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 DC, 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 widely applied to real-world applications [2, 12, 13, 15, 17, 18, 23, 25], among which VCG is an important auction mechanism which receives lots of attraction. 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 [14]. Despite its good economic properties, VCG has security vulnerabilities, e.g. it is vulnerable to 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 [21, 26], 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 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 computation 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 section 2, we introduce related work. In section 4, we outline the most important preliminaries. In section 6, we present our scheme in detail. In section 8, 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 section 9.

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 [6, 24], homomorphic encryption, and hash functions.

Kobayashi, Morita and Suzuki use hash chains to form a sealed-bid auction [13,25]. 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 [8, 10], attribute-based encryption [5, 9, 10], image security [7] and so on. Later, Suzuki and Yokoo combine dynamic programming and secret sharing to build a secure auction scheme [26]. 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 [19], but this scheme also requires a secure channel and it can not resist collusion attacks between evaluators and the third parties. Larson et al. [15] 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 [11], 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 [23], Goldwasser-Micali encryption is used to design a new sealed-bid auction. In [2], a secure McAfee double auction scheme is proposed using homomorphic encryption for spectrum auctions. In [22], 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 [16]. There is also some research on leveraging homomorphic encryption to secure VCG, such as [20, 21, 26]. 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 Models and Design Goals

3.1 Auction Model

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:

$$b_i(S) = \{b_i(A_1), b_i(A_2), b_i(A_3), ..., b_i(A_{|S|})\}, \tag{1}$$

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 auction strategy. Take VCG auction for example:

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 [14]. Thus, by adopting VCG, we simply assume that each bidder submits its true valuation in the auction.

3.2 System Model

As shown in our system model consists of three entities: bidders, auctioneer and server. Let p_i be the public key of a bidder i and p_A be the public key of the auctioneer. The corresponding private keys are denoted by s_i and s_A, respectively. We

denote the encryption to ciphertext c of data d with public key p by $c = E_p(d)$, and decryption of ciphertext c with private key s by $d = D_s(c)$. The roles of the three entities are described as follows

- *Bidders:* The bidders made their bids and send them to the server for computation.
- *Auctioneer:* The auctioneer publishes the bidding strategy and final results.
- *Server:* The server is responsible for computing auction results for the auctioneer, and associate a bidder to verify the results.

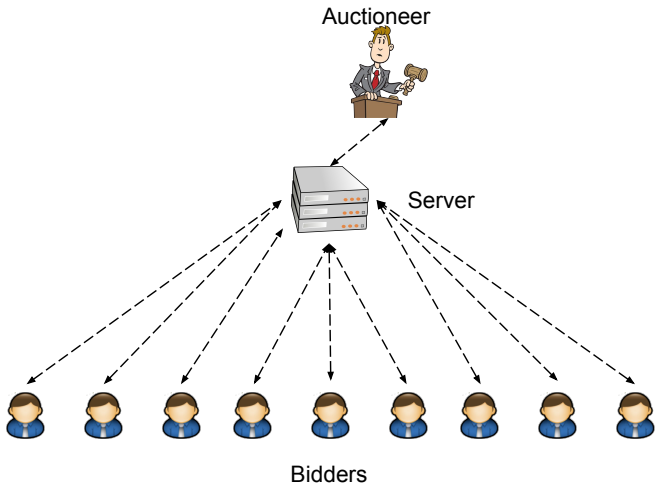

Fig. 1. A communication architecture

3.3 Security Model

We adopt a semi-honest mode, where the server is honest-but-curious. The server is used for storing data of an auction, re-encrypting data for data sharing, and computing results based on the auction strategy. The server is willing to know the information of the auction, but will not modify the data. The auctioneer could maliciously modify the results and publish fake results for more profits. However, our verification mechanism will enable a bidder or any agent to check the results without knowing the bidding information of each bidder.

4 Preliminaries

4.1 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. We adopt Elgamal cryptosystem [3] to perform an additive homomorphic encryption on the bids so that the server is able to compute the sum of the bids without seeing the individual share. More generally, given an encryption function E, $E(x_1 + x_2) = E(x_1) \cdot E(x_2)$.

4.2 Bilinear Map

Bilinear Map [4] establishes a relationship between two cryptographic groups. The notations of bilinear map are as follows: $\mathbb{G}$ and $\mathbb{G}_1$ are two multiplicative cyclic groups of finite order n and g is a generator of $\mathbb{G}$. e is a blinear map that $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$. Bilinear map has the following property that given $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}$, we have $e(g^a, h^b) = e(g, h)^{ab}$. Such maps can be achieved by Weil and Tate pairing that can be efficiently computed [**?**].

4.3 AFGH Re-encryption

Re-encryption is used to securely transfer a ciphertext from one secret key to another, without the need of decrypting a ciphertext. For example, a user Alice encrypts her message m with her public key P_a, and sends $E_{P_a}(m)$to the server; if Alice decides later to share the message with Bob, she could ask the server to re-encrypt the message to $E_{P_b}(m)$ so that Bob is able to decrypt the message. We give an introduction of AFGH re-encryption scheme [1], which has the following two good features:

(a) No presharing: the re-encryption key is generated by S_a and P_b, and private key of Bob is not required.
(b) Unidirectionality: the re-encryption key from Alice to Bob does not allow re-encryptions from Bob to Alice.

AFGH defines system parameters as $(g, e, Z, q, \mathbb{G}, \mathbb{G}_1)$ where $g \in \mathbb{G}$, $Z = e(g, g) \in \mathbb{G}_1$ and e as the map: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$. $\mathbb{G}$ and $\mathbb{G}_1$ are both cyclic groups of the same prime order q. Alice selects a random value $b \in \mathbb{Z}_q^*$ as private key S_a and computes public key $P_a = g^a$. Similarly, Bob selects a random value $b \in \mathbb{Z}_q^*$ as private key S_b and computes public key $P_a = g^b$. Alice also computes a token for re-encryption based on her private key and Bob's public key: $R_{A \rightarrow B} = (g^b)^{1/a} = g^{b/a}$. The process of AFGH is described as follows:

(a) Encryption for Alice:

$$C_a = (Z^r \cdot m, g^{ra}) \tag{3}$$

(b) Decryption for Alice:

$$m = \frac{Z^r \cdot m}{e(g^{ra}, g^{1/a})} \tag{4}$$

(c) Re-encryption:

$$C_b = (Z^r \cdot m, e(g^{ra}, R_{A \rightarrow B})) = (Z^r \cdot m, e(g^{ra}, g^{b/a})) = (Z^r \cdot m, Z^{rb}) \tag{5}$$

(d) Decryption for Bob:

$$m = \frac{Z^r \cdot m}{(Z^{rb})^{1/b}} \tag{6}$$

4.4 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:

$$b_i(S) = \{b_i(A_1), b_i(A_2), b_i(A_3), ..., b_i(A_{|S|})\}, \tag{7}$$

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

5 Main Idea

6 Proposed Scheme

6.1 Requirements

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

1. *Correctness :* The computation result must be correct, and strictly follows the policy of VCG scheme. This should be verifiable.
2. *Confidentiality :* Users' bid value 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.

6.2 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,

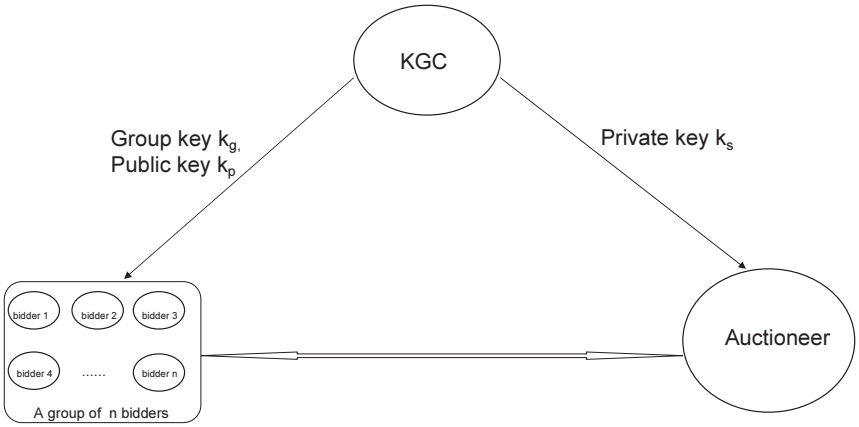

Fig. 2. System Model

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 price. 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.

6.3 Secure VCG auction based on Homomorphic Encryption(SVHE)

System Model The system model is described in Fig.2: 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, a pair of asymmetric keys for the 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.

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 keyK_g.

$$\begin{aligned} E_{k_g}(E_{k_p}(b_i(S))) =& E_{k_g}((E_{k_p}(b_i(A_1)), E_{k_p}(b_i(A_2)), E_{k_p}(b_i(A_3)), ..., \\ & E_{k_g}(b_i(A_{|S|})), 1 \leq i \leq n \end{aligned} \tag{8}$$

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

$$\begin{aligned} E_{k_p}(b_i(S)) =& \{(E_{k_p}(b_i(A_1)), E_{k_p}(b_i(A_2)), E_{k_p}(b_i(A_3)), ..., \\ & E_{k_p}(b_i(A_{|S|})\}, 1 \leq i \leq n \end{aligned} \tag{9}$$

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 obtain:

$$\begin{aligned} D_{k_s}(\prod_{i=1}^{n} E_{k_p}(b_i(S))) &= D_{k_s}(\prod_{i=1}^{n} E_{k_p}(b_i(A_1)), \prod_{i=1}^{n} E_{k_p}(b_i(A_2)), \prod_{i=1}^{n} E_{k_p}(b_i(A_3)), ..., \\ & \prod_{i=1}^{n} E_{k_p}(b_i(A_{|S|})) \\ &= (\sum_{i=1}^{n} b_i(A_1), \sum_{i=1}^{n} b_i(A_2), \sum_{i=1}^{n} b_i(A_3), ..., \sum_{i=1}^{n} b_i(A_{|S|}) \end{aligned} \tag{10}$$

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

$$S^* = argmax\{\sum_{i=1}^{n} b_i(A_1), \sum_{i=1}^{n} b_i(A_2), \sum_{i=1}^{n} b_i(A_3), ..., \sum_{i=1}^{n} b_i(A_{|S|})\} \tag{11}$$

In this step, the auctioneer only needs to decrypt a few groups of messages from the 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 result, it is reasonable to believe that the correct result is obtained. 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 so that the bidders see the result.

4. Once the bidders obtain S^*, they will be able continue computation for the VCG scheme. Here, we use Δp_i to denote a set of possible prices that the bidder should pay.

$$\begin{aligned} E_{k_p}(\Delta p_i) &= \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(S))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))} \\ &= (\frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_1))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_2))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_3))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, ..., \\ &\quad \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_{|S|}))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}) \end{aligned} \tag{12}$$

Then computation results from all the bidders will be sent to the auctioneer again for decryption.

5. The auctioneer decrypts the message, and obtains:

$$\begin{aligned} \Delta p_i &= D_{k_s}(\frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_1))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_2))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_3))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}, ..., \\ &\quad \frac{\prod\limits_{j\neq i} E_{k_p}(b_j(A_{|S|}))}{\prod\limits_{j\neq i} E_{k_p}(b_j(S^*))}) \\ &= \sum_{j\neq i} b_j(S) - \sum_{j\neq i} b_j(S^*) \end{aligned} \tag{13}$$

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

$$\begin{aligned} p_i = max\{\Delta p_i\} &= max\{\sum_{j\neq i} b_j(S) - \sum_{j\neq i} b_j(S^*)\} \\ &= max \sum_{j\neq i} b_j(S) - \sum_{j\neq i} b_j(S^*), \end{aligned} \tag{14}$$

7. The auctioneer broadcasts the results. The winners pay the right amount of money to the auctioneer and win the corresponding goods.

Discussion The computation complexity in SVHE is high because of the high computation cost of homomorphic encryption. Furthermore, this scheme has one drawback: if some of the bidders are not honest, and they sell the other bidders' bids to the auctioneer in sacrifice of their own privilege in the auction, then the auctioneer is able to know all the bidder's bid price. Thus We explore to find out a scheme, which has very low cost, and is vulnerable to the collusion problem between the auctioneer and the bidders. We now propose our second scheme: Secure VCG Auction based on Masking Values(SVM).

7 Secure VCG Auction based on Masking Values(SVMV)

7.1 System Model

In SVHE, we do not need a KGC to assign the group key, so we let the bidders and the auctioneer generate their own public key pair and broadcast the public key to the public. Besides, we need to employ some proxy servers acting as mix net nodes to help transfer the nose. Therefore, the system consists of the auctioneer, bidders and the mix net nodes.

7.2 Basic Idea

We consider to use masking values instead of homomorphic encryption to hide the bid prices. The bidder i will firstly choose a random noise to hide his bid price, and then send the noise δ_i to the auctioneer through mix net. Then the bidders encrypts their bid prices using the noise they choose and send them to the auctioneer. The auctioneer is able to aggregate the data and find out the solution for VCG auction based on the encrypted data and the noises. The hard problem is how could the auctioneer use the information he has to solve this problem. We will illustrate it in detail in the protocol.

7.3 System Initialization

The auctioneer generate their private and public keys based on RSA public-key cryptosystem, and announce his public keys. Formally, we use k_s and k_p to denote the auctioneer's private and public keys.

At this stage, each bidder i uniformly and randomly picks up a noise value, δ_i, from the range of $[\underline{\delta}_i, \bar{\delta}_i]$, where $\underline{\delta}_i$ is the lower-bound and $\bar{\delta}_i$ is the upper-bound of the noise range. Then, each bidder i sends its encrypted noise value to the mix net by using the auctioneer's public key k_p. That is, $k_p(\delta_i)$ is sent from bidder i to the server. Note that for each allocation A, the bidders need to create a group of noise, because the repetitive use of a noise by one bidder will expose the noise information to the auctioneer or an adversary. Formally the noise group is denoted as: $\delta_i = (\delta_i(A_1), \delta_i(A_2), \ldots, \delta_i(A_{|S|}))$, in which $\delta_i(A_j)$ is the noise value for assignment A_j and is selected uniformly and randomly from $[\underline{\delta}_i, \bar{\delta}_i]$ for $1 \leq j \leq |S|$.

7.4 Bidding Process

1. To hide the bid price, each bidder computes a masked bid $b'_i = b_i + \delta_i$ for each allocation, and sends the them to the auctioneer. The data sent can be concatenated with a salt to avoid miscellaneous attack from an adversary. To make it simple, we do not write the salt in our expression. Therefore, data sent from the bidders to the auctioneer is denoted as: $(b_i(A_1) + \delta_i(A_1), b_i(A_2) + \delta_i(A_s), b_i(A_3) + \delta_i(A_3), \ldots, b_i(A_{|S|}) + \delta_i(A_{|S|})$.
2. The auctioneer computes the sum of the bid prices plus noise for each allocation: $\{\sum_{i=1}^{n} b_i(A_1) + \delta_i(A_1), \sum_{i=2}^{n} b_i(A_2) + \delta_i(A_2), \sum_{i=3}^{n}(b_i(A_3) + \delta_i(A_3), ..., \sum_{i=1}^{n} b_i(A_{|S|}) + \delta_i(A_{|S|}\}$
3. The auctioneer cancels the sum of noise for each allocation and find out the allocation which leads to the maximum sum of bid prices:

$$S^* = argmax\{\sum_{i=1}^{n} b_i(A_1), \sum_{i=1}^{n} b_i(A_2), \sum_{i=1}^{n} b_i(A_3), ..., \sum_{i=1}^{n} b_i(A_{|S|)}\} \tag{15}$$

4. The auctioneer calculates the price that each bidder should pay:

$$p_i = \max \sum_{j \neq i} b_j(S) - \sum_{j \neq i} b_j(S^*) = [\max \sum_{j \neq i} (b_j(A) + \delta(A))] \tag{16}$$

8 Discussion

8.1 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.

8.2 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 can be obtained by the auctioneer.

8.3 First-Price Auction

Under the same auction model, 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 can be protected. Therefore, non-repudiation can be achieved because none of the bidders in the system is able to deny his behavior.

8.4 Limitation

One limitation of our scheme is that it introduces more computations compared to [26], 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.

9 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 US National Science Foundation grants: CNS-1407986, CNS-1318872, CNS-1442642, and CNS-1443858.

References

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, 9(1):1–30, 2006.

[2] Zhili Chen, Liusheng Huang, Lu Li, Wei Yang, Haibo Miao, Miaomiao Tian, and Fei Wang. Ps-trust: Provably secure solution for truthful double spectrum auctions. In *INFOCOM, 2014 Proceedings IEEE*, pages 1249–1257. IEEE, 2014.

[3] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology*, pages 10–18. Springer, 1985.

[4] Eu-Jin Goh. *Encryption schemes from bilinear maps*. Stanford University, 2007.

[5] Chunqiang Hu, Xiuzhen Cheng, Zhi Tian, Jiguo Yu, Kemal Akkaya, and Limin Sun. An attribute-based signcryption scheme to secure attribute-defined multicast communications.

[6] Chunqiang Hu, Xiaofeng Liao, and Xiuzhen Cheng. Verifiable multi-secret sharing based on LFSR sequences. *Theoretical Computer Science*, 445:52–62, 2012.

[7] Chunqiang Hu, Xiaofeng Liao, and Di Xiao. Secret image sharing based on chaotic map and chinese remainder theorem. *International Journal of Wavelets, Multiresolution and Information Processing*, 10(03):1250023(1–18), May 2012.

[8] Chunqiang Hu, Fan Zhang, Xiuzhen Cheng, Xiaofeng Liao, and Dechang Chen. 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*, pages 31–36. ACM, 2013.

[9] Chunqiang Hu, Fan Zhang, Tao Xiang, Hongjuan Li, Xiao Xiao, and Guilin Huang. A practically optimized implementation of attribute based cryptosystems. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 197–204. IEEE, 2014.

[10] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng, and Xiaofeng Liao. Body area network security: A fuzzy attribute-based signcryption scheme. *Selected Areas in Communications, IEEE Journal on*, 31(9):37–46, 2013.

[11] Qianyi Huang, Yixin Tao, and Fan Wu. Spring: A strategy-proof and privacy preserving spectrum auction mechanism. In *INFOCOM, 2013 Proceedings IEEE*, pages 827–835. IEEE, 2013.

[12] Tao Jing, Chenyu Zhao, Xiaoshuang Xing, Yan Huo, Wei Li, and Xiuzhen Cheng. A multi-unit truthful double auction framework for secondary market. In *IEEE ICC*, 2013.

[13] Kunio Kobayashi, Hikaru Morita, Koutarou Suzuki, and Mitsuari Hakuta. Efficient sealed-bid auction by using one-way functions. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 84(1):289–294, 2001.

[14] Vijay Krishna. *Auction theory*. Academic press, 2009.

[15] Maya Larson, Chunqiang Hu, Ruinian Li, Wei Li, and Xiuzhen Cheng. 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, 2015.

[16] Maya Larson, Wei Li, Chunqiang Hu, Ruinian Li, and Xiuzhen Cheng. A secure multi-unit sealed first-price auction mechanism. In *The 10th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2015)*. Springer, August 2015.

[17] Wei Li, Xiuzhen Cheng, Rongfang Bie, and Feng Zhao. An extensible and flexible truthful auction framework for heterogeneous spectrum markets. In *ACM MobiHoc*, pages 175–184, Philadelphia, USA, August 2014.

[18] Wei Li, Shengling Wang, Xiuzhen Cheng, and Rongfeng Bie. Truthful multi-attribute auction with discriminatory pricing in cognitive radio networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 18(1):3–13, January 2014.

[19] Mehrdad Nojoumian and Douglas R Stinson. Efficient sealed-bid auction protocols using verifiable secret sharing. In *Information Security Practice and Experience*, pages 302–317. Springer, 2014.

[20] Miao Pan, Jinyuan Sun, and Yuguang Fang. Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem. *Selected Areas in Communications, IEEE Journal on*, 29(4):866–876, 2011.

[21] Miao Pan, Xiaoyan Zhu, and Yuguang Fang. Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer. *Wireless Networks*, 18(2):113–128, 2012.

[22] Kun Peng. Efficient proof of bid validity with untrusted verifier in homomorphic e-auction. *IET Information Security*, 7(1):11–21, 2013.

[23] Kun Peng, Colin Boyd, and Ed Dawson. A multiplicative homomorphic sealed-bid auction based on goldwasser-micali encryption. In *Information Security*, pages 374–388. Springer, 2005.

[24] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[25] Koutarou Suzuki, Kunio Kobayashi, and Hikaru Morita. Efficient sealed-bid auction using hash chain. In *Information Security and Cryptology—ICISC 2000*, pages 183–191. Springer, 2001.

[26] Koutarou Suzuki and Makoto Yokoo. Secure generalized vickrey auction using homomorphic encryption. In *Financial Cryptography*, pages 239–249. Springer, 2003.