Privacy Preserving Second-Price Sealed Bid Auction System

Lu Li
Yancheng Teachers University

Xiangyu Xiong
Yancheng Teachers University

Abstract

Sealed auction has become a commodity trade mode which is loved by most people, due to it's fairness and high allocation efficiency. The previous research is mainly devoted to design a auction scheme satisfying authenticity, namly the bidder can get the maximum profit ony if he give the real estimate price of the goods. However, the true estimate price is the typical private infomation. The malicious auctioneer and some other bidders can use these private infomation illegally to get profit once a bidder reveal his infomation to them, this will damage the interest of honest bidders. Therefore, it's significant to ensure that the real estimate prices of all bidders are not be leaked out. Under this background, we implement a secure and efficient privacy preserving auction protocal via *Yao protocal* and *Paillier homomorphic cryptosystem*, taking second-price sealed auction as a original model. In this protocal, all participants (including auctioneer) won't get any intermediate information except that the results of auction are made known to public. This will make sure that bids of all bidders are not leaked out. Meanwhile, we make the privacy preserving second-price sealed bid auction system based on *FastGC framework*. The results of experiment show that the running time is less than 4 s with 50 bidders. This meets the requirement of real application.

1 Introduction

Auction has been a favorite trade mode beacuse of it's fairness and high allocation efficiency. Realness is the main object of an auction scheme. In recent years, many research work [1,3,4,7,8,15–18,20] have devoted to design the auction scheme with realness. However, the true estimate price is the typical private infomation. The malicious auctioneer and some other bidders can use these private infomation illegally to get profit once a bidder reveal his infomation to them, this will damage the interest of honest bidders. As mentioned in bibliography [11], a malicious auctioneer may make use of private bids of honest bidders to collude with other bidders. In addition, a bidder will not use his real estimate price to participate auction when he knows the private bids of other bidders. This will make the auction scheme loss the properties of realness when it is carried out repeatedly. Thus, it's important to make sure that the real estimate prices of all bidders are not be leaked out.

Over the past decade, a lot of research work about privacy preserving of auction mechanism has been done by scholars. They make tradeoff between efficiency and private preserving for auction scheme [19] and bring forward the corresponding auction framework. Brandt and Sandholm have researched the unconditional security problems [2]. The researchers use different cryptographic methods to guarantee the security of privacy for different auction mechanism [9, 12–14, 22]. However, these work is either not secure (for example, the range of marked price for buyers will be exposed to auctioneer [14]) or need exponential time complexity in auction application. Recently, there have been some spectrum auction schemes [5, 11]which can protect privacy. Nevertheless, all of these work can not guarantee the security. Until 2014, an auction scheme based on homomorphic encryption was presented. It makes paillier [10] homomorphic encryption for every bit of bids to guarantee the correctness and security. However, this theme can't apply to practical application due to it's low time efficiency.

Auction has been a popular trade method currently, it need an effective auction mechanism. The second-price sealed auction is just an effective auction mechanism theoretically. Because at this time, the best strategy for every bidder is to bid according to his own estimated price of the goods he wants. This is obviously a trade mode in accordance with incentive compatibility principle. Furthermore, it is an allocation method which can make both the buyers and sellers reach *pareto optimality*. But the implementation of the auction may face many problems in practice. For instance, the effectiveness of the trade mode will be broken if the bidders collude with each other or the bidders collude the auctioneer.

2 Contibution

The main problem of privacy preserving second-price auction system is to get the index of *1*-th largest value b$_i$, namely i, and the *2*-th largest value b$_j$ in buyer's bid sequence without revealing any bid of buyers. The main contributions of this paper are as follow:

- We construct a security protocol which can let two parties find the index of *1*-th largest value b$_i$ and the *2*-th largest value b$_j$ in bid sequence efficiently. Further, we implement the protocal based on Yao protocal [21] and FastGC framework [6].
- We design the complete privacy preserving second-price sealed bid auction protocal and implement secure and efficient second-price auction system, via paillier homomorphic encryption algorithm and above constructed protocal.

3 Cryptographic Background

This section mainly introduce cryptographic tools that we use: Pillier homomorphic cryptosystem and Yao protocal.

3.1 Paillier Homomorphic Cryptosystem

Paillier homomorphic cryptosystem is a probabilistic public key encryption system invented by Paillier in 1999, based on the difficult problem of compound residual class. The specific process is as follows:

System Parameter: Choose two big primes p and q and compute $n = pq$. Choose random integer g which meets the equation $gcd(L(g^{\lambda} modn^2), n) = 1$, and $L(x) = \frac{x-1}{n}$. The system public key is (n, g) and system private key is $\lambda(n) = lcm((p-1),(q-1))$.

Encryption: choose random $r \in z_p^*$, $E(m) = g^m r^n modn^2$.

Decryption: $m = \frac{L(E(m)^{\lambda(n)} modn^2)}{L(g^{\lambda(n)} modn^2)} modn$.

Homomorphic encryption scheme. For the plaintext m_1, m_2 encrypted, the ciphertext are $E(m_1) = g^{m_1} r_1^n modn^2$, $E(m_2) = g^{m_2} r_2^n modn^2$ respectively. Furthermore, for $E(m_1)E(m_2) = g^{m_1+m_2}(r_1 r_2) modn^2$, we have $D(E(m_1)E(m_2)) = m_1 + m_2$ after decryption.

3.2 Yao Protocal

Yao protocal is also known for constructing two-party security protocol method. It assumes that two participants, *Cloud A* and *Cloud B* hold private data x and y respectively. They want to evaluate an arbitrary function $f(x, y)$ without leaking their inputs and any intermediate values. Yao's main ideal is that let one participant (assume he is *Cloud A*, who is also called circuit generator) construct an encrypted version of boolean circuit to evaluate *f*, and the other participant (assume he is *Cloud B* called circuit evaluator) computes obliviously in the encrypted boolean circuit.

4 Implementation Overview

The privacy preserving second-price sealed bid auction system we design can make the highest bidder win commodity of auction. Howerver, the winning bidder just need to pay the second highest bid. The source code of this system and the corresponding application can be get from https://github.com/yXiangXiong/. Our auction model encrypt the infomation of the auction process by Paillier homomorphic encryption algorithm and send it out for communication (see Section 4.1), this guarantee the security of the system. we design a secure protocal to find index of *1*-th largest value b$_i$, and the *2*-th largest value b$_j$ in buyer's bid sequence(see Section 4.2). In the end, we show the details about how to contruct the garbled circuit for auction process (see Section 4.3).

4.1 Auction Model Design

Our model include three kind of parties: auction agent, auctioneer and some bidders. We assume that the agent not to collude with auctioneer. They cooperate with each other to finish computation in auction. First of all, we need to let the auctioneer and the agent share the bids of buyers (see Algorithm 1). In the begin of this protocal, every bidder uses the public key choosen by agent to encrypt his private bid, and send the encrypted bid along with his ID to the auctioneer. Once receiving an encrypted value from the bidders. The auctioneer masks this value by a random number chosen in a sufficiently large domain, and submits the masked bid to the agent. The execution of this protocol ensures that all the bids are additively secret shared between the auctioneer and the agent. You can see the complete model in Figure 1.

Algorithm 1 Data Outsourcing

```
Input:
    Agent: $(p_k, s_k)$; Buyers: $b_1, ..., b_n$;
Output:
    Auctioneer and Agent: $[[b_1]], ..., [[b_n]]$.
1: Agent chooses a key pair $(p_k, s_k)$ in the Paillier cryptosystem and sends public key $p_k$ to all bidders.
2: Each buyer encrypts $b_i$, sends $E_{p_k}(b_i)$ and his ID to auctioneer.
3: Auctioneer generates $n$ random numbers $r_1, ..., r_n$, calculates $E_{p_k}(b_1) * E_{p_k}(r_1), ..., E_{p_k}(b_n) * E_{p_k}(r_n)$, and sends this sequence together with the corresponding ID of sequence element to agent.
4: Agent decrypts received data to get $b_1 + r_1, ..., b_n + r_n$ as the share of bids. Auctioneer use $-r_1, ..., -r_n$ as the share of bids.
```

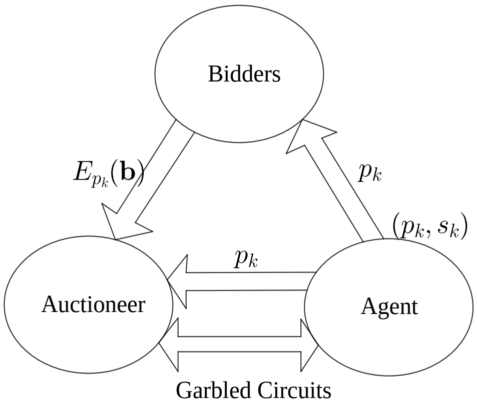

Figure 1: Security auction model.

4.2 Security Protocol

Since FastGC has a basic framework of garbled circuit already for Yao protocal , we add the garbled circuit designed based on it to satisfy the auction demand. The auctioneer make the random numbers they hold multiply by negative one(see Algorithm 1, Step 4). These negative numbers were taken as inputs of circuit genetator. Agent take the decrypted value(see Algorithm 1, Step 4) as inputs of circuit evaluator. The Auctioneer will get the expected result through the garbled circuit module. The process is shown in Algorithm 2 as below.

Algorithm 2 Security Protocol

```
Input:
    Agent: $r_1, ..., r_n$ and $id_1, ..., id_n$;
    Buyers: $b_1 + r_1, ..., b_n + r_n$ and $id_1, ..., id_n$;
Output:
    Auctioneer: $id(max\{b_1, ..., b_n\}), secondMax\{b_1, ..., b_n\}$.

1: Auctioneer make the random numbers $r_1, ..., r_n$ multiply by negative one to get the sequence $-r_1, ..., -r_n$.
2: Auctioneer takes the sequence $-r_1, ..., -r_n$ as inputs of circuit genetator. Agent takes the sequence $b_1 + r_1, ..., b_n + r_n$ as inputs of circuit evaluator.
3: Auctioneer gets the ID of 1-th largest value of sequence $b_1, ..., b_n$ and 2-th largest value of squence $b_1, ..., b_n$, via garbled circuit module.
```

4.3 Garbled Circuits For Auction

Yao protocal has been an effective cryptographic tool to construct the high-level security protocal at present. It's more efficient to use Yao protocal deal with non linear operation than to use additive homomorphic cryptosystem. Therefore, we make use of Yao protocal to deal with non linear operation too. We construct the high-leve circuit via Yao Protocal for computing auction, see Figure 2. Firstly, this circuit calulate the sum of two l-bit number from the two input sequence in order respectively. Secondly, it uses a subcircuit Filter to calculate the index of *1*-th largest value and the *2*-th largest value in the sum sequence. The output of this subcircuit are d-bit index of *1*-th largest value and $l+1$-bit *2*-th largest value int the sum sequence.

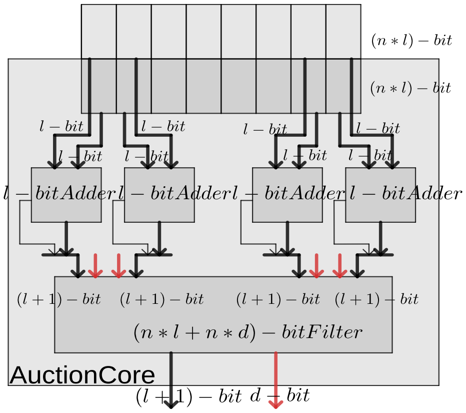

Figure 2: Implementations of Acution core circuit.

Figure3 shows the construction of subcircuit Filter. This subcircuit takes each element of the input sequence with element's index as the inputs. Firstly, it calulates the *1*-th largest value with index and the 2-th largest value with index between *1*-th element and 2-th element. Secondly, it uses the later elements to update the *1*-th largest value with index and the 2-th largest value with index. Of course, we only reserve the index of *1*-th largest value and the 2-th largest value.

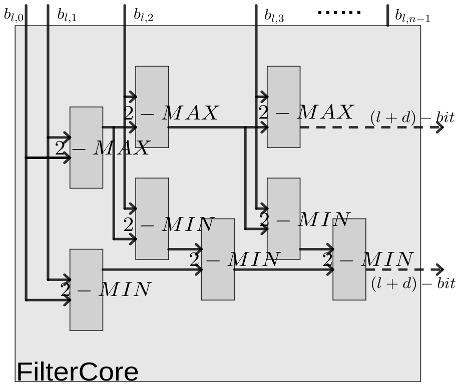

Figure 3: Implementation of FilterCore Circuit.

5 Result

The security and correctness of the system are guaranteed by it's own system scheme. So we only track the time that the garbled circuit modulde has been running. This running time creases with the increase of number of buyers. You can set up parameters such as the number of buyers according to auction requirement in our system. The highest bidder will receive the second highest bid he should pay.

We use some same Lenovo computers(2GHz CPU and 4GB RAM) to test the auction system. We test three times on the given number of buyers and take the average value as the running time of garbled circuit. The result of the test is shown in Figure 4.

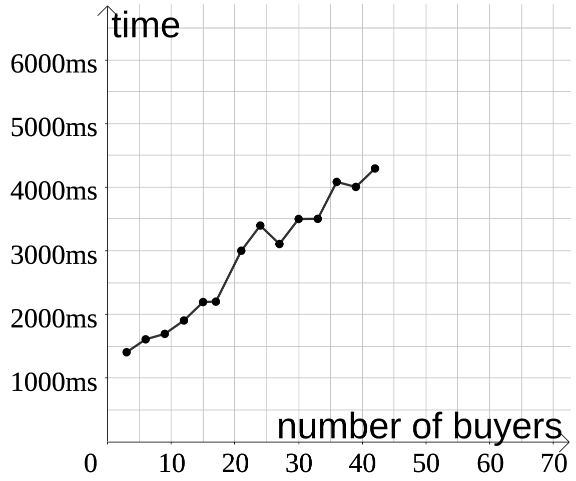

Figure 4: Running time of our garbeled circuit modulde for different number of buyers.

Result analysis: The running time is direct proportion increased with number of buyers. Although the number of buyers increase, the consuming time is still in a small time range. This proofs that our system is of high efficiency, and it can satisfy actual application.

6 Conclusion

It is significant to guarantee the real evaluation infomation of all bidders not to leak during the sealed auction process. Based on this background, we construct a privacy preserving auction protocal of security and high efficiency, taking second-price sealed auction as a original mode, based on Yao protocal and Paillier homomorphic cryptosystem. In this protocal, the final auction result is the only infomation revealed to the participates. All participates(including auctioneer) won't learn any intermediate infomation. This makes the private bids of all users not leak out. Through some test, the system can not only finish second-price sealed auction but also sovle the existing privacy problems. It completely meets the needs of practical application.

Acknowledgments

We thank our country.

References

[1] M. Al-Ayyoub and H. Gupta. Truthful spectrum auctions with approximate revenue. In *2011 Proceedings IEEE INFOCOM*, pages 2813–2821, April 2011.

[2] Felix Brandt and Tuomas Sandholm. *On the Existence of Unconditionally Privacy-Preserving Auction Protocols*. 2008.

[3] Wu Fan and Nitin Vaidya. Small: A strategy-proof mechanism for radio spectrum allocation. In *Infocom, IEEE*, 2011.

[4] X. Feng, , J. Zhang, and Q. Zhang and. Tahes: Truthful double auction for heterogeneous spectrums. In *2012 Proceedings IEEE INFOCOM*, pages 3076–3080, March 2012.

[5] Qianyi Huang, Yixin Tao, and Wu Fan. Spring: A strategy-proof and privacy preserving spectrum auction mechanism. In *Infocom, IEEE*, 2012.

[6] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In *Usenix Conference on Security*, 2011.

[7] Juncheng Jia, Qian Zhang, Qin Zhang, and Mingyan Liu. Revenue generation for truthful spectrum auction in dynamic spectrum access. pages 3–12, 05 2009.

[8] Ali Kakhbod, Ashutosh Nayyar, and Demosthenis Teneketzis. Revenue maximization in spectrum auctions for dynamic spectrum access. In *International Icst Conference on Performance Evaluation Methodologies & Tools*, 2011.

[9] Moni Naor, Benny Pinkas, and Reuban Sumner. Privacy preserving auctions and mechanism design. In *Proc Acm Conference on Electronic Commerce*, 1999.

[10] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, pages 223–238, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

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

[12] Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan. Robust, privacy protecting and publicly verifiable sealed-bid auction. 2002.

[13] Koutarou Suzuki and Makoto Yokoo. Secure generalized vickrey auction using homomorphic encryption. In *International Financial Cryptography Conference*, 2003.

[14] Changjie Wang, Hofung Leung, and Yumin Wang. Secure double auction protocols with full privacy protection. In *Information Security & Cryptology-icisc, International Conference, Seoul, Korea, November, Revised Papers*, 2003.

[15] Qinhui Wang, Baoliu Ye, Tianyin Xu, Sanglu Lu, and Guo Song. Dota: A double truthful auction for spectrum allocation in dynamic spectrum access. IEEEWirelessCommunicationsandNetworking-Conference(WCNC2012), 2012.

[16] Shi Guang Wang, Xu Ping, Xiao Hua Xu, Shao Jie Tang, and Liu Xin. Toda: Truthful online double auction for spectrum allocation in wireless networks. In *IEEE Symposium on New Frontiers in Dynamic Spectrum*, 2015.

[17] Zuying Wei, Tianrong Zhang, Fan wu, Guihai Chen, and Xiaofeng Gao. Shield: A strategy-proof and highly efficient channel auction mechanism for multi-radio wireless networks. volume 7405, 08 2012.

[18] Zhou Xia and Heather Zheng. Trust: A general framework for truthful double spectrum auctions. In *Infocom*, 2009.

[19] Sui Xin and Craig Boutilier. Efficiency and privacy tradeoffs in mechanism design. In *Aaai Conference on Artificial Intelligence*, 2011.

[20] Dejun Yang, Xiang Zhang, and Guoliang Xue. Promise: A framework for truthful and profit maximizing spectrum double auctions. In *Proceedings - IEEE INFOCOM*, pages 109–117. Institute of Electrical and Electronics Engineers Inc., 2014.

[21] A. C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 160–164, Nov 1982.

[22] Makoto Yokoo and Koutarou Suzuki. Secure generalized vickrey auction without third-party servers. In *Financial Cryptography, International Conference, Fc, Key West, Fl, Usa, February, Revised Papers*, 2004.