# A Verifiable Combinatorial Auction with Bidder's Privacy Protection

Mingwu Zhang[1,2,3(✉)] and Bingruolan Zhou[1]

[1] School of Computer Science, Hubei University of Technology, Wuhan 430000, China
csmwzhang@gmail.com, brlzhou@163.com
[2] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China
[3] School of Computer Science and Information Security,
Gulin University of Electronic Technology, Guilin, China

**Abstract.** Combinatorial auctions are employed in many fields such as spectrum auction and energy auction. However, data concerning bidders' bid and bundle might reveal sensitive information, such as personal preference and competitive relation. In order to solve this problem, this paper proposes a privacy-preserving and verifiable combinatorial auction scheme to protect bidders' privacy and ensure the correctness of the result. In our scheme, we employ a one-way and monotonically increasing function to protect each bidder's bid, so that the auctioneer is able to pick out the largest bid without disclosing any information about bids. Moreover, we convert the question of judging whether a bidder is a winner to the question of judging whether the vector product is 0. In our scheme, crypto service provider (CSP) is responsible for key distribution and blind signature to verify the authenticity and correctness of the result. Besides, we put forward a privacy-preserving and verifiable payment determination model to compute the payment the winner should pay.

**Keywords:** Privacy-preserving · Combinatorial auction

## 1 Introduction

With the rapid development and wide application of Internet, the number of online e-commerce activities is increasing. The auction is gradually changing from traditional auction to electronic auction and becoming an important part of e-commerce. For example, spectrum [2] and energy [4] can be auctioned on the Internet. The electronic auction system generally consists of auctioneer, sellers and bidders. The seller entrusts the auctioneer to arrange the auction, accept the bids, and declare the winner [1]. In a single auctioneer combinatorial auction, the auctioneer sells multiple heterogeneous goods simultaneously, and bidders bid on any combination of the goods (called bundle or set) instead of just one [5]. Such


D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 397–405, 2021.
https://doi.org/10.1007/978-3-030-66922-5_27

auctions have been researched extensively recently, in part due to the generality of it, and in part due to growing application scenarios where combinatorial auction is necessary [14].

In privacy-preserving combinatorial auction protocols, bidders protect their private information using cryptographic technique. After the execution of the auction, only the auction outcomes, i.e., who are winners and the corresponding payments, are revealed. The losers' bids and bundles are kept private in the auction because the auctioneers may use losers' bids to maximize their revenues in future auctions [1]. For example, the average of losers' bids can motivate auctioneers to increase the starting price in future auction of similar goods. In addition, private information of bidders, such as bundle and bids, can be used to disclose personal preference and how much bidders want to pay. In auctions where there is serious competition between bidders, these information are vital and need to be protected.

In private-preserving combinatorial auction, an important problem to be solved is how to determine the winner, i.e., how to pick out a set of disjoint goods, the value of which is the maximized. [12] use dynamic programming approach to solve the problem of winner determination in privacy-preserving combinatorial auction because dynamic programming can well solve the problem of finding the shortest path of directed graph.

Shamir's threshold secret sharing scheme can also be used to solve the privacy-preserving problem in combinatorial auctions. For example, [6] employs secret sharing scheme to share bids between the evaluators, which could resist the passive adversary model. All evaluators come together to find out the optimal solution through secure dynamic programming. Considering the communication cost of the protocols, [3] proposed an authentic property without increasing the communications cost in combinatorial auctions. Homomorphic encryption provides an available approach to protect each bidder's bidding values with a vector of cipher texts, and ensure the auctioneer to figure out the maximum value securely [7–9,11,13].

Various approaches are proposed to achieve the privacy-preserving combinatorial auction, such as dynamic programming, Shamir's threshold secret sharing scheme, homomorphic encryption and secure multi-party computation, etc.

[12] employed dynamic programming to solve the problem in the combinatorial auction. However, with the increase of the number of bidders and goods, dynamic programming will lead to non-polynomial time computation time. [6] implemented the privacy-preserving combinatorial auction through Shamir's threshold secret sharing scheme, and through further improvements, [3] reduced the communications cost in designing the secure auction protocol. [7–9,11,13] gave combinatorial auction protocols that are based on homomorphic encryption technique in ciphertext fields, however, these protocols need a high computational cost. [10] employed the technique of secure multi-party computation to implement privacy-preserving combinatorial auction, where the protocols are not scalable since the inputs of combinatorial auction can not be pre-determinated.

## 2 Privacy Preserving Combinatorial Auction Model

### 2.1 System Model

As shown in Fig. 1, auctioneer has a series of goods $G = \{g_1, ..., g_m\}$, which will be auctioned to $N$ bidders $B = \{B_1, ..., B_n\}$. Each bidder $B_i$ gives his own bundle $S_i \in G$ that he expects to obtain and his bid $b_i(S_i)$, i.e. the price $B_i$ is willing to pay on his bundle $S_i$. Crypto service provider is responsible for key distribution and collaborative computation. Besides, CSP will generate blind signature for bidders' bid and bundle, which will be used to verify the correctness of the result later.

The winners are chosen by the auctioneer as follows:

$$W = \text{argmax} \sum_{B_i} b_i(S_i) \quad s.t. \quad \cap_{B_i} S_i = \emptyset \tag{1}$$

i.e., a set of conflict-free bidders whose total bid is maximized, and $A = \cup_{B_i \in W} S_i$ is the set of winners' bundle. After that, the auctioneer will determine the price that the winner should pay according to some mechanism.

We assume that each bidder has only one sequence of goods expected to buy. That is, if at least one good in the bundle that a bidder expects to get has been auctioned, the bidder will not get the remaining goods. This assumption is equivalent to the restriction that each bidder is limited to one bid only. We simplify bid $b_i(S_i)$ as $b_i$ and denote the auctioneer as E.

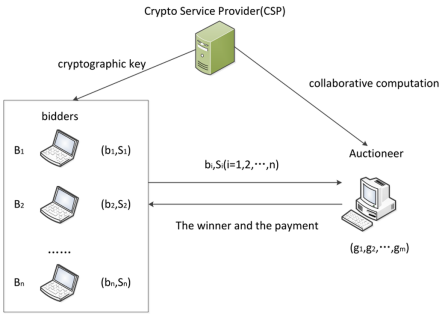


**Fig. 1.** System model

### 2.2 Adversary Model

When the allocation terminates, the auctioneer is supposed to only know the winners, their bundles and their bids. Each bidder only knows whether he is a winner. The bidder will also be informed the price he should pay, if he is the winner. Each bidder does not know anything about others' bundle or bid. CSP

is responsible for key distribution and signature generation. In addition, CSP will help auctioneer to decrypt but will know nothing about auction results.

The auctioneer is assumed to be curious, malicious and ignorant. He is interested in bidders' bundles and bids to improve his business (i.e., "*curious*"). For example, the auctioneer may try to infer bidders' preferences and competitive relationship based on the bundles and bids. The auctioneer may also report a fake price to the winners (i.e., "*malicious*"), but he is not aware of bidders' side information such as distribution of bid or bidders' preference on goods (i.e., "*ignorant*").

Bidders are assumed to be curious, and non-cooperative. They are interested in others' bundles and bids to help them make decision (i.e., "*curious*"). However, they will not collude with each other or the auctioneer (i.e., "*non-cooperative*").

CSP is assumed to be honest, curious and non-cooperative. CSP follows the protocol steps honestly but try to learn bidders' bundles and bids (i.e., "*curious*"). But CSP will not collude with the auctioneer (i.e., "*non-cooperative*").

## 3 Our Proposed Scheme

Before auction, all bidders blind sign their bundle $S_i$ and average value $\varphi_i$ through the crypto service provider (CSP). Since we use the blind signature scheme, CSP will not get any relevant information. These signatures will be used for verification later.

### 3.1 Privacy-Preserving Winner Determination Model

**Algorithm 1.** Greedy Winner Determination

1: Mark the set of auctioned goods as $A$, the set of winners as $W$. During the initial phase, $A = \emptyset, W = \emptyset$. Each $B_i (i = 1, \cdots, n)$ computes average value $\varphi_i = \frac{b_i}{|S_i|}$.
2: Sort $B_i$ in a non-increasing good according to the value of the $\varphi_i$, that is, the bigger the $\varphi_i$, the former the $B_i$. The sorted sequence is called $L$.
3: Check the $B_i$ in $L$ from front to back to see whether $A \cap S_i = \emptyset$. If true, update sets $A$ and $W$, $A = A \cup S_i$, $W = W \cup B_i$.
4: After auction, $W$ is the set of winners, and $A$ is the set of goods that have been auctioned.

Algorithm 1 proposes a greedy winner determination model. Because the comparison and sorting will reveal the private information $S_i$ and $b_i$ of the bidders, we cannot directly compare $\varphi_i$ and sort $B_i$ on the plaintext (step 2) or directly select the winner (step 3). We use the monotonically increasing and one-way function to protect the bidder's $b_i$, which enables the auctioneer to pick out the largest $b_i$ without knowing anything about $b_i$. Besides, the auctioneer needs to check whether $B_i$'s bundle $S_i$ contains the good that has already been auctioned. We use m-dimensional binary vector $\boldsymbol{A}$ to represent the auction status of m goods, where the $k$-th bit $a_k = 1$ if the $k$-th good $g_k$ has already been

auctioned and $a_k = 0$ if the k-th good $g_k$ has not been auctioned. Similarly, we use another $m$-dimensional binary vector $\boldsymbol{S_i}$ to represent $B_i$'s bundle $S_i$, where $k$-th bit $s_{i,k} = 1$ if the $k$-th good $g_k \in S_i$ and $s_{i,k} = 0$ if the $k$-th good $g_k \notin S_i$.

If $B_i$'s bundle $S_i$ does not contain the good that has already been auctioned, then

$$\boldsymbol{A_i} \cdot \boldsymbol{S_i} = 0 \Leftrightarrow \Sigma_{k=1}^{m} a_k \cdot s_{i,k} = 0$$

If vector product is $\theta$, that means $B_i$'s bundle $S_i$ includes $\theta$ already-auctioned goods.

Thus, we can propose a privacy-preserving winner determination model (Algorithm 2), which can be regarded as a black-box algorithm and only outputs the winner and the corresponding bundle.

**Algorithm 2.** Privacy-preserving Winner Determination

1: Mark the set of auctioned goods as $A$, the set of winners as $W$. During the initial phase, $A = \emptyset, W = \emptyset$. Each $B_i (i = 1, \ldots, n)$ computes average value $\varphi_i = \frac{b_i}{|S_i|}$.

2: CSP picks a pair of Elgamal algorithm key: $mpk = (h_1 = g^{s_1}, h_2 = g^{s_2}, \cdots, h_m = g^{s_m})$, $msk = \boldsymbol{S} = (s_1, s_2, \cdots, s_m)$, and publishes $mpk$.

3: Each $B_i$ picks a random number $r_i$ and encrypts $\boldsymbol{S_i} = (s_{i,1}, s_{i,2}, \cdots, s_{i,m})$

$$c_{i,1} = h_1^{r_i} \cdot g^{s_{i,1}}, c_{i,2} = h_2^{r_i} \cdot g^{s_{i,2}}, \cdots, c_{i,m} = h_m^{r_i} \cdot g^{s_{i,m}}, c_{i,m+1} = g^{r_i}$$

4: Each $B_i$ sends a request to CSP.

5: CSP selects a large number $U$, calculates $\Delta = l \cdot U^2$ and selects $a_1, a_2, \cdots, a_n$ that satisfy $a_i > \Delta^i$ for $i = 1, 2, \cdots, n$. And then, CSP randomly choose noise $e$ from $(\Delta, a_1 + a_2 + \cdots + a_n)$. Finally, CSP sends $a_1, a_2, \cdots, a_n$, $e$ and $\Delta$ to $B_i$

6: After receiving $a_1, a_2, \cdots, a_n$, $e$ and $\Delta$, $B_i$ computes $f(\varphi_i) = a_1(\varphi_i (\text{mod } \Delta)) + a_2(\varphi_i (\text{mod } \Delta))^2 + \cdots + a_n(\varphi_i (\text{mod } \Delta))^n + e$ and sends $f(\varphi_i)$ to E.

7: E picks out the $B_i$ with the largest average value $\varphi_i$, and checks whether the bundle of $B_i$ contains the good that has already been auctioned through the step 8 - step 12.

8: E sends $\boldsymbol{A} = (a_1, a_2, \cdots, a_m)$ to CSP.

9: CSP computes $sk_y = \boldsymbol{S} \cdot \boldsymbol{A} = (s_1 a_1 + s_2 a_2 + \cdots + s_m a_m)$ and sends $sk_y$ to E.

10: E picks the largest $f(\varphi_i)$ and asks the corresponding $B_i$ to send $c_{i,1}, c_{i,2}, \cdots, c_{i,m}, c_{i,m+1}$ to the auctioneer E.

11: Upon receiving the ciphertext $c_{i,1}, c_{i,2}, \cdots, c_{i,m}, c_{i,m+1}$, the auctioneer E computes $\Pi_{j=1}^{m} \frac{c_{i,j}^{a_j}}{c_{i,m+1}^{sk_y}} = g^{\langle \boldsymbol{S_i}, \boldsymbol{A} \rangle}$ and check whether it is equal to 1.

12: If the result is 1 after decryption, $B_i$ is the winner. E puts the $B_i$ into the winner set W and marks its corresponding bundle as auctioned in set A. Otherwise, $B_i$ is not the winner. E will remove $B_i$ from bidders. Then repeat step 8 - step 12 until no set can be updated.

In Algorithm 2, each $B_i$ calculates $f(\varphi_i)$ and sends $f(\varphi_i)$ to the auctioneer E. Because $f(\varphi_i)$ is a one-way increasing function, the auctioneer E picks the largest $f(\varphi_i)$ by comparing the value of $f(\varphi_i)$, which is equivalent to picking the largest $\varphi_i$. Besides, E verifies whether the bidder's bundle contains the good that has already been auctioned through judging whether $g^{\boldsymbol{S_i} \cdot \boldsymbol{A}}$ is equal to 1. If $g^{\boldsymbol{S_i} \cdot \boldsymbol{A}} = 1$, that means compared with other bidders, the average value of $B_i$ is the largest, and the corresponding bundle is also available, which means $B_i$

is the winner of this round. The auctioneer will update $A$ and $W$ to continue the search for the next winner. If $g^{\boldsymbol{S_i \cdot A}} \neq 0$, the final output is indistinguishable from a random number in $\mathbb{Z}_n$ from the auctioneer's perspective, which means the bundle of $B_i$ contains at least one good that has been auctioned. E will remove $B_i$ from bidders and re-select the bidder with the largest average value.

After the winner is selected, $E$ will inform the winner to send the average value $\varphi_i$, bundle $S_i$, $Sig(\varphi_i)$, $Sig(S_i)$ to $E$, and the signatures $Sig(\varphi_i)$ and $Sig(S_i)$ can guarantee the integrity of $\varphi_i$ and $S_i$.

### 3.2 Privacy-Preserving Verifiable Payment Determination Model

We propose privacy-preserving verifiable payment determination model (Algorithm 3) as follow. Because $E$ cannot know any information about $B_j$' bundle $S_j$ from Algorithm 2, so $E$ cannot know any information about $b_j$ from $\frac{b_j}{|S_j|}$. Similarly, the winner $B_i$ can't get any information about $B_j$'s bundle $S_j$ and $b_j$, and $B_i$ even does not who is $B_j$. $B_j$ does not get any information in this process. Since $E$ and $B_i$ have the signature $Sig(\varphi_j)$ generated by CSP, $E$ can believe that $B_j$ gives him the correct $\varphi_j$, and $B_i$ can verify that $E$ does not send the wrong $p_i$.

**Algorithm 3.** Privacy-preserving and Verifiable Payment Determination

1: $E$ removes the winner $B_i$ from bidders, and modifies $A$ to $(A - S_i)$, where $A$ is the set of auctioned goods and $S_i$ is the bundle of $B_i$. Then thorough Algorithm 3, $E$ chooses a new winner $B_j$, who is the candidate of $B_i$. $E$ notifies $B_j$ to send average value $\varphi_j = \frac{b_j}{|S_j|}$ and $Sig(\varphi_j)$ to $E$.

2: If the candidate of $B_i$ can be successfully found, $E$ computes $p_i = \frac{b_j}{|S_j|}|S_i|$ and sends $p_i$ and $Sig(\varphi_j)$ to $B_i$. If no candidate is found, $E$ sets $p_i$ as the agreed default value and notifies $B_j$ that $p_i$ is the default value.

3: If $p_i$ is not the default value, $B_i$ can recover $\varphi_j$ from $\frac{p_i}{|S_i|}$ and verify whether $\varphi_j$ is correct through $Sig(\varphi_j)$. If they are not equal to each other, $B_i$ knows that the payment is not correct.

## 4 Security Analysis

**Theorem 1.** *An adversarial auctioneer E's advantage $abv_{S_i}$ is negligible.*

`Proof`. Every winner's bundle $S_i$ is given to $E$, therefore we have:

$$adv_{S_i} = Pr[S_i|\mathcal{S}, Output \leftarrow \mathcal{A}_{our}(1^k)] - [S_i|Output \leftarrow \mathcal{A}_{black}] = 1 - 1 = 0$$

if $B_i$ is a winner. Further, because the ElGamal encryption algorithm is semantically secure, during the privacy-preserving Winner Determination (Algorithm 2),

all that an adversarial $E$ learns is whether there exists a feasible bundle. This reveals nothing about losers' $S_j$, therefore any adversary's view on losers' bundle in our model is the same as the one in an ideal black-box algorithm. Therefore,

$$adv_{S_j} = Pr[S_j|\mathcal{S}, Output \leftarrow \mathcal{A}_{our}(1^k)] - [S_j|Output \leftarrow \mathcal{A}_{black}] < negl(\kappa)$$

if $B_j$ is a loser, where $negl(\cdot)$ is a negligible function.

**Theorem 2.** *An adversarial auctioneer E's advantage $adv_{b_j}$ is negligible for all loser.*

`Proof`. In the payment determination model of the winner $B_i$, the candidate $B_j$'s average value $\varphi_j$ is disclosed to $E$. Because of the privacy-preserving Winner Determination (Algorithm 2), $E$ knows nothing about $S_j$, and he does not learn $b_j$ from $\varphi_j = \frac{b_j}{|S_j|}$. Therefore,

$$adv_{b_j} = Pr[b_j|\mathcal{S}, Output \leftarrow \mathcal{A}_{our}(1^k)] - [b_j|Output \leftarrow \mathcal{A}_{black}] < negl(\kappa)$$

## 5 Performance Analysis

In our combinatorial auction scheme, each bidder needs to transfer $(m + 1)$ ciphertext, so N bidders need to transfer a total of $N \cdot (m + 1)$ ciphertext, and the auctioneer needs to return the result. The security parameter used in our scheme is $\tau$, and the length of the ciphertext of Elgamal is $2\tau$. Because the length of the result is relatively small compared to $\tau$, so it can be ignored. Therefore, in our combinatorial auction scheme, the communication overhead is $N \cdot (m + 1) \cdot (2\tau) = 2N(m + 1)\tau$.

To evaluate the computation overhead, we conducted a simulation experiment. The experimental environment was Windows 8 64-bit operating system, memory 4G, Intel(R) Core(TM) i5-4210U CPU @ 1.70 GHz. In order to exclude the communication I/O during the simulation, we generated all strings in the communication and conducted the computation in the local instance. Security parameter $\kappa$ is 128-bit and every operation is run 1000 *times* to get the average run time.

As can be seen from Fig. 2, the auctioneer's computation overhead increases linearly with the increase of the amount of total bidders. But Fig. 2 shows that in our protocol, the auctioneer's computation overhead grows with a small constant factors linearly. Figure 2 shows that the amount of total bidders do not have a big impact on bidder's computation overhead, because each bidder calculates the average values $\varphi_i$, $f(\varphi_i)$ and encrypts the bundle $\boldsymbol{S_i}$ locally.

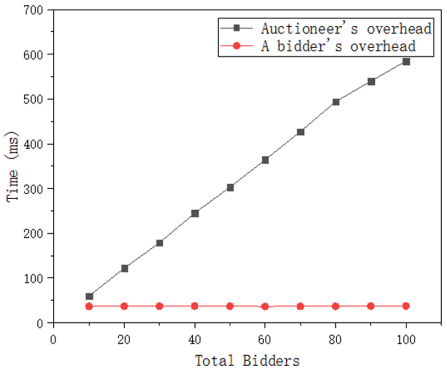


**Fig. 2.** Auctioneer's and bidder's overhead in winner determination.

## 6 Conclusion

In this paper, we proposed a privacy-preserving combinatorial auction scheme to protect bidder's privacy and ensure the security and verifiability of the result. We employed a one-way and monotonically increasing function to ensure the auctioneer to pick out the largest bid without discloseing the bid. We designed a privacy-preserving winner determination model to guarantee the correctness of the result. In our scheme, crypto service provider (CSP) is responsible for key distribution and blind signature. Besides, we put forward a privacy-preserving verifiable payment determination model to compute the payment the winner should pay. We extensively analyzed the security of our scheme to show that any adversary's view is the same as the one in a black-box algorithm. However, our work is not necessarily suitable for any context, we firmly believe we can continue to improve our work in the future.

**Acknowledgment.** This work is supported by the National Natural Science Foundation of China under grants 61672010 and 61702168, the Open Research Project of State Key Laboratory of Cryptology of China, and the Key projects of Guangxi Natural Science Foundation under grant 2019JJD170020.

## References

1. Alvarez, R., Nojoumian, M.: Comprehensive survey on privacy-preserving protocols for sealed-bid auctions. Comput. Secur. **88**, 101502 (2019)
2. Chen, Y., Ma, Z., Wang, Q., Huang, J., Zhang, Q.: Privacy-preserving spectrum auction design: challenges, solutions and research directions. IEEE Wirel. Commun. **PP**(99), 1–9 (2019)
3. Hu, C., Li, R., Mei, B., Li, W., Alrawais, A., Bie, R.: Privacy-preserving combinatorial auction without an auctioneer. Eurasip J. Wirel. Commun. Netw. **2018**(1), 38 (2018). https://doi.org/10.1186/s13638-018-1047-z

4. Lin, J., Pipattanasomporn, M., Rahman, S.: Comparative analysis of auction mechanisms and bidding strategies for P2P solar transactive energy markets. Appl. Energy **255**, 113687 (2019)
5. Jung, T., Li, X.Y.: Enabling privacy-preserving auctions in big data (2013)
6. Kikuchi, H.: $(M + 1)$st-price auction protocol. In: Syverson, P. (ed.) FC 2001. LNCS, vol. 2339, pp. 351–363. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46088-8_27
7. Larson, M., Li, R., Hu, C., Li, W., Cheng, X., Bie, R.: A bidder-oriented privacy-preserving VCG auction scheme. In: Xu, K., Zhu, H. (eds.) WASA 2015. LNCS, vol. 9204, pp. 284–294. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21837-3_28
8. Larson, M., Li, W., Hu, C., Li, R., Cheng, X., Bie, R.: A secure multi-unit sealed first-price auction mechanism. In: Xu, K., Zhu, H. (eds.) WASA 2015. LNCS, vol. 9204, pp. 295–304. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21837-3_29
9. Miao, P., Zhu, X., Fang, Y.: Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer. Wirel. Netw. **18**(2), 113–128 (2012). https://doi.org/10.1007/s11276-011-0390-3
10. Palmer, B., Bubendorfer, K., Welch, I., Development and evaluation of a secure, privacy preserving combinatorial auction. In: Australasian Information Security Conference (2011)
11. 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)
12. Parkes, D.C., Rabin, M.O., Thorpe, C.: Cryptographic combinatorial clock-proxy auctions (2009)
13. Xing, K., Hu, C., Yu, J., Cheng, X., Zhang, F.: Mutual privacy preserving k-means clustering in social participatory sensing. IEEE Trans. Ind. Inform. **13**, 2066–2076 (2017)
14. Zaman, S., Grosu, D.: Combinatorial auction-based allocation of virtual machine instances in clouds. J. Parallel Distrib. Comput. **73**(4), 495–508 (2013)