I.J. Wireless and Microwave Technologies **2012, 1, 60-65**
Published Online February 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012.01.09

Available online at http://www.mecs-press.net/ijwmt

A double auction scheme based on secret sharing and safe comparing protocol

[a1] Bin Zhang, [a2] Qiuliang Xu, [a3] Han Jiang

[a] *School of computer science and technology Shandong University Jinan, China*

Abstract

At present most practical electrical auction schemes that based on secret sharing, group signature and hash chain assume the existence of a trusted thid party, while the schemes that based on commitment, zero knowledge or homomorphic encryption without the TTP model face the problem of high cost of communication and computation. The double auction scheme proposed by Bogetoft is based on secure multiparty computation without a TTP and get very high efficiency. In this article, we improve the above scheme. Based on secret sharing and constant round safe comparing protocol, we reduce the requirement of honest majority in the original scheme. We improve the security of the scheme while maintain the high efficiency.

Index Terms: Double auction, safe comparing, secret sharing, secure multiparty computation

1. Introduction

With the development of electronical commerce, more and more electronical auntion appear on the internet. Electronical auntion can be sorted as English auction, Holand auction and sealed-bid auction according to bid fashion, or sorted as first price auction and second price auction according to winning price[1].

Sealed-bid auction catch most attention in the research field. Franklin[2] gave the earliest sealed-bid electronical auction protocol based on secret sharing, Kudo[3] proposed the distributed auction system based on public key encryption scheme, Sakurai[4] gave the auction scheme based on group signature, Suzuki[5] construct hash chain protocol based on the onewayness and high efficiency of hash function, and make the protocol very efficiently, but the protocols rely on trusted auctioneer or other trusted third party, and the condition is not fulfiled in the real world. Beside this kind of protocol, Abe[6] proposed receipt free auction based on Chameleon commitment and interactive zero knowledge proof, Brandt[7] proposed perfect secure auction based on homomorphic encryption,but these protocols had high comunication and computation cost, and can't be used to realize large scale practical system. Bogetoft[8] proposed a double electronical auction system based on secret sharing,safe comparing and other multiparty computation technique. There is no TTP in the

Corresponding author:
E-mail address: [1]tthammer@163.com, [2]xuqiuliang@sdu.edu.cn, [3]jianghan@sdu.edu.cn

scheme and it get high efficiency. In this article, we make further improvement on the Bogetoft scheme,reduce the condition of honest majority, make the scheme more secure and maintain the high efficiency.

2. preliminaries

2.1. Double electronical auction

In Double electronical auction scenario, there are many buyers and sellers. For goods to be traded, every buyer give the amount he want to buy at every price, and every seller give the amount he want to sell at every price. All the data are sent to the auctioneer and the total supply *S* and total demand *D* on every price are computed. It can be assumed that with the rise of the price, total supply increase and total demand decrease, and there must be a price that *S* equal to *D*. The price is called the clearing price of the market, and at this price all the bidder give their amount will trade according to their amount.

In the concrete scenario of Bogetoft scheme, the parties are producers of the goods, the default auctioneer is the company D which purchase the goods. The target to be traded is the contract between the producers and the company, trading is between the producers.To realize the trading, a scheme with correctness, fairness and security should be designed.

Double auction in the scenario need special security feature, for the data of every bidder reveal some private information, such as his economic status and his productivity. And because the situation of company D in the market, the producer don't want it to be the auctioneer, for it may use the private information in the auction to get advantage in the new contract signing. On the other side, because the authorized amount in the contract is related to the company, and it has responsibility to the contract, the company want to attent the auction to make sure about the fairness of the auction. Because of the distrust among the producers and the company, and the high cost of engage a trusted organization to be the auctioneer, a electronical auction system based on secure multi-party computation without a TTP is a better approach for the situation.

2.2. Constant round safe comparing protocol

In the electronical auction protocol based on secure multi-party computation, safe comparing protocol is the basic sub-protocol, and is the most time-consuming sub-protocol, its efficiency will affect the auction efficiency directly. In the Bogetoft scheme a safe comparing protocol with logarithmic round was used, and the most efficient protocol now is const round. We change a const round safe comparing protocol based on homomorphic encryption to a protocol based on secret sharing, and make it convenient to be embeded in the Bogetoft scheme, and make it more efficient.

3. Bogetoft auction protocol based on SMPC

In Bogetoft scheme, a multi-party computation was used to play the role of auctioneer, the parties in the computation include company D, organization of the producers and the project designer. In the scheme, the input data from the clients was shared among the three parties through secret sharing, and the clearing price was calculated through multi-party among the three servers.

It is assumed that there exist point-to-point secure channel between servers, this can be realized by standard cryptography tools. A standard secret sharing was used among the n servers. The computation was in a prime field Z_p .It is assumed that there exists a static passive adversary, which can corrupt any number of clients and minority of servers. A polynomial f was randomly choosed to share a number x , which the degree is no more than *t*. Let $f(0) = x$, and the shares of x are $f(1),...,f(n)$. $[x]$ was used to represent the set of shares of x . In the concrete scene of the scheme, $n = 3$ and $t = 1$. The scheme is composed of these parts:

Setup: It is assumed that before computation, public and private key pairs are generated for servers. That is, for every unauthorized server set A, there is a private key sk_A and a public key pk_A for all the servers outside A.

Non-interactive input: Not as general sharing method, a non-interactive VSS method was used, and a simple edition was get when $n = 3$. We assume that there are three key pairs $(pk_i, sk_i), i = 1,2,3$, Server i has two sk_j where $j \neq i$. Now let $f_i(x), i = 1,2,3$ represent a polynomial which degree is no more than 1, and it fulfil that $f_i(0) = 1, f_i(i) = 0$. And we share the input $x_1,...,x_P$ to the servers as follows:

1. For a pseudorandom function F , let index *j* as its input and choose K_1, K_2, K_3 as it's keys,
2. Output encryptions $E_{pki}(K_i)$; i = 1, 2, 3.
3. For $j = 1,...,P$, compute and output $y_j = F_{K_1}(j) + F_{K_2}(j) + F_{K_3}(j) + x_j \bmod p$

Each server P_a can now process such an encryption and compute a Shamir share of each number:

1. Decrypt the two ciphertexts $E_{pki}(K_i)$ where $i \neq a$.
2. Compute the share $share_{a,j}$ of x_j as follows: $share_{a,j} = y_j - F_{K_1}(j)f_1(a) - F_{K_2}(j)f_2(a) - F_{K_3}(j)f_3(a)$

It is straightforward to see that if we define the polynomial g_j as $g_j = y_j - F_{K_1}(j)f_1 - F_{K_2}(j)f_2 - F_{K_3}(j)f_3$, then indeed $\deg(g) \leq 1$, $g_j(0) = x_j$ and $g_j(a) = share_{a,j}$, so that a valid set of shares has indeed been computed. And we can generalize the method to any number of servers with threshold *t*.

Addition and Multiplication: After input stage, all the input data have been shared with polynomials which degree are no more than *t*, and the addition and multiplication can be done with standard protocol.

Random Bit: All servers secretly share a random value, and add all shares locally, to form a sharing $[u]$ of a random unknown *u*. We then compute $[v] = [u^2 \bmod p]$ and open *v*. If $v = 0$ we start over, otherwise we publicly compute a square root *w* of *v*, say we choose the smallest one. Then We compute $w^{-1}[u] \bmod p$ which will be 1 with probability 1/2 and -1 with probability 1/2. Therefore, $[(w^{-1}u + 1)/2 \bmod p]$ will produce the random shared binary value we wanted.

Safe comparing: In the protocol below, we assume it can access the functionality F including the parts above. We define a operator $\diamond$ on bit-pairs as below:

$$(x, X) \diamond (y, Y) = (x \wedge y, y(X \oplus Y) \oplus X)$$

where ^ denotes the Boolean AND operator. Note that if we have $[a]$,$[b]$, where *a*, *b* are guaranteed to be 0/1 values, then $[a \oplus b]$ can be computed using operations from F as $[a] + [b] - 2[ab]$. So we can assume that $\oplus$ on binary values is available, and so $\diamond$ can also be implemented. It is easy to verify that $\diamond$ is associative.

Concrete protocol: Input $[d]$, $[s]$. Output: 1 if $d \geq s$, 0 otherwise

For $i = 0,...,l + k + 1$, call RandomBit to generate $[r_i]$ for random $r_i \in \{0,1\}$. Compute $[r] = \sum_i 2^i [r_i]$.

Compute $[a] = 2^{l+k+1} - [r] + 2^l + [d] - [s]$. Open a ,and compute the bits a_i of a

Now compute the carry bit at position l of $a + r = 2^{l+k+1} + 2^l + [d] - [s]$ as below

$$([a_{l-1} \oplus r_{l-1}], [a_{l-1}]) \diamond ... \diamond ([a_0 \oplus r_0], [a_0]) \diamond ([0], [0])$$

Compute [res]=$a_l \oplus [r_l]$ $[Z]$,open and output res。

Based on the sub-protocols above, it is easy to compute the total demands and total supplies on the price chain securely, and make bisearch on the price chain based on safe comparing of total demands and total supplies. Finaly with UC composition theorem the double auction protocol can be securely realized.

4. Improved double auction scheme

The condition of honest majority is required in the Bogetoft scheme, but in some real-life situation this requirement may not be fulfiled. So we improve the original protocol, make the original server as adding server and add another two comparing server. At the input stage, the data of client are blinded and shared between the adding servers. The adding servers complete the computation of total supplies and total demands and send them to comparing servers seperately and securely. The comparing servers do secure comparing of total supplies and total demands on the price chain with bisearch and at the position where total supply equal to total demand they get the clearing price. Because the new scheme is based on the safe comparing, there should be a safe comparing protocol with high round efficiency and high computation efficiency.

4. 1 Constant round safe comparing based on secret sharing

Let's assume the safe parameter be k. A big prime p with $2k+1$ bit shoud be generated first, and the follow computation should be done in the finite field Z_p . Let's assume Alice take the input a , Bob take the input b , while their bit number do not exceed k. Alice and Bob may carry out the follow protocol to compare their inputs without leak information about them to each other.

CCOM safe comparing protocol is as follow:

First step: Alice randomly choose a polynomial with degree 1: $f_1(x) = c_1 ? x \quad a$ and send $f_1(2)$ to Bob.

Second step: Bob randomly choose three number u , v and w with bit number not exceeding k, and they fulfil the condition $0 < v - w < u$; Bob then randomly choose two polynomial with degree 1: $f_2(x) = c_2 ? x \quad u$ and $f_3(x) = c_3 ? x \quad v$; finally Bob send $f_2(1)$, $f_3(1)$ and $Y = ub + w$ to Alice.

Third step: Alice and Bob compute $X = ua + v$ jointly.

Fourth Step: Bob send the secret share of X to Alice

Fifth Step: Alice get the plaintext of X with Lagrange interpolation. Alice judge that if $X > Y$ then $a \geq b$, else $a < b$. Alice send the comparing result to Bob. Since $X-Y = (ua+v)-(ub+w) = u(a-b)+(v-w) < u(a-b)+u = u(a-b+1)$ and $X-Y > u(a-b-1)$ with the same reason, when $a \geq b$,there must be $X > Y$, and when $a < b$, $X < Y$. So the protocol is correct. And we point out that since the computation is executed on Z_p , the judgement of $X > Y$ is to determine the bit number of $X - Y$ do not exceed $2k$, which means that there is not addition with p ,otherwise it means $X < Y$.

Since in the protocol there is only one multiplication operation taked with multiparty computation, the protocol is constant round. And because the protocol is the migration of [9]under the secret sharing mode, so the security argument is similar.

4. 2 Concrete auction scheme

The concrete auction process is as follows:

Setup: It is the same as the Bogetoft scheme, in this stage the system parameter should be generated according to the safe parameter, the secret key and public key pairs of server groups should be generated, and the point-to-point secure channel between servers should be set up.

Non-Interactive Input: It is similar to Bogetoft scheme, while the difference is that the input of clients should be blinded to prevent the comparing server get the total supplies or total demands on the price chain. Let's assume there are m clients $C_1, C_2, \ldots, C_m$ in the system, and the input of client C_i is $x_{i,j}$, $y_{i,j}$, $j = 1, \ldots, P$, P is the upper bound of the price of goods. $x_{i,j}$ represent the number of goods that client C_i want to buy, and

$y_{i,j}$ represent the number of goods that client C_i want to sell. Client C_i randomly choose $r_{i,j}$? Z_p, j 1,...,P , set $x_{i,j}$ * = $x_{i,j}$ + $r_{i,j}$, $y_{i,j}$ * = $y_{i,j}$ + $r_{i,j}$ .The client share $x_{i,j}$ * and $y_{i,j}$ * on the price chain according to the sharing method used in the Bogetoft method,and encrypt them with corresponding group public key and send them to corresponding adding servers.

Addition: The aim of this step is to compute the blinded total supplies and total demands on the price chain. It is similar as Bogetoft scheme,the adding server decrypt the encrypted data, and get the sharing of blinded data of clients after computation. To complete the adding operation of input [a] and [b], the server only need to add their shares of [a] and [b] locally. With this method, the adding servers get the shares of blinded total supplies and total demands on the price chain after computation. That is

$$D_j^* = \sum_{i=1}^{m} y_{i,j}^* = \sum_{i=1}^{m} y_{i,j} + \sum_{i=1}^{m} r_{i,j}$$

$$S_j^* = \sum_{i=1}^{m} x_{i,j}^* = \sum_{i=1}^{m} x_{i,j} + \sum_{i=1}^{m} r_{i,j}$$

Open on the comparing servers: The adding servers send the shares of total demands [D_j *] to the demand server securely and send the shares of total supplies [S_j *] to the supply server. The demand server get D_j * by Lagrange interpolation with [D_j *] and the supply server get S_j * accordingly.

Compute the clearing price: The comparing server make bisearch on the price chain based on safe comparing. They execute the following iterative algorithm:

①set $pl = 1, pr = P$;

②compute $pm = \lfloor (pl + pr)/2 \rfloor$;

③The demand server give D_{pm} * as input, The supply server give S_{pm} * as input, they invoke CCOM protocol to compare D_{pm} * and S_{pm} * safely.

④If $pl = pm$, then output pm , stop. If D_{pm} * ³ S_{pm} * , let $pl = pm$; else let $pr = pm$. Goto ②.

5. security and efficiency analysis

Because the clients only blind and share their input data, they can't get any other information,so the protocol can bear any number of semi-honest clients. To the adding servers, to get the information of client's blinded input data, the adversary must control more then t servers, otherwise it can only get random number,so the protocol can bear no more then t semi-honest adding server. To comparing servers, any party of the two get a number indistinguishable with a random number, only when the adversay can get all the information on the two server, can it get the relation between the total supplies S_j and the total demands D_j . So the protocol is safe under any number of semi-honest clients, no more then t semi-honest adding servers and no more then 1/2 semi-honest comparing servers.

Because the communication round number in the input stage and the comparing stage are all constant, and the round number of Bogetoft scheme are $O(\log(l))$ round ,so the efficiency of our scheme is better.

Moreover, our scheme inherit the advantage of the non-interactive VSS in the Bogetoft scheme:the client need not to generate different cipher with different server for a same plaintext,it can broadcast a same cipher; and between client and servers it do not need more interaction except that the client send secret shares by a one time

communication; and if some adding servers whose number not exceeding *t* lost their keys,other adding servers could help to recover their keys,so this scheme inherit the robustness of the Bogetoft scheme.

6. Conclusion

In this article we argue the double auction protocol and the realization scheme, we improve the Bogetoft scheme, reduce the requirement of honest majority condition, and realize better security, and we also make some improvement in the efficiency of the scheme. The scheme can be used in situations which require more security and better efficiency.

Acknowledgment

The authors wish to thank anonymous reviewers for giving helpful suggestions. This work is supported by the National Nature Science Foundation of China under Grant No. 60873232, China Postdoctoral Science Foundation of No. 20090461220, Natural Science Foundation of Shandong Province, China (No.ZR2010FM045), and Independent Innovation Foundation of Shandong University.

References

[1] Chen Xiaofeng, Wang Yumin. The research status and development of electronical auction.. Academic journal of communication. 23(12):pp 73 - 81. 2002, （in Chinese）

[2] M. Franklin, and M. Reiter, The Design and Implementation of a Secure Auction Service. In Proc. IEEE Symp. on Security and Privacy (Oakland, Ca, 1995), IEEE Computer Society Press, pp. 2–14. 1995

[3] M. Kudo. Secure Electronic Sealed-bid Auction Protocol with Public Key Cryptography[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, 81(1): pp.20-27. 1998,

[4] K.Sakurai and S.Miyazaki, An anonymous electronic bid- ding protocol based on a new convertible group signature scheme, in Proceedings of the 5th Australasian Conference on Information and Privacy (ACISP 2000), pp. 385-399, 2000.

[5] K.Suzuki, K. Kobayashi, and H. Morita, “Efficient sealed-bid auction using hash chain," in Proceedings of the 3th Interna- tional Conference on Information Security and Cryptology (ICISC 2000), pp. 189-197, 2000.

[6] M. Abe, K. Suzuki .Receipt free sealed bid auction. In : Proceedings of ISC 2002. LNCS 2433 , pp 191～199. 2002.

[7] F. Brandt . Fully private aucti ons in a constant number of rounds. Proceedings of the 7th Annual Conference on Financial Cryptography (FC) ,LNCS 2742 . Berlin: Springer Verlag,: pp 223 - 238 . 2003

[8] P. Bogetoft, D.L. Christensen, I. Damgard, M. Geisler, T. Jakobsen, M. Krøigaard, J.D. Nielsen, J.B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach and T. Toft. Multi-Party Computation Goes Live. Cryptology ePrint Archive, Report 2008/068, 2008.

[9] Qin Bo, Qin Hui, Zhou Kefu, Wang Xiaofeng, Wang Yumin.The Millionaire protocol with constant round complexity. Journal of Xi’an University of Technology. Vol. 21 No. 2, pages 149~152, 2005（in Chinese）