# A Bidder-Oriented Privacy-Preserving VCG Auction Scheme

Maya Larson[1], Ruinian Li[1](✉), Chunqiang Hu[1], Wei Li[1],
Xiuzhen Cheng[1], and Rongfang Bie[2](✉)

[1] Department of Computer Science,
The George Washington University, Washington, D.C., USA
{maya_,ruinian,chu,weili,cheng}@gwu.edu
[2] College of Information Science and Technology,
Beijing Normal University, Beijing, China
rfbie@bnu.edu.cn

**Abstract.** Vickrey-Clarke-Groves (VCG) is a type of sealed-bid auction of multiple items which has good economic properties. However, VCG has security vulnerabilities, e.g. it is vulnerable to auctioneer fraud. To make VCG more practical, bid prices must be well protected. To tackle this challenge, we propose a bidder-oriented, privacy-preserving auction scheme using homomorphic encryption, where the bidders can calculate the results by themselves, and the auctioneer is able to verify the results. Compared to previous research, our scheme is more trustworthy with stronger privacy.

**Keywords:** Privacy-preserving · Homomorphic encryption · VCG

## 1 Introduction

Over past years, auctions have been widely applied to real-world applications [1,9,10,12,14,15,21,23], among which VCG is an important auction mechanism which receives a lot of attention. In VCG, bidders submit their sealed bids without knowing other bids, and each bidder is charged its social opportunity cost. It has been proven that VCG has good economic properties of incentive-compatibility, Pareto-efficiency and individual-rationality [11]. Despite its good economic properties, VCG has security vulnerabilities, one of which is auctioneer fraud. For example, if an auctioneer knows the highest bid, he can create a fake bid which is very close to the highest bid, thus gaining more profits.

To tackle this problem, we propose a bidder-oriented privacy-preserving VCG scheme based on homomorphic encryption. In previous work using homomorphic encryption [19,25], the bids are encrypted with the auctioneer's public key, and all the computations are done on the auctioneer's side. This is not secure because the auctioneer has all the information needed to get bidders' information. Different from previous work, we let the bidders calculate the results by themselves, and the auctioneer is only able to verify the results. In our scheme, each bid is

K. Xu and J. Zhu (Eds.): WASA 2015, LNCS 9204, pp. 284–294, 2015.
DOI: 10.1007/978-3-319-21837-3_28

encrypted twice, first by the auctioneer's public key and then a group key. The auctioneer is not able to see the contents of bids without the group key. The computed result can be verified by the auctioneer to make sure that it is correct. Compared to previous work, our scheme provides stronger privacy.

The contribution of this paper can be summarized as follows:

- We propose a bidder-oriented privacy-preserving VCG auction scheme using homomorphic encryption. This scheme achieves high privacy because it does not need a trusted third party. Furthermore, even the auctioneer is not supposed to be trusted in this scheme.
- We analyze the security and privacy protection of our scheme, and discuss how it achieves correctness, confidentiality, and verification.

The remainder of the paper is organized as follows: In Sect. 2, we introduce related work. In Sect. 3, we outline the most important preliminaries. In Sect. 4, we present our scheme in detail. In Sect. 5, we discuss the scheme from the following angles: security analysis, limitations, and how to easily adapt our scheme for a first-price auction. Finally, we give a conclusion in Sect. 6.

## 2 Related Work

Much work has been done to ensure the security and user privacy of auctions, in which the common cryptographic tools are secret sharing [3,22], homomorphic encryption, and hash functions.

Kobayashi, Morita and Suzuki use hash chains to form a sealed-bid auction [10,23]. H.Kikuchi proposed (m+1)-st price auction with secret sharing, which is a useful cryptographic tool and is utilized in many applications such as body area networks [5,7], attribute-based encryption [6,7], image security [4] and so on. Later, Suzuki and Yokoo combine dynamic programming and secret sharing to build a secure auction scheme [24]. However, the scheme only works in passive adversary models, and the evaluators have to obtain their shares from a third party via a secure channel. Nojoumian *et al.* applies verifiable secret sharing to construct sealed-bid auctions in [16], but this scheme also requires a secure channel and it can not resist collusion attacks between evaluators and the third parties. Larson *et al.* [12] present a scheme to secure auctions without an auctioneer via verifiable secret sharing. The scheme can resist passive attacks and collusion attacks and does not require a secure channel. A truthful and privacy preserving auction mechanism called SPRING was proposed in [8], and this scheme introduces a trust-worthy agent to interact with the auctioneer and the bidders. An obvious weakness is that there is a trusted third party in this system.

Leveraging homomorphic encryption to protect bidder's privacy is not a new idea. In [21], Goldwasser-Micali encryption is used to design a new sealed-bid auction. In [1], a secure McAfee double auction scheme is proposed using homomorphic encryption for spectrum auctions. In [20], a new proof technique is explored to improve efficiency and privacy of homomorphic e-auction applications. Larson *et al.* employ homomorphic encryption to protect the security and privacy in first price auctions [13]. There is also some research on leveraging homomorphic encryption to secure VCG, such as [18,19,25]. However, in the previous research, all the computations are done on the auctioneer's side, and the auctioneer holds the secret key for decryption. These schemes are not secure unless the auctioneer can be completely trusted.

In this paper, we propose a bidder-oriented privacy-preserving VCG auction scheme using homomorphic encryption. The bidders calculate the final result by themselves, and the auctioneer decrypts this result and broadcasts it to the bidders. During this process, the auctioneer does not need to have the bids, thus the privacy of the bidders is highly protected. Furthermore, the results from the bidders can be verified. The correctness of the scheme is determined by the majority of the bidders.

## 3 Preliminaries

### 3.1 Homomorphic Encryption

Homomorphic encryption is an important cryptographic primitive where the computation party can operate on the ciphertext, without seeing the contents of the plaintext. In our scheme, we adopt multiplicative homomorphic encryption, such as pallier cryptosystem [17] and ElGamal cryptosystem [2]. More generally, given an encryption function $E$, $E(x_1 \cdot x_2) = E(x_1) \cdot E(x_2)$. With this property, encrypted data could be processed without knowing the plaintext. Furthermore, different ciphertexts from the same plaintext are indistinguishable, which means that no one can succeed in distinguishing the corresponding plaintext with a probability much higher than 1/2. With these properties, Pallier or ElGamal cryptosystem are fit for privacy-preserving systems.

### 3.2 VCG Auction

In this subsection, we explain the details of VCG auction.

We consider a market with a set of g goods: $G = 1, 2, 3, ...i...g$, and a set of of $b$ bidders: $B = \{1, 2, 3, ...i...b\}$. Consequently, the set of allocations of goods $G$ to bidders in $B$ is denoted as: $S = \{A : B \rightarrow G\}$. Suppose the bidder i's evaluation function is $b_i$ where $b_i = S \rightarrow Z^+$, then bidder i's bid value for each assignment is denoted as $b_i(A)$. Therefore, $b_i(S)$ represents the set of bid i's bid values for all possible allocations:

$$b_i(S) = \{b_i(S_1), b_i(S_2), b_i(S_3), ..., b_i(S_{|S|})\}, \tag{1}$$

where $|S|$ is the number of allocations in the auction.

At the beginning of the auction, each bidder submits his bid $b_i$ to the auctioneer. Based on the VCG auction mechanism, the auctioneer determines the allocation and the clearing prices by the following procedures:

1. *Finding the maximum sum of bid values:* The auctioneer reveals the sealed bid values and determines the allocation that can achieve the maximum sum of bid values, which is denoted as $S^*$.
2. *Computation of the clearing prices:* We use $p_i$ to denote the clearing price of bidder $i$ for $1 \leq i \leq b$:

$$p_i = \max \sum_{j \neq i} b_j(S) - \sum_{j \neq i} b_j(S^*), \tag{2}$$

   in which $\max \sum_{j \neq i} b_j(S)$ is the maximum sum of bid values when bidder $i$ does not join the auction, and $\sum_{j \neq i} b_j(S^*)$ is the sum of bid values for allocation $S^*$ without bidder $i$'s value. Note that $p_i$ is the so-called "social opportunity cost".

   In VCG, as long as the optimal solution $S^*$ is obtained, incentive-compatibility can be guaranteed; that is, for any bidder, the optimal strategy is bidding its true bid value [11]. Thus, by adopting VCG, we simply assume that each bidder submits its true valuation in the auction.

# 4 Proposed Scheme

## 4.1 Requirements

The system for a privacy-preserving auction should meet the following requirements:

1. *Correctness:* The computation result must be correct, and strictly follow the policy of VCG scheme. This should be verifiable.
2. *Confidentiality:* Users' bid values must be encrypted such that neither the auctioneer nor the other bidders can see the original prices.
3. *Verification:* The correctness of the result can be verified, and fake messages from bidders can be detected.

Correctness is the basic requirement, which means that the auction result must strictly follow the policy of VCG. Confidentiality is to guarantee that bidders' privacy is well protected. To achieve this goal, the bids will be encrypted twice with the auctioneer's public key and a group key of the bidders. In this way, the bidders can share their bids for computation, but they still can not see the contents because they are encrypted by the auctioneer's key.

## 4.2 Basic Idea

We utilize a key generation center (KGC) to assign group key $k_g$ to a group of bidders before the auction itself. The KGC also assigns a pair of asymmetric keys $k_p$ and $k_s$ to the auctioneer, and broadcasts the public key $k_p$ to the group of bidders. Each bidder i will first encrypt his own bid using the auctioneers' public key $k_p$, then encrypt the bid again using the group key $k_g$. The encrypted message $E_{k_g}(E_{k_p}(b_i))$ will be shared among this group. Each bidder can decrypt the message received from other bidders, and get $E_{k_p}(b_i)$, but they can not decrypt $E_{k_p}(b_i)$ as they do not know the private key of the auctioneer. Then each bidder is able to perform a computation to find the allocation where the sum of the bidding price is maximized based on the homomorphic property, and sends the result to the auctioneer for decryption. The auctioneer will decrypt the message from the bidders and broadcast the result, $S^*$. Once the result is received from the auctioneer, the bidders use the maximum allocation $S^*$ to perform another homomorphic computation to find the final allocation according to the VCG scheme. Then the bidders send the encrypted results to the auctioneer for decryption. The auctioneer then decrypts the message and obtains the final allocation result.

During this process, the auctioneer is only responsible for decryption, which is the most complicated and time-consuming step. The key characteristic is that the auctioneer only receives the encrypted results which have been processed, rather than the original bid prices. The bidders are responsible for performing homomorphic computations twice during this process. If we suppose there are n bidders in this system, then there will be n copies of results sent to the auctioneer, thus the auctioneer will be able to verify the correctness of the result by checking that the n copies are consistent. In general, the correctness of the system is guaranteed by the whole group of bidders, not a single trusted individual. We assume there is no collusion between the auctioneer and bidders: In this system, each bidder is bidding his true value, and neither the auctioneer nor the bidder know the other bidder's bids. Thus a bidder should not be willing to risk colluding with the auctioneer.

### 4.3 Proposed Scheme

**System Model.** There are three phases: the system initialization, the bidding process, and the computation process. The system model is described in Fig. 1: The KGC constructs a group key and a pair of asymmetric keys. It then sends the secret key $k_s$ to the auctioneer, and sends the public key $k_p$ and the group key $k_g$ to the group of bidders. The bidders in this group share each other's information; all the bidders are able to communicate with the auctioneer.

**System Initialization**

1. KGC constructs a group key $k_g$ and a pair of asymmetric keys in preparation of an auction. Suppose there are $n$ bidders in an auction.
2. The bidders who want to take part in the auction contact the KGC for a registration, and obtain the the group key $k_g$ .
3. The KGC assigns the secret key $k_s$ to the auctioneer and broadcasts the public key $k_p$ to the group of bidders.
4. The auctioneer publishes the set of possible allocations S.

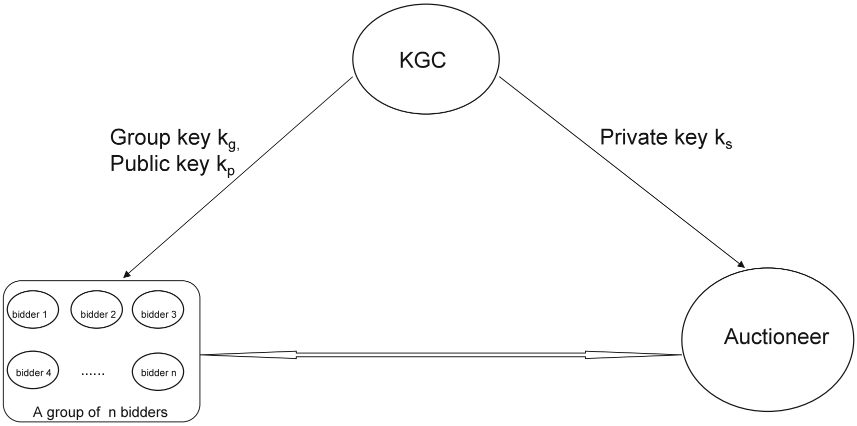

**Fig. 1.** System Model

### Bidding Process

1. Each bidder first applies Pallier or ElGamal method to encrypt his bids using the public key of the auctioneer $k_p$, then encrypts the bids again using the group key$K_g$.

$$\begin{aligned}E_{k_g}(E_{k_p}(b_i(S))) =& E_{k_g}((E_{k_p}(b_i(S_1)), E_{k_p}(b_i(S_2)), E_{k_p}(b_i(S_3)), ...,\\ & E_{k_g}(b_i(S_{|S|})), 1 \leq i \leq n\end{aligned} \tag{3}$$

2. The bidders share their encrypted bids with the other bidders in the same group. Then each bidder decrypts the message received from the others using the group key and obtains $E_{k_p}(b_i)$, where

$$\begin{aligned}E_{k_p}(b_i(S)) =& \{(E_{k_p}(b_i(S_1)), E_{k_p}(b_i(S_2)), E_{k_p}(b_i(S_3)), ...,\\ & E_{k_p}(b_i(S_{|S|})\}, 1 \leq i \leq n\end{aligned} \tag{4}$$

### Computation Process

1. Each bidder computes $\prod_{i=1}^{n} E_{k_p}(b_i(S))$, and sends this set to the auctioneer.
2. The auctioneer decrypts the message from the bidders, and obtains:

$$\begin{aligned}D_{k_s}(\prod_{i=1}^{n} E_{k_p}(b_i(S))) &= D_{k_s}(\prod_{i=1}^{n} E_{k_p}(b_i(S_1)), \prod_{i=1}^{n} E_{k_p}(b_i(S_2)), \prod_{i=1}^{n} E_{k_p}(b_i(S_3)), ...,\\ &\prod_{i=1}^{n} E_{k_p}(b_i(S_{|S|}))\\ &= (\sum_{i=1}^{n} b_i(S_1), \sum_{i=1}^{n} b_i(S_2), \sum_{i=1}^{n} b_i(S_3), ..., \sum_{i=1}^{n} b_i(S_{|S|})\end{aligned} \tag{5}$$

3. Once the plaintext is obtained, the auctioneer can find the allocation $S^*$ which achieves the maximum sum of bid values:

$$S^* = argmax\{\sum_{i=1}^{n} b_i(S_1), \sum_{i=1}^{n} b_i(S_2), \sum_{i=1}^{n} b_i(S_3), ..., \sum_{i=1}^{n} b_i(S_{|S|)}\} \tag{6}$$

   In this step, the auctioneer only needs to decrypt a subset of messages from the group of bidders. The strategy can be designed in a flexible way by the auctioneer; when the auctioneer decrypts a sufficient proportion of the n messages and gets consistent results, it is reasonable to believe that the results are accurate. This solution will guarantee that the computation result from the bidders is correct, as the correctness is determined by the majority of the group. After obtaining the correct $S^*$, the auctioneer broadcasts it to the bidders.
4. Once the bidders obtain $S^*$, they will continue computation according to the VCG scheme. Here, we use $\Delta p_i$ to denote a set of possible prices that the bidder should pay.

$$\begin{aligned} E_{k_p}(\Delta p_i) &= \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))} \\ &= (\frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_1))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_2))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_3))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, ..., \\ &\quad \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_{|S|}))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}) \end{aligned} \tag{7}$$

   Then the computation results from all the bidders will be sent to the auctioneer again for decryption.
5. The auctioneer decrypts the message, and obtains:

$$\begin{aligned} \Delta p_i = D_{k_s}(&\frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_1))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_2))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_3))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, ..., \\ &\frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S_{|S|}))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}) \\ = &\sum_{j\neq i} b_j(S) - \sum_{j\neq i} b_j(S^*) \end{aligned} \tag{8}$$

6. The auctioneer finds the maximum value in this set, which is the price that bidder i would pay:

$$p_i = max\{\Delta p_i\} = max\{\sum_{j\neq i} b_j(S) - \sum_{j\neq i} b_j(S^*)\}$$
$$= max \sum_{j\neq i} b_j(S) - \sum_{j\neq i} b_j(S^*), \tag{9}$$

7. The auctioneer broadcasts the results. The winners pay the auctioneer and receive the corresponding goods.

# 5 Discussion

## 5.1 Correctness

The proposed scheme follows the VCG scheme strictly and the result is correct. In this scheme, the computations are processed on the bidder's side, and the auctioneer is able to decrypt the messages from the bidders and get the result. Unless a large proportion of bidders collude and send the identical wrong results to the auctioneer, the fake result can be detected by the auctioneer. It is reasonable to assume that most of the bidders are honest, and therefore the correctness is guaranteed.

## 5.2 Security Analysis

**Confidentiality.** The bidding prices are encrypted twice: first using the auctioneer's public key, and then using the group key. The bidders cannot see the bids of other bidders because they do not have the auctioneer's private key to decrypt the message. The auctioneer cannot see the original contents of the bids because all the messages sent to the auctioneer have been processed. In this way, the confidentiality of the bids is well protected.

**Verification.** Verification can be achieved in our scheme. As discussed above, the auctioneer can verify the correctness of the computation from the bidders because he receives n copies of results instead of one. Thus the result's correctness is based on the majority of the bidders. Unless the majority of the bidders are cheating in this auction, the correct result will be obtained by the auctioneer.

## 5.3 First-Price Auction

Our proposed scheme can be easily applied to a first-price auction and still maintains correctness, confidentiality and verification. Notice that the third step of our computation process is to find the allocation $S^*$ which maximizes the sum of bid values. This result indicates the clearing prices for all bidders, as the clearing price of each winner is the amount he bids for the item. Specifically, bidder $i$ will know whether he wins an item and how much he should pay for this auction based on $S^*$. Furthermore, non-repudiation is easy to achieve in this process.

For example, suppose the final result shows that bidder $i$ should pay 500 dollars for one item, but bidder $i$ denies that he did bid 500 dollars. Then the auctioneer can request the other bidders to reveal this bidder's original bids and check if it is 500 dollars. Intuitively, this system is under surveillance of all the bidders. In this system, a dishonest bidder can be spotted by the auctioneer and proved to be cheating by other bidders. Unless all other bidders help this dishonest bidder, the auctioneer's profit will be protected. Therefore, non-repudiation can be achieved because none of the bidders in the system is able to deny his behavior.

### 5.4 Limitation

One limitation of our scheme is that it introduces more computations compared to [25], because all the bidders need to perform the computation. However, our scheme offers much higher security levels and brings more trustworthy results to the bidders. This is a trade-off between bidder's privacy and computation efficiency. To alleviate the problem, the bidders could employ a cloud processor to do the computations.

## 6 Conclusion and Future Work

In this paper, we propose a bidder-oriented privacy-preserving VCG auction scheme using homomorphic encryption. This scheme achieves strong privacy by letting the bidders calculate the auction result. The auctioneer gets the final result and is able to verify the correctness. Furthermore, the correctness of this scheme is based on the majority of the bidders, not a trusted party, and all bidder's information is highly protected. Our future research lies in designing a more efficient mechanism to ensure bidders' privacy and data security in VCG auction, which will work better in practical applications.

**Acknowledgment.** The authors would like to thank all the reviewers for their helpful comments. This project was supported by the US National Science Foundation (ECCS-1407986, AST-1443858, CNS-1265311, and CNS-1162057), and the National Natural Science Foundation of China (61171014).

## References

1. Chen, Z., Huang, L., Li, L., Yang, W., Miao, H., Tian, M., Wang, F.: Ps-trust: provably secure solution for truthful double spectrum auctions. In: 2014 IEEE Proceedings on INFOCOM, pp. 1249–1257. IEEE (2014)
2. El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985)

3. Hu, C., Liao, X., Cheng, X.: Verifiable multi-secret sharing based on LFSR sequences. Theor. Comput. Sci. **445**, 52–62 (2012)
4. Hu, C., Liao, X., Xiao, D.: Secret image sharing based on chaotic map and Chinese remainder theorem. Int. J. Wavelets Multiresolut. Inf. Process. **10**(03), 1250023 (1–18) (2012)
5. Hu, C., Zhang, F., Cheng, X., Liao, X., Chen, D.: Securing communications between external users and wireless body area networks. In: Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy, pp. 31–36. ACM (2013)
6. Hu, C., Zhang, F., Xiang, T., Li, H., Xiao, X., Huang, G.: A practically optimized implementation of attribute based cryptosystems. In: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 197–204. IEEE (2014)
7. Hu, C., Zhang, N., Li, H., Cheng, X., Liao, X.: Body area network security: a fuzzy attribute-based signcryption scheme. IEEE J. Sel. Areas Commun. **31**(9), 37–46 (2013)
8. Huang, Q., Tao, Y., Wu, F.: Spring: a strategy-proof and privacy preserving spectrum auction mechanism. In: 2013 IEEE Proceedings on INFOCOM, pp. 827–835. IEEE (2013)
9. Jing, T., Zhao, C., Xing, X., Huo, Y., Li, W., Cheng, X.: A multi-unit truthful double auction framework for secondary market. In: IEEE ICC (2013)
10. Kobayashi, K., Morita, H., Suzuki, K., Hakuta, M.: Efficient sealed-bid auction by using one-way functions. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **84**(1), 289–294 (2001)
11. Krishna, V.: Auction theory. Academic press, San Diego (2009)
12. Larson, M., Hu, C., Li, R., Li, W., Cheng, X.: Secure auctions without an auctioneer via verifiable secret sharing. In: Workshop on Privacy-Aware Mobile Computing (PAMCO) 2015 In conjunction with ACM MobiHoc 2015. ACM, pp. 1–6 (2015)
13. Larson, M., Li, W., Hu, C., Li, R., Cheng, X.: A secure multi-unit sealed first-price auction mechanism. In: The 10th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2015), vol. 9204, pp. 295–304. Springer, Heidelberg (2015)
14. Li, W., Cheng, X., Bie, R., Zhao, F.: An extensible and flexible truthful auction framework for heterogeneous spectrum markets. In: ACM MobiHoc, pp. 175–184. Philadelphia, USA, August 2014
15. Li, W., Wang, S., Cheng, X., Bie, R.: Truthful multi-attribute auction with discriminatory pricing in cognitive radio networks. ACM SIGMOBILE Mob. Comput. Commun. Rev. **18**(1), 3–13 (2014)
16. Nojoumian, M., Stinson, D.R.: Efficient sealed-bid auction protocols using verifiable secret sharing. In: Huang, X., Zhou, J. (eds.) ISPEC 2014. LNCS, vol. 8434, pp. 302–317. Springer, Heidelberg (2014)
17. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)
18. Pan, M., Sun, J., Fang, Y.: Purging the back-room dealing: secure spectrum auction leveraging paillier cryptosystem. IEEE J. Sel. Areas Commun. **29**(4), 866–876 (2011)
19. Pan, M., Zhu, X., Fang, Y.: Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer. Wirel. Netw. **18**(2), 113–128 (2012)

20. Peng, K.: Efficient proof of bid validity with untrusted verifier in homomorphic e-auction. IET Inf. Secur. **7**(1), 11–21 (2013)
21. Peng, K., Boyd, C., Dawson, E.: A multiplicative homomorphic sealed-bid auction based on goldwasser-micali encryption. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 374–388. Springer, Heidelberg (2005)
22. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
23. Suzuki, K., Kobayashi, K., Morita, H.: Efficient sealed-bid auction using hash chain. In: Won, D. (ed.) ICISC 2000. LNCS, vol. 2015, pp. 183–191. Springer, Heidelberg (2001)
24. Suzuki, K., Yokoo, M.: Secure combinatorial auctions by dynamic programming with polynomial secret sharing. In: Blaze, M. (ed.) FC 2002. LNCS, vol. 2357, pp. 44–56. Springer, Heidelberg (2003)
25. Suzuki, K., Yokoo, M.: Secure generalized vickrey auction using homomorphic encryption. In: Wright, R.N. (ed.) FC 2003. LNCS, vol. 2742, pp. 239–249. Springer, Heidelberg (2003)