong, "An air-ground integration approach for mobile edge computing in IoT," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 40–47, Aug. 2018.
[3] Z. Zhou, Y. Guo, Y. He, X. Zhao, and W. M. Bazzi, "Access control and resource allocation for M2M communications in industrial automation," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3093–3103, May 2019.
[4] C. Zhang and Z. Zheng, "Task migration for mobile edge computing using deep reinforcement learning," *Future Gener. Comput. Syst.*, vol. 96, pp. 111–118, Jul. 2019.
[5] X. Zhou and H. Zheng, "TRUST: A general framework for truthful double spectrum auctions," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 999–1007.
[6] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "TAHES: A truthful double auction mechanism for heterogeneous spectrums," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 4038–4047, Nov. 2012.
[7] C. Yi and J. Cai, "Multi-item spectrum auction for recall-based cognitive radio networks with multiple heterogeneous secondary users," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 781–792, Feb. 2015.
[8] X. Wang, Y. Ji, H. Zhou, and J. Li, "A nonmonetary QoS-aware auction framework toward secure communications for cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5611–5623, Jul. 2016.
[9] Z. Zhou, M. Dong, K. Ota, G. Wang, and L. T. Yang, "Energy-efficient resource allocation for D2D communications underlaying cloud-RAN-based LTE–a networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 428–438, Jun. 2016.
[10] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA, USA: MIT Press, 1991.
[11] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proc. 1st ACM Conf. Electron. Commerce (EC)*, 1999, pp. 129–139.
[12] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, no. 1, pp. 8–37, Mar. 1961.
[13] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jun. 1985.
[14] C. Phillips, M. Ton, D. Sicker, and D. Grunwald, "Practical radio environment mapping with geostatistics," in *Proc. IEEE Int. Symp. Dynamic Spectr. Access Netw.*, Oct. 2012, pp. 422–433.
[15] A. Nika, Z. Zhang, X. Zhou, B. Y. Zhao, and H. Zheng, "Towards commoditized real-time spectrum monitoring," in *Proc. 1st ACM Workshop Hot Topics Wireless (HotWireless)*, 2014, pp. 25–30.
[16] D.-H. Shin, S. He, and J. Zhang, "Joint sensing task and subband allocation for large-scale spectrum profiling," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 433–441.
[17] Z. Zhou, H. Liao, B. Gu, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, "Robust mobile crowd sensing: When deep learning meets edge computing," *IEEE Netw.*, vol. 32, no. 4, pp. 54–60, Jul. 2018.
[18] A. Ullah, S. Bhattarai, J.-M. Park, J. H. Reed, D. Gurney, and B. Bahrak, "Multi-tier exclusion zones for dynamic spectrum sharing," in *Proc. IEEE Int. Conf. Commun.(ICC)*, Jun. 2015, pp. 7659–7664.
[19] S. Bhattarai, A. Ullah, J.-M.-J. Park, J. H. Reed, D. Gurney, and B. Gao, "Defining incumbent protection zones on the fly: Dynamic boundaries for spectrum sharing," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, Sep. 2015, pp. 251–262.
[20] X. Wang, Y. Ji, H. Zhou, and J. Li, "Auction-based frameworks for secure communications in static and dynamic cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2658–2673, Mar. 2017.
[21] X. Wang, M. Umehira, P. Li, Y. Gu, and Y. Ji, "Fine-grained incentive mechanism for sensing augmented spectrum database," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[22] X. Wang, M. Umehira, P. Li, Y. Gu, and Y. Ji, "Incentivizing crowdsourcing for exclusion zone refinement in spectrum sharing system," in *Proc. 23rd Asia–Pacific Conf. Commun. (APCC)*, Dec. 2017, pp. 1–6.
[23] X. Wang, M. Umehira, B. Han, P. Li, Y. Gu, and C. Wu, "Online incentive mechanism for crowdsourced radio environment map construction," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[24] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. 27th Annu. Symp. Found. Comput. Sci. (SFCS)*, Oct. 1986, pp. 162–167.
[25] M. Abe and K. Suzuki, "M + 1-st price auction using homomorphic encryption," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. E86-A, vol. 1, pp. 136–141, Jan. 2003.
[26] K. Sako, "An auction protocol which hides bids of losers," in *Proc. 3rd Int. Workshop Pract. Theory Public Key Cryptogr.*, Jan. 2000, pp. 422–432.
[27] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 866–876, Apr. 2011.
[28] M. Pan, X. Zhu, and Y. Fang, "Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer," *Wireless Netw.*, vol. 18, no. 2, pp. 113–128, Feb. 2012.
[29] F. Wu, Q. Huang, Y. Tao, and G. Chen, "Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks," *IEEE/ACM Trans. Netw.*, vol. 23, no. 4, pp. 1271–1285, Aug. 2015.
[30] X. Zhou, Z. Zhang, G. Wang, X. Yu, B. Y. Zhao, and H. Zheng, "Practical conflict graphs for dynamic spectrum distribution," *SIGMETRICS Perform. Eval. Rev.*, vol. 41, no. 1, p. 5, Jun. 2013.
[31] D. B. West, *Introduction to Graph Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 2000.
[32] X. Wang, Y. Ji, H. Zhou, Z. Liu, Y. Gu, and J. Li, "A privacy preserving truthful spectrum auction scheme using homomorphic encryption," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
[33] M. Cheng, X. Gong, and L. Cai, "Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3770–3779, Jul. 2009.

**XIAOYAN WANG** (Member, IEEE) received the B.E. degree from Beihang University, China, and the M.E. and Ph.D. degrees from the University of Tsukuba, Japan. From 2013 to 2016, he worked as an Assistant Professor (by special appointment) with the National Institute of Informatics (NII), Japan. He is currently working as an Assistant Professor with the Graduate School of Science and Engineering, Ibaraki University, Japan. His research interests include networking, wireless communications, cloud computing, big data systems, and security and privacy.

**MASAHIRO UMEHIRA** (Member, IEEE) received the B.E., M.E., and Ph.D. degrees from Kyoto University, Kyoto, Japan, in 1978, 1980, and 2000, respectively. Since joining NTT (Nippon Telegraph and Telephone Corporation) in 1980, he has been engaged in the research and development of modem and TDMA equipment for satellite communications, TDMA satellite communication systems, broadband wireless access systems for mobile multimedia services, and ubiquitous wireless systems. From 1987 to 1988, he was with the Communications Research Center, Department of Communications, Canada, as a Visiting Scientist. Since 2006, he has been a Professor with Ibaraki University, Ibaraki, Japan. His research interests include broadband wireless access technologies, wireless networking, cognitive radio, future satellite communication systems, and wireless-based ubiquitous systems. He received the Young Engineer Award and the Achievement Award from IEICE, in 1987 and 1999, respectively, the Education, Culture, Sports, Science and Technology Minister Award, in 2001, and the TELECOM System Technology Award from the Telecommunications Advancement Foundation, in 2003.

**BIAO HAN** (Member, IEEE) received the B.S. and M.S. degrees from the National University of Defense Technology (NUDT), China, in 2007 and 2009, respectively, and the Ph.D. degree in computer science from the University of Tsukuba, Japan, in 2013. He is currently an Associate Professor of computer science with NUDT. He has published over 50 peer-reviewed articles in top journals, such as JSAC, TPDS, ComNets, and TVT, and top conferences, such as INFOCOM and SIGCOMM. His research interests mainly focus on cybersecurity for the IoT and computer networks, including big data privacy, AI-based networking, and wireless communications. He was a recipient of the Best Paper Award at the IEEE LANMAN 2014.

**HAO ZHOU** (Member, IEEE) received the B.S. and Ph.D. degrees in computer science from the University of Science and Technology of China, Hefei, China, in 1997 and 2002, respectively. From 2014 to 2016, he worked as a Project Lecturer with the National Institute of Informatics (NII), Japan. He is currently an Associate Professor with the University of Science and Technology of China. His research interests are in the areas of the Internet of Things, wireless communications, and software engineering.

**PENG LI** (Member, IEEE) received the B.S. degree from the Huazhong University of Science and Technology, China, in 2007, and the M.S. and Ph.D. degrees from the University of Aizu, Japan, in 2009 and 2012, respectively. He is currently an Associate Professor with the University of Aizu. His research interests mainly focus on cloud computing, the Internet of Things, big data systems, as well as related wired and wireless networking problems. He received the Young Author Award of the IEEE Computer Society Japan Chapter, in 2014, and the Best Paper Award of the IEEE TrustCom 2016. He has supervised the students to win the First Prize of the IEEE ComSoc Student Competition,in 2016.

**CELIMUGE WU** (Senior Member, IEEE) received the M.E. degree from the Beijing Institute of Technology, China, in 2006, and the Ph.D. degree from The University of Electro-Communications, Japan, in 2010. He is currently an Associate Professor with the Graduate School of Informatics and Engineering, The University of Electro-Communications. His current research interests include vehicular networks, sensor networks, intelligent transport systems, the IoT, 5G, and mobile cloud computing. He is serving as an Associate Editor for IEEE Access, the *IEICE Transactions on Communications*, the *International Journal of Distributed Sensor Networks*, and *Sensors* (MDPI).