EURASIP Journal on
Information Security

RESEARCH Open Access

Secure first-price sealed-bid auction scheme

Zhen Guo[1,2], Yu Fu[3*] and Chunjie Cao[2]

Abstract

In modern times, people have paid more attention to their private information. The data confidentiality is very important in many economic aspects. In this paper, we proposed a secure auction system, in which the bids will not be revealed, and no one can fake the winning identity and the winner cannot change the winning bid. The communication cost of our scheme is low; only two rounds communication are needed between the bidders and the auctioneer. And we show that our scheme achieves the desired security requirements.

Keywords: Auction system, Privacy protection, Comparable encryption

1 Introduction

With the rapid development of the Internet in recent years, e-commerce, online trading, and electronic auction are becoming more and more popular. Auction has a long history, from the early days of ancient Babylon, auction has gradually become an efficient form of allocation of resources, as time goes by, and traditional auction theory has quite mature.

Due to the prosperity of electronic commerce, traditional auction also transferred to the network platform, electronic auction is the online form of traditional auction, with more and more customers and a wide variety of auctioned things. Related economic theories have proved that auction can maximize the interests of the participants (both seller and bidder) under certain conditions.

Electronic auction is the online form of traditional auction. The seller can use online auction platform to show their products by using multimedia technology with the help of the traditional auction intermediaries and platform service providers.

Electronic auction is mainly in the following three forms: English auction, which is the most common form of trade, is identified with the property that prices are non-decreasing. Users compete for the highest price they are willing to pay. The transaction will be stopped when the transaction deadline has come. The goods will be sold to the highest bidder. The first-price sealed-bid auction, the bidders will seal the bids. After the auction, the auctioneer opens the tenders and publishes the highest bid. The goods will sell to the highest bidder. The second-price sealed-bid auction, the first-price bidder is the winning bidder who buys the goods with the second price.

Electronic auction should satisfy the following properties.

- The bidder anonymity; even after the publication of auction results, any person cannot inform of the identity of the failures and his/her bid.
- Non-repudiation; the winning bidder cannot deny that he/she has submitted the highest bid and can accurately obtain the winning identity.
- Verifiability; anyone can publicly verify the validity of the winner and can verify the winning bidder is the first-price bidder in all bidders.
- Non-deception; no one can pretend a registered bidder to join in the auction.
- Correctness; the auctioneer should give the correct auction results.

The computer and network technology in the application of the electronic auction is in order to make the information transfer more quickly and communication more comprehensively, to reduce economic welfare loss caused by the information asymmetry and poor communication. But in the current network environment, information

* Correspondence: fu.yu1981@163.com
[3]School of Management, Sichuan University of Science and Engineering, Zigong, Sichuan, People's Republic of China
Full list of author information is available at the end of the article

asymmetry phenomenon has not disappeared, but increased to some extent, also the deceptive behaviors occurred in the e-auction frequently. In the 2010 report of IFCC (Internet Fraud Complaint Center), e-auction fraud accounted for 10.3% of the Internet fraud, this situation hampered the development of the electronic auction.

On the other hand, buyers' price information is commercial secrets or personal privacy, especially in a large auction, such as spectrum auction, exploitation of mineral rights, and real estate property rights, the tender's information may be abused, and this hampered the effectiveness of the transaction and reduced the social and economic benefits. According to the result of the survey of SCET (Secure Computing, Economy and Trust) project, 78% of buyers want their information is confidential. From the above, we need to pay attention to the security and privacy of electronic auction system, promote the development of network auction system, and increase the social welfare.

The network is a virtual environment, and the bidders are anonymous on the Internet. Although anonymity can protect the privacy of individuals, it brings many security issues to the online auctions. How to design the fair auction scheme with privacy preserving is an important research in modern auction system.

1.1 Our contributions

In this paper, we focus on the confidentiality protection of the bids in auction system. We construct a novel first-price sealed-bid auction scheme; the main contributions are as follows.

- The bids are keeping secret in the process of auction. The auctioneer cannot get the value of each bid.
- No one can fake the winning identity, which ensures the fairness of auction.
- The winning bid cannot be faked, and the winner cannot change it.
- The communication of our scheme is low; only two rounds communication is needed.

1.2 Related work

The private comparison is often discussed in our daily life. A common problem of ciphertext comparison is millionaires' problem. Yao [15] solved it in 1986. In order to keep the privacy of the data in the comparison process, order preserving encryption (OPE) [8, 9] is proposed. However, there are many interactions between the client and the server in OPE schemes. In 2013, Furukawa [5] proposed a request-based comparable encryption scheme which only needs one round communication. In 2015, Chen et al. [3] improved the comparison efficiency with sliding window method.

There are many researches on auctions, such as [6, 10, 13, 14]; however, most of them do not study the confidentiality of the bids. The general way to keep the auction privacy is using homomorphic encryption, such as [1, 12]. Peng et al. [11] proposed a new first-bid e-auction scheme based on secret sharing, which achieved bids privacy. Franklin and Reiter [4] proposed the design and implementation of a distribute service for performing sealed-bid auctions. Li et al. [7] proposed an anonymity auction scheme with zero knowledge proof. Brandt and Sandholm [2] studied the bid privacy problem in sealed bid auctions, and the authors proved that the first-price sealed-bid auction can be emulated by an unconditionally fully private protocol. However, there are many interactions between bidders and auctioneer.

1.3 Organization of this paper

The organization of this paper is as follows. Some preliminaries are given in Section 2. The privacy preserving auction system is given in Section 3. Then in Section 4 we give our protocol of secure auction. The security analysis is given in Section 5. The comparisons and efficiency analysis are given in Section 6. Finally, conclusion will be made in Section 7.

2 Preliminaries

2.1 Hash function

A hash function takes arbitrary data as input and returns a fixed-size bit string as output.

The secure hash function has four main properties:

- x, the computation of $h(x)$ is efficient.
- y, find x, which satisfies the equation $h(x) = y$, is computational infeasible.
- Given x_1, find x_2, which satisfies the equation $h(x_1) = h(x_2)$, is computational infeasible.
- Find x_1 and x_2, which satisfy the equation $h(x_1) = h(x_2)$, is computational infeasible.

2.2 Comparable encryption

We follow the definition in [5]. The comparable encryption has four algorithms, Gen, Enc, Der, and Cmp.

- Gen: Inputs a security parameter $\lambda \in \mathrm{N}$ and a range parameter $\mathrm{n} \in \mathrm{N}$, outputs a master key *mkey*. (*pa* is the parameter)

  $$(pa, mkey) \leftarrow Gen(\lambda, n)$$

- Der: Inputs the master key *mkey*, and a number $0 \le num < 2^n$, outputs a token t.

  $$t \leftarrow Der(mkey, num)$$

- Enc: Inputs the *mkey*, and a number $0 \le num < 2^n$, outputs a ciphertext c.

$$ciph \leftarrow Enc(mkey, num)$$

- Cmp: Inputs two ciphertexts c and $c^{'}$, and a token t, outputs {− 1,1,0}.

$$Cmp\left(ciph, ciph^{'}, t\right) \in \{-1, 1, 0\}$$

We assume the ciphertext c and the token t input to Cmp.

$$t = Der(mkey, num)$$

and

$$c = Enc(mkey, num).$$

The output of Cmp is {− 1,0,1}, respectively, when

$$num < num^{'},$$

$$num = num^{'},$$

or

$$num > num^{'}.$$

3 Privacy preserving auction system

3.1 Design goals

The design goals of our system are as follows.

- *Confidentiality.* To prevent the private information of each entity. Each bid should be only known by the bidder himself before the bid opening phase starts.
- *Correctness.* To make sure that the authority returns the correct results. The auction results should be determined according to the auction rule.
- *Privacy.* To make sure the losing bids are keeping secret. The losing bids should not be revealed in the process of the auction.
- *Secure Comparison*. The bids will not be revealed in the comparison process.
- *Fairness.* The bidders cannot be able to modify and/or deny the submitted bids.
- *Verification.* Participants could verify the winning bid.

3.2 Auction model

The auction system contains two parties, auctioneer (AU) and the bidders.

In order to keep the privacy of the bids, the bids should be encrypted before sending to AU.

AU constructs the action system and then generates the system parameters and the master key.

Bidders encrypt the data with the master key and generate the tokens with their random values.

The system model is shown in Fig. 1.

The auction system can be described as follows.

- *Setup.* The bidders share the masker key, which will be used to generate the ciphertexts and the tokens.
- *Token generation.* Each bidder generates the tokens of his/her encrypted data and sends the ciphertexts and tokens to AU.
- *Bidding comparison.* AU does some computations on the tokens and finds out the first different value of the ciphertexts. And then, it will give the bidding result.
- *Verification.* AU publishes token of the highest bid. The bidder who wins the auction should send the ciphertext to the auctioneer as a proof. The auctioneer checks whether the bidder is the winner

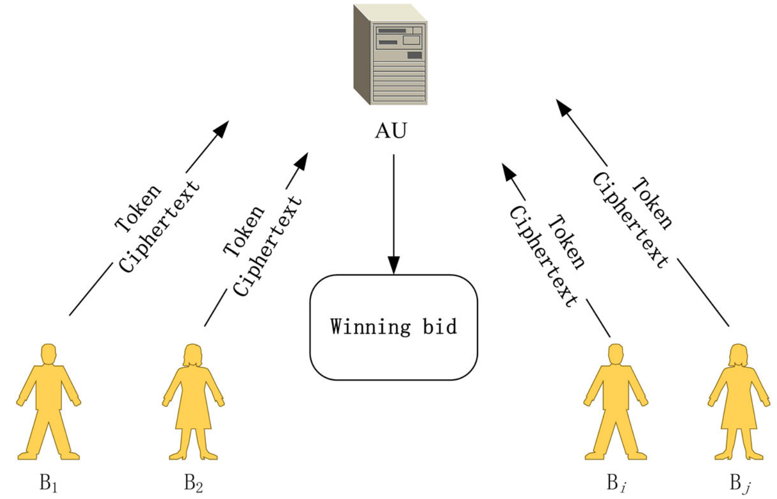

Fig. 1 Auction model

or not with the random number provided by the bidder.

4 Our construction of auction system with privacy protection

In this section, we give our privacy preserving scheme for first-price sealed-bid auction. We assume bidders do not collude with the auctioneer.

Setup. One of the bidders, such as B_1, generates the master key *mkey*, and then B_1 sends *mkey* to other bidders through a secure channel.

Token generationToken generation. Bidder B_j transforms the bid into binary form.

$$\text{bid} = \sum_{i=0}^{m} 2^{\mathrm{i}}\mathrm{b}_{\mathrm{i}} = (b_m, , b_{m-1}, \ldots, , b_1, b_{m0} \quad).$$

The token is generated as follows.

$$\begin{aligned} d_m &= H(mkey, (0, 0, 0)) \\ d_i &= H(mkey, (1, d_{i+1}, , b_i)) \end{aligned}$$

for $i = m - 1, \ldots, 0$.

B_i outputs the token

$$t = (d_0, , d_1, \ldots, , d_m).$$

Ciphertext generation. The bidder B_t randomly chooses $R \in Zp$ (p is a large prime number), and generates

$$\begin{aligned} c_i &= H(d_i, (2, 0, H(R))) \\ e_i &= H(mkey, (4, d_{i+1}, 0)) + b_i \bmod 3 \\ f_i &= H(d_{i+1}, (5, 0, H(R))) + e_i \bmod 3 \end{aligned}$$

for $i = m - 1, \ldots, 0$.

The output ciphertext is

$$ciph = (H(R), (c_0, \ldots, , c_{m-1}), (f_0, \ldots, , f_{m-1})).$$

Then, B_t sends the ciphertext *ciph* to auctioneer and publishes $H(R||f_0||f_1||\cdots||f_{m-1})$ as the winning proof.

Bidding comparison. The comparison of two bids is as follows.

1. Auctioneer selects two ciphertexts *ciph* and *ciph*$'$ and gets $H(R)$ and $H(R')$, then auctioneer compares the sequences in the two ciphertexts, until the first different pair appears. Let $0 \leq j \leq m - 1$, if k, $j < k \leq m - 1$,

$$c'_k = H\left(d_k, \left(2, 0, H\left(R'\right)\right)\right) \wedge \left(c'_j \neq H\left(d_j, \left(2, 0, H\left(R'\right)\right)\right)\right)$$

is true, then b_j and b'_j are the first different bits.

If $\forall k, 0 \leq k \leq m - 1$,

$$c'_k = H\left(d_k, \left(2, 0, H\left(R'\right)\right)\right)$$

holds, that means $bid = bid'$.

2. Auctioneer computes

$$\begin{aligned} \text{diff} \quad &= f_j - H\left(d_{j+1}\left(5, 0, H\left(R\right)\right)\right) \\ &\quad - \left(f_j - H\left(d_{j+1}, \left(5, 0, H\left(R'\right)\right)\right)\right) \quad \bmod 3 \\ &= b_j - b'_j \quad \bmod 3. \end{aligned}$$

If $bid > bid'$, then diff = 1 mod 3; else if $bid < bid'$, then diff = − 1 = 2 mod 3.

The comparisons will not stop until all the ciphertexts are compared, then the auctioneer outputs the winning result.

Verification. After the above comparison steps, the auctioneer publishes token and the ciphertext of the highest bid. The bidder who acclaims that he/she is the winner should send to the auctioneer his/her bid as the winning bid and the value R^* as the proof. The auctioneer check whether the bidder is the winner or not through the equation

$$H(R^*) \overset{?}{=} H(R).$$

If the verification is passed, the auctioneer publishes the winner's bid. And every bidder can verify the winning result.

5 Security analysis

5.1 Security of parameters

Theorem 1 *The bids will not be revealed in the comparison process.*

Proof The bid is as

$$bid = (b_m, , b_{m-1}, \cdots, , b_1, , b_0).$$

The token is $t = (d_0, d_1, \ldots, d_m)$, where

$$\begin{aligned} d_m &= H(mkey, (0, 0, 0)) \\ d_i &= H(mkey, (1, d_{i+1}, , b_i)) \end{aligned}$$

for $i = m - 1, \ldots, 0$.

And the ciphertext is $ciph = (H(R), (c_0, \ldots, c_{m-1}), (f_0, \ldots, f_{m-1}))$,

where

$$\begin{aligned} c_i &= H(d_i, (2, 0, H(R))) \\ e_i &= H(mkey, (4, d_{i+1}, 0)) + b_i \bmod 3 \\ f_i &= H(d_{i+1}, (5, 0, H(R))) + e_i \bmod 3 \end{aligned}$$

for $i = m - 1, \ldots, 0$.

The ciphertext is generated by the token, and the master key *mkey* is unknown to the auctioneer; thus, the auctioneer cannot generate a valid token, i.e., he/she cannot test the bids with other values.

On the other hand, the auctioneer only knows the difference ranges of the bids. Auctioneer knows the first different of two bids, that means the difference of the two bids is less than 2^j. If the auctioneer keeps on comparing, he/she cannot get any information about the bids.

In the comparison phase, auctioneer computes as follows: Set j form $m - 1$ to 0, if $\forall k, j < k \leq m - 1$,

$$c_k^{'} = H\left(d_k, \left(2, 0, H\left(R^{'}\right)\right)\right) \wedge \left(c_j^{'} \neq H\left(d_j, \left(2, 0, H\left(R^{'}\right)\right)\right)\right)$$

is true, then j is the location of the first different bit.

If auctioneer continues comparing with the rest of the information, in this case, $d_{j+1} = d_{j+i}^{'}$ and $d_j \neq d_j^{'}$. This means

$$\begin{aligned} & f_j - 1 - H\left(d_j, (5, 0, H(R))\right) - \left(f_j^{'} - 1 - H\left(d_j, \left(5, 0, H\left(R^{'}\right)\right)\right)\right) \\ & = H\left(d_j, (5, 0, H(R))\right) + e_j - H\left(d_j, (5, 0, H(R))\right) \\ & - \left(H\left(d'_j, \left(5, 0, H\left(R^{'}\right)\right)\right) - e_j^{'} + H\left(d_j, \left(5, 0, H\left(R^{'}\right)\right)\right)\right) \\ & = H\left(mkey, \left(4, d_j, 0\right)\right) + b_j - H\left(mkey, \left(4 \cdot d'_j, 0\right)\right) - b'_j \\ & \neq b_i - b_i^{'}. \end{aligned}$$

Hence, the auctioneer cannot do any further comparison.

Theorem 2 *No one can forge the winning identity, and the winner cannot change the winning bid.*

Proof If any bidder other than the winner acclaims that he/she is the winner, then he/she should generate the same ciphertext corresponding to the winning bid. Since he/she has no knowledge of random value R, and $H(.)$ is the non-collision hash function; thus, the probability that $H(R^*) = H(R)$ is negligible.

On the other hand, if the winner wants to change the winning bid, he/she should generate a valid ciphertext, which is less than the winning bid, and more than other bids. However, $H(.)$ is the non-collision hash function, it is impossible to generate the ciphertext and the random value equals the winning proof $H(R||f_0||f_1||\cdots||f_{m-1})$.

6 Comparisons and efficiency

6.1 Comparisons

Some comparisons with related work are shown in Table 1.

6.2 Efficiency analysis

We implement our mechanism using C language and pairing-based cryptography (PBC) library. The testing activity has been carried out on a LINUX machine with Intel Core TM i5-3239M processors running at 2.60 GHz and 4G memory. The time cost in token generation and comparison phase is shown in Figs. 2 and 3.

Table 1 Comparisons

Protocol	Auctioneer	Verifiability	Privacy	Round
[15]	m	√	√	O(n)
[7]	3	√	√	O(n)
Ours'	1	√	√	2

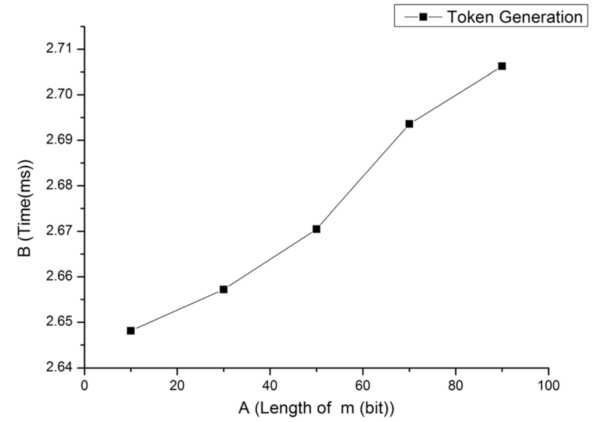

Fig. 2 Time cost of token generation

7 Conclusions

Fairness is one of the most important parts in all kinds of auctions. The basic of the fairness is the confidentiality of the bids. Anyone except the bidder should not know the real value of his/her bid in the auction process. In this paper, an efficient scheme for the construction of first-price sealed-bid auction based on comparable encryption is proposed. In our scheme, the confidentiality of each bid is protected, and the winning bid cannot be faked. In addition, we reduce the communication round between the bidders and the auctioneer, only two rounds are needed. Our scheme is practical, which can protect the bids of each bidder in the auction process.

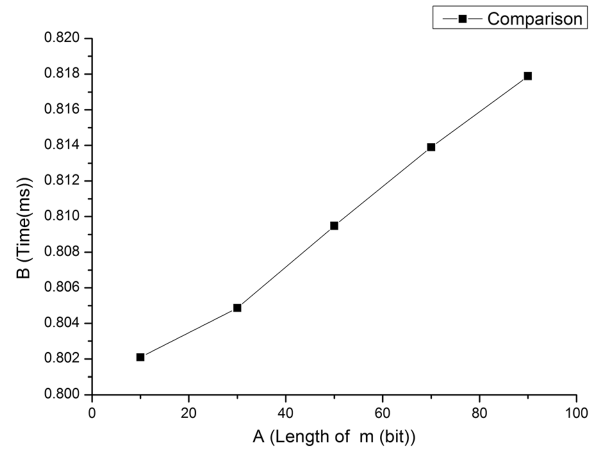

Fig. 3 Time cost in comparison phase

Acknowledgements

This work was supported in part by the Natural Science Foundation of Hainan Province (nos. 20156217 and 20166217), National Natural Science Foundation of China (no. 61661019), the Major Science and Technology Project of Hainan Province (no. ZDKJ2016015), and Research Center for Sichuan Liquor Industry Development (CJZ17-08).

Authors' contributions

ZG carried out the conception and design of the proposed auction scheme and drafted the manuscript. YF carried out the analysis and evaluation of the proposed method and the results' analysis and correctness. CC conceived of the study and participated in its design and completed the writings. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]School of Network and Information Security, Xidian University Xi'an, Shaanxi, People's Republic of China. [2]State Key Laboratory of Marine Resource Utilization in the South China Sea, College of Information Science and Technology, Hainan University, Hainan, People's Republic of China. [3]School of Management, Sichuan University of Science and Engineering, Zigong, Sichuan, People's Republic of China.

Received: 28 August 2017 Accepted: 31 October 2017
Published online: 22 November 2017

References

1. Baudron, O, & Stern, J (2001). Non-interactive private auctions. In *Proc. of the 5th International Conference on Financial Cryptography, FC 2001, Grand Cayman, British West Indies, February 19-22, 2002*, (p. 354).
2. F. Brandt and T. Sandholm, On the existence of unconditionally privacy-preserving auction protocols, *ACM Transaction on Information and System Security*, vol. 11, no. 2, pp. 6:1–6:21, 2008.
3. Chen, P, Ye, J, Chen, X (2015). A new efficient request-based comparable encryption scheme. In *Proc. of the 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Gwangiu, South Korea, March 24-27, 2015*, (pp. 436–439).
4. Franklin, MK, & Reiter, MK. (1996). The design and implementation of a secure auction service. *IEEE Transaction on Software Engineering*, *22*(5), 302–312.
5. Furukawa, J (2013). Request-based comparable encryption. In *Proc. of the 18th European Symposium on Research in Computer Security Computer Security, ESORICS 2013, Egham, UK, September 9-13, 2013, vol. 8134*, (pp. 129–146).
6. Gerkey, BP, & Mataric, MJ. (2002). Sold!: auction methods for multirobot coordination. *IEEE Transaction on Robotics and Automation*, *18*(5), 758–768.
7. Li, M, Juan, JS, Tsai, JH. (2011). Practical electronic auction scheme with strong anonymity and bidding privacy. *Information Science*, *181*(12), 2576–2586.
8. Liu, Z, Chen, X, Yang, J, Jia, C, You, I. (2016). New order preserving encryption model for outsourced databases in cloud environments. *Journal of Network and Computer Applications*, *59*, 198–207.
9. Mavroforakis, C, Chenette, N, O'Neill, A, Kollios, G, Canetti, R (2015). Modular order-preserving encryption, revisited. In *Proc. of the 2015 ACM SIGMOD International Conference on Management of Data, vol. 7115*, (pp. 763–777).
10. Ono, C, Nishiyama, S, Horiuchi, H (2002). An efficient winner determination algorithm for combinatorial ascending auctions. In *Proc. of the International Conference on Artificial Intelligence, IC-AI'02, June 24–27, 2002*, (vol. 1, pp. 52–56).
11. Peng, K, Boyd, C, Dawson, E (2005). Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing. In *Proc. of the First International Conference on on Cryptology in Malaysia in Cryptology - Mycrypt'05, Kuala Lumpur, Malaysia, September 28-30, 2005*, (pp. 84–98).
12. Wang, X, Ji, Y, Zhou, H, Liu, Z, Gu, Y, Li, J (2015). A privacy preserving truthful spectrum auction scheme using homomorphic encryption. In *Proc. of 2015 IEEE Global Communications Conference, GLOBECOM 2015, San Diego, CA, USA, December 6-10, 2015*, (pp. 1–6).
13. Wellman, MP, Walsh, WE, Wurman, PR, MacKie-Mason, JK. (2001). Auction protocols for decentralized scheduling. *Games and Economic Behavior*, *35*(1-2), 271–303.
14. Wurman, PR, Wellman, MP, Walsh, WE. (2001). A parametrization of the auction design space. *Games and Economic Behavior*, *35*(1-2), 304–338.
15. Yao, AC (1986). How to generate and exchange secrets. In *Proc. of the 27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, October 27-29, 1986*, (pp. 162–167).