ELECTRONIC SEALED-BID AUCTION WITH THE EFFICIENT COMMUNICATION COMPLEXITY USING TOURNAMENT OPENING-METHOD

Her, Yong-Sork
Graduate school of Information Science and Electrical Engineering, Kyushu Univ.

Ryou, Jae-Cheol
Division of Electrical and Computer Engineering, Chungnam National University

Sakurai, Kouichi
Faculty of Computer Science and Communication Engineering, Kyushu Univ.

出版情報：Proc. of Business and Information(BAI 2004). 1, 2004-02
バージョン：
権利関係：

ELECTRONIC SEALED-BID AUCTION WITH THE EFFICIENT COMMUNICATION COMPLEXITY USING TOURNAMENT OPENING-METHOD

Yong-Sork Her
Graduate school of Information Science and Electrical Engineering, Kyushu Univ., 6-10-1,Hakozaki, Higashi-ku, Fukuoka, 812—8581, Japan
ysher@itslab.csce.kyushu-u.ac.jp

Jae-Cheol Ryou
Division of Electrical and Computer Engineering, Chungnam National University 220 Gung-dong, Yusung-ku, Daejon, 305 - 764, Korea,
jcryou@home.cnu.ac.kr

Kouichi Sakurai
Faculty of Computer Science and Communication Engineering, Kyushu Univ., 6-10-1,Hakozaki, Higashi-ku, Fukuoka, 812—8581, Japan
sakurai@csce.kyushu-u.ac.jp

ABSTRACT

Recently, an electronic sealed-bid auction using cryptography techniques has been proposed. An electronic sealed-bid auction is a type of electronic auctions. The aim of an auction including an electronic sealed-bid auction is to decide the price of goods fairly. So, the decision method of the price on goods in an electronic auction is very important scheme. In this paper, we propose the electronic sealed-bid auction with efficient communication complexity using a tournament opening-method. A tournament game method is used to decide the winner in sports game. We apply a tournament game to the decision of the winning price. That is, an auctioneer plays a role as a referee, and the bidding price takes part in a tournament game. In our scheme, a tournament opening-method plays a role as mix-net anonymous channel. Our e-auction scheme can keep anonymity and security of all bidders including the winner, and get more efficient communication complexity than other schemes [OM00][AS02-2].

Keyword: Sealed-bid auction, Mix-net anonymous channel, Security, Privacy, Cryptography

1. INTRODUCTION

1) Motivation

An auction is a kind of trade for special goods which have not a fixed price. In real world, a various type auctions have been enforced for decision of price. Recently, many e-auctions using cryptography techniques have been proposed. Generally, E-auction is divided by three types. One is an English auction scheme (including Dutch auction), another is a first-price sealed-bid auction scheme, and the other is a second-price sealed-bid auction scheme. In the English auction scheme, seeing the bidding price, a bidder repeatedly places a bid in real time. After the bidding time is over, the bidding price is decided as the highest price. During bidding, all bidders can see the bidding price in the English auction. In case of a first-price sealed-bid auction, it needs only the highest price and a bidder should not know the bidding price of other bidder. The method of a second-price sealed-bid auction is the same with that of a

first-price sealed-bid auction. But, the winner in a second-price sealed-bid auction gets a good in the second highest price.
In this paper, we concentrate on the first-price sealed-bid auction scheme. In case of e-auction, it needs only one result such as the highest price or the lowest price. It should keep security on the winning price as well as loosing prices. It is very important scheme to decide the price of goods in e-auction. The scheme of the price decision has an influence on the communication and computation complexity. In this paper, we propose e-auction with efficient communication complexity using a tournament opening-method.

2) Related works

There are many schemes for sealed-bid auction. Kikuchi, Harkavy and Tygar proposed the method that deals with tie-breaking in sealed-bid auctions [KHT98]. Omote and Miyaji proposed sealed-bid action with binary trees which is emphasized efficiency and entertainment [OM00] [OM01]. Naor, Pinkas and Sumner introduced a sealed-bid auction that uses two-server auction system in order to ensure privacy and correctness [NPS 99]. Juels and Szydlo improved the scheme of [NPS99] in aspect of the amount of computation and communication [JS02]. Baudron and Stern proposed a sealed-bid auction based on circuit evaluation using homomorphic encryption [BS01]. Abe and Suzuki proposed M+1-st price auction using homomorphic encryption [AS02-1]. Lee, Kim and Ma proposed public auction with one-time registration and public verifiability [LKM01]. Abe and Suzuki [AS02] proposed the first receipt-free scheme for e-auction. Chen, Lee and Kim proposed electronic auction schemes with receipt-freeness using homomorphic encryption [CLK03].

3) Our results

Many e-auction schemes have been proposed for secure and convenient auction. The goal of e-auction is to decide the price goods. So, the scheme of the price decision is very important scheme in e-auction, because the scheme of the price decision can affect the communication and computation complexity. In case of first-price sealed-bid auction, the winner is the bidder who bids the highest price. To be efficient e-auction, it needs the efficient opening method. In this paper, we concentrate on the efficient opening method for e-auction. Also, our scheme can keep the security of the winner as well as loosing bidders. To satisfy the above scheme, we apply a tournament game to the decision of the winning price. In conclusion, our e-auction scheme has *2O(m)* in communication complexity, while [OM00] has *5O(m),* and [AS02-2] has *3O(m)+ O(b)* as Table 1. Also, the used tournament in our e-auction scheme plays a role as mix-net anonymous channel. In our e-auction scheme, an auctioneer plays a role as a referee, and the bidding price takes part in a tournament game. A bidder does not know who is a referee on his own bidding price. So, a bidder can keep anonymity and security.

Table 1 Comparison of communication complexity

	Volume
Our scheme	*2O(m)*
[OM00]	*5O(m)*
[AS02-2]	*3O(m)+ O(b)*

(*m*: the number of bidding prices, *b*: the number of bidders)

This paper is organized as follows: In Section 2, we introduce preliminaries for our e-auction scheme. We propose e-auction scheme using a tournament opening-method in Section 3. We prove security on the proposed e-auction in Section 4. We compare the communication complexity of our protocol to other schemes in Section 5. In Section 6, we conclude the paper.

2. PRELIMINARY

1) Homomorphic encryption *VS.* Tournament method

- **Homomorphic encryption for opening stage**

In this section, we explain the price decision using homomorphic encryption for e-auction. Let M_1 and M_2 denote a plaintext, and Z denotes a homomorphic encryption function, the following equation holds.

$$Z(M_1)\times Z(M_2)=Z(M_1+M_2)$$

Because homomorphic encryption has the computational easiness, it used to counting or opening of e-voting and e-auction [HS00][AS02-1][CLK03].

But, homomorphic encryption uses with ZKIP (Zero Knowledge Interactive Protocol) to confirm the security of a key or a random number. Therefore, the computation and communication complexity of e-auction based on homomorphic encryption are increased in opening stage. Table 2 shows the computational complexity of [CLK03] scheme based on homomorphic encryption.

Table 2 Computational complexity in homomorphic encryption

	Volume
One bidder	*n* encryptions and proofs
Seller	*mn* verifications and proofs
A and AI	at most *2mn* multiplications, *n* decryptions and verifications

(*n*: the number of bidding prices, *m*: the number of bidders, *A* : Auctioneers, *AI* : Auction issuer)

- **Tournament method**

Usually, a tournament method is used to decide the winner in sports game, and is a kind of binary tree structure. In case of binary tree structure, bidding points are 2^k, and then *k* is the size of the representation of bids.

In [OM00], Omote and Miyaji proposed e-auction using binary trees. But, their scheme is not a tournament method. In their scheme, a bidder generates a bid vector M_i as follows.

$$M_i=[class\ 1, class\ 2, \cdots, class\ k, ID_i]$$

The bid vector M_i consists of the value expressing 0 or 1 in each class. If the *class1* value of all bidders is 1, all bidders go to *class 2*. That is, *class 1* is a tie. The number of bidding price does not decrease in *class 1*. But our scheme using a tournament method is different from [OM00]. In each class of binary trees, an auctioneer compares with bidding prices. So, the number of bidding prices is decreased by half in *class 1*. Table 3 shows the computational complexity of our scheme.

Table 3 Computational complexity in our scheme

	Volume
***n* bidder**	*n* encryptions
Bidding (games)	*(n-1)* verifications(games)

opening	*1* decryption for winner

2) Requirements of sealed-bid auction

In this section, we explain the following requirements for sealed-bid auction [KHT98][OM00][LKM01].

Privacy of bid : No bid is revealed to anyone except the winner and the winning bid.

Proof of winner : Everyone can verify the winner and the winning price which are decided correctly.

Non-repudiation : The winner cannot repudiate his/her bidding at the winning price.

Accountability of bidder : Any auctioneer can verify that bidders follow a protocol to cast their bids.

Bid Security : Nobody can forge (falsify) and tap a bid.

Robustness : Even if a bidder sends an invalid bid, the auction process is unaffected.

3) Our mix-net anonymous channel by a tournament method

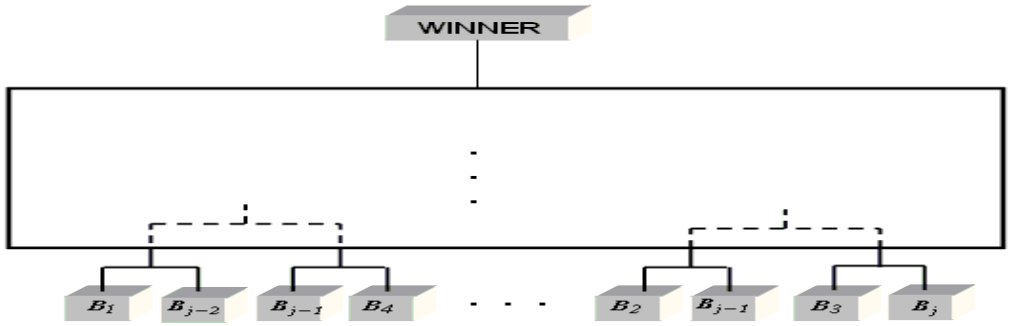


Figure 1 Anonymous channel of mix-type by a tournament method

The aim of e-auction is to decide goods as the highest price (or the lowest price). After a bidder bids, everyone does not know a flow of a tournament game. Moreover, a bidder price is mixed in the first tournament game. During a tournament game in order to decide the price, a bidder does not know the progressing of a tournament game. Also, a bidder does not know 'who is a referee on his own bidding price'. Figure 1 shows anonymous channel of mix-net type by a tournament method. After our tournament game is over, the winner is decided only by a bidding price, and the last auctioneer decrypts the encrypted bidder's ID in order to publish the winner.

3. PROTOCOL DESCRIPTION

1) Overview

There are mainly three entities in our auction as follows.

- Auctioneer (A_i): They decide the winner in each level of a tournament opening-method, and play a role as a referee.
- Bidder ($B^k{}_j$): They want to buy the special goods.
- Bulletin Board (BB): Everyone can see the content of BB and can not erase/modify it.

Figure 2 shows the tournament method of our scheme and is divided two types by the number of bidder. That is, one is that the number of bidder is an even number, and the

other is an odd number. In case of an odd number, it can be happened an unearned win. In sports games (e.g. soccer, baseball and so on) using a tournament method, the team which has an unearned win is lucky. But, it has not good luck in e-auction. In case of sports games using a tournament method, the number of game has an influence on victory or defeat. But, the number of game is not related in e-auction.

2) Proposed sealed-bid auction

■ **Notations**

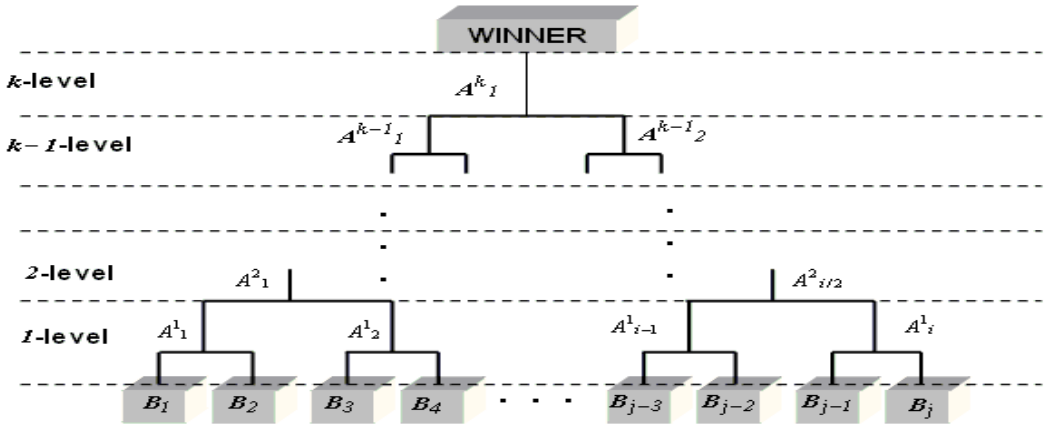
Notations are defined as follows.

- A^k_i : An auctioneer (i is the number of auctioneer, where $i = j/2$. k is a level of tournament)
- B_j : A bidder (j is the number of bidder)
- $\{p^k_i(1), q^k_i(1), d^k_i(1)\}, \{p^k_i(2), q^k_i(2), d^k_i(2)\}$: Two private-key pairs of auctioneer A^k_i
- $\{e^k_i(1), N^k_i(1)\}, \{e^k_i(2), N^k_i(2)\}$: Two public-key pairs of the auctioneer A^k_i (p^k_i, q^k_i : large random primes, $N^k_i = p^k_i q^k_i$, $\phi^k_i = (p^k_i - 1)(q^k_i - 1)$, $e^k_i d^k_i = 1 \bmod \phi^k_i$)
- p_j, q_j, d_j: Private-key of the last auctioneer A^k_1 to encrypt a bidder's ID
- e_j, N_j: Public-key of the last auctioneer A^k_1 to decrypt a bidder's ID
- r^k_i: a random number of an auctioneer A^k_i
- l_j : Bidding price of bidder B_j
- CB^k_i : The encrypted bidding price by the public key of the auctioneer A^k_i
- Z_i : The encrypted bidder's ID by the public key of the last auctioneer A^k_1
- || : Concatenation

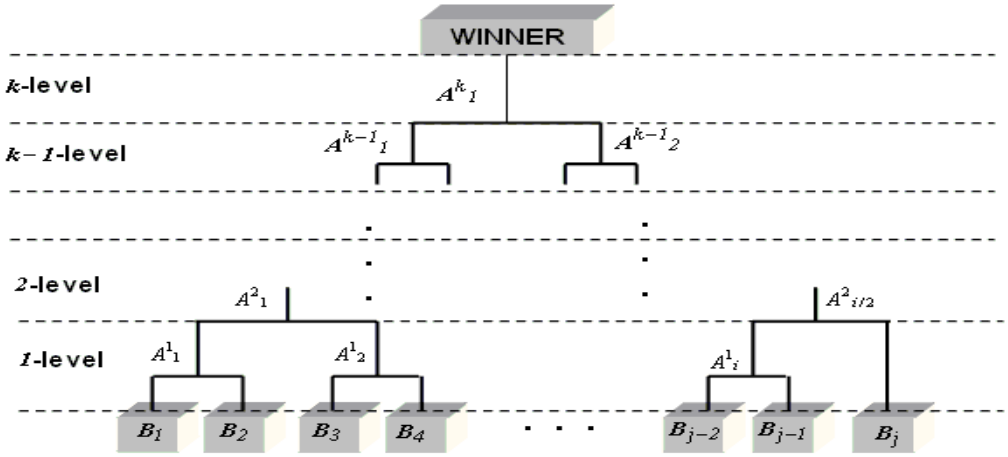
Each auctioneer has two public-key pairs and two private-key pairs because each auctioneer decides two bidding prices as following Table 4.

Table 4 ***Two public-key pairs and private-key pairs of each auctioneer.***

Auctioneer 1**-level**	**Keys**		…	**Auctioneer** k **-level**	**Keys**	
A^1_1	Private -key (1)	$p^1_1(1), q^1_1(1), d^1_1(1)$	…	A^k_1	Private -key (1)	$p^k_1(1), q^k_1(1), d^k_1(1)$
	Public -key (1)	$e^1_1(1), N^1_1(1)$	…		Public -key (1)	$e^k_1(1), N^k_1(1)$
	Private -key (2)	$p^1_1(2), q^1_1(2), d^1_1(2)$	…		Private -key (2)	$p^k_1(2), q^k_1(2), d^k_1(2)$
	Public -key (2)	$e^1_1(2), N^1_1(2)$	…		Public -key (2)	$e^k_1(2), N^k_1(2)$
…	…	…	…			
A^1_i	Private -key (1)	$p^1_i(1), q^1_i(1), d^1_i(1)$	…			
	Public -key (1)	$e^1_i(1), N^1_i(1)$	…			
	Private -key (2)	$p^1_i(2), q^1_i(2), d^1_i(2)$	…			
	Public -key (2)	$e^1_i(2), N^1_i(2)$	…			



(a) When the number of bidder is an **even number** (B_j : a bidder, A_i : an auctioneer)



(b) When the number of bidder is an **odd number** (B_j : a bidder, A_i : an auctioneer)

Figure 2 **The tournament structure of our protocol for electronic sealed-bid auction**

■ Decision of the highest price

Let $\{A^t_i \mid i = 1,2,...,a \quad and \quad t = 1,2,...,k\}$ be auctioneers and $\{B_j \mid j = 1,2,...,b\}$ be bidder. In order to make public the winner and the winning price, anyone should know the relation of the winner and the winning price. The last auctioneer A^k_1 (k-level) plays the role that publishes the winner and the winning price. Others auctioneers except the last auctioneer A^k_1 don't know the relation of the winner and the winning price during bidding. The detailed procedure is as follows.

- Bidder B_j receives public key from the last auctioneer A^k_1.
- Bidder generates one's ID ID_j and encrypts ID_j with the public key of the last auctioneer.
- Bidder decides his/her bidding price l_j.
- Auctioneer $A^1_i \{i = 1,...,a\}$ (1-level) compares each two bidding prices and decides the winner.

But, Auctioneer A^1_i (1-level) can not know bidder's ID because bidder's ID is

encrypted by the last auctioneer A^k_1 (k-level).

- Auctioneer A^1_i generates a random number r^1_i and encrypts the winner data with a random number r^1_i.
- As increasing the auctioneer's level, it is iterated such as the above procedure till k-level of A^k_1.

■ **Mix-net anonymous channel using a tournament method**

The encryption procedure of auctioneers is as follows.

- ***1-level*** : Auctioneers is from A^1_1 to A^1_i , the number of i is $j/2$, where j is the number of bidder. Each auctioneer generates two private-key pairs and public-key pairs for encrypting bidder's price.
- ***2-level*** : Auctioneers is from A^2_1 to $A^2_{i/2}$. Each auctioneer generates two private-key pairs and public-key pairs for auctioneer of ***1***-level.
- ***From 3-level to k-1 -level*** : In each level, auctioneer is decreased to 2^{k-t}. Each auctioneer in each level generates two private-key pairs and public-key pairs for auctioneers of the lower level.
- ***k -level*** : The last auctioneer A^k_1 decides the winner and the winning price.

Each bidding price should be checked by auctioneer of each level. The highest price is flown till the last auctioneer of ***k -level***. During the highest price flows, the highest price is checked ***k -time.*** That is, if one of k auctioneers is trust, nobody knows the relation of the bidder and the bidding price during bidding. This is mix-net anonymous channel.

3) Procedure

■ **Registration step**

- Bidder B_j generates one's ID ID_j.
- Bidder B_j receives the public key $<e_j, N_j>$ from the last auctioneer A^k_1 and encrypts ID_j as follows.

$$Z_j = ID_j^{e_j} \bmod N_j$$

■ **Bidding step**

- Bidder B_j decides his/her bidding price l_j

■ **Opening step**

The first game (by *1*-level auctioneers)

- Bidder B_j receives the public-key $e^1_i(1), N^1_i(1)$ of the auctioneer A^1_i.
- Bidder B_j encrypts his/her bidding price l_j as follows.

$$CB^1_i = (l_j \| Z_j)^{e^1_i(1)} \bmod N^1_i(1)$$

- Bidder B_j sends CB^1_i to Bulletin Board BB.
- Auctioneers A^1_i of *1*-level get CB^1_i from BB and decrypt CB^1_i. But, auctioneers A^1_i of *1*-level can not know the bidder's ID.
- Auctioneers A^1_i of *1*-level check the bidding price as Table 5. The boxed variable represents winners of the *l*-level game in Table 5.

Table 5 ***The checked bidding prices by auctioneers A^1_i of 1-level.***

Auctioneers of *l*-level	A^1_1		A^1_2		…	A^1_{i-1}		A^1_i	
The encrypted bidding price	l_1	$\boxed{l_2}$	$\boxed{l_3}$	l_4	…	l_{i-3}	$\boxed{l_{i-2}}$	l_{i-1}	$\boxed{l_i}$
Winners of *1*-level	l_2		l_3		…	l_{i-2}		l_i	

- For winners of *1*-level, the checked auctioneer generates a random number r^1_i.
- Auctioneer A^1_i for winners in *1*-level encrypts with r^1_i and the public-key $e^2_i(1), N^2_i(1)$ of the auctioneer $A^2_{i/2}$.

$$CB^2_i = (r^1_i \| l_j \| Z_j)^{e^2_i(1)} \bmod N^2_i(1)$$

- Auctioneer A^1_i of *1*-level sends CB^2_i to Bulletin Board BB.
- If two bidding prices (l_j, l'_j) are same, auctioneer A^1_i encrypts as follows.

$$CB^2_i = (r^1_i \| l'_j \| Z'_j \| l_j \| Z_j)^{e^2_i(1)} \bmod N^2_i(1)$$

The second game (by *2*-level auctioneers)

- Auctioneers A^2_i of *2*-level get CB^2_i from BB and decrypt CB^2_i. But, Auctioneers A^2_i of *2*-level also can not know the bidder's ID.
- Auctioneers A^2_i of *2*-level check the bidding price and decides winners as *1*-level
- For winners of *2*-level, the checked auctioneer generates a random number r^2_i.
- Auctioneer A^2_i for winners in *2*-level encrypts with r^2_i and the public-key $e^3_i(1), N^3_i(1)$ of the auctioneer A^3_i.

$$CB^3_i = (r^2_i \| l_j \| Z_j)^{e^3_i(1)} \bmod N^3_i(1)$$

- Auctioneer A^2_i of *2*-level sends CB^3_i to Bulletin Board BB.

From 3-level to k-1 -level (by *3*-level - *k-1* -level auctioneers)

- Auctioneers $(A^3_i - A^{k-1}_i)$ from *3*-level to *k-1* –level compute as the first and the second games.

The last game (by *k* –level auctioneer)

- The last auctioneer A^k_1 decides the highest price, and decrypt Z_j
- The last auctioneer announces the winner and the winning price.

4. SECURITY ON THE PROPOSED E-AUCTION

Our scheme satisfies the following requirements for electronic sealed-bid auction.
Privacy of bid : Our scheme provides mix-net anonymous channel using a tournament. Mix-net anonymous channel provides the privacy of bid. A bidder does not know that his/her own bidding price is lost in any bidding point. Also, if one of participating auctioneers is trust, our scheme provides privacy which nobody knows the relation of the winner and the winning price.
Proof of winner : During bidding, auctioneers except the last auctioneer can not know a bidder's ID, because bidder's ID is encrypted by the public-key $<e_j, N_j>$ of the last auctioneer. For proof of winner, the participated auctioneers can verify their

random numbers. Moreover, to prevent the cheated bidding price by the last auctioneer, auctioneers which take part in games of the winner can verify whether the highest price is changed or not.

Non-repudiation : The bidding price is encrypted by all auctioneers. The encrypted bidding price is sent to bulletin board. If a bidder denies one's bidding price, we can confirm the bidding price from the encrypted bidding price of bulletin board. More-over, to prevent the fabrication of the bidding price by participated auctioneers, we can verify the bidding price using the encrypted bidding price by the participated auctioneers.

Accountability of bidder : Each auctioneer know two bidding prices that take part in tournament game. After the bidding time is over, a bidder can verify his/her own game.

Bid security : It keeps bid security by the participating auctioneers using tournament opening-method.

Robustness : Even if a bidder sends an invalid bid, our auction process is unaffected.

5. COMMUNICATION COMPLEXITY

Table 6 shows communication complexities of [OM00], [AS02-2] and our scheme. The number of auctioneers A_i, bidders B_j and bidding prices is *a*, *b*, *m* respectively. Also, the number of center and bulletin board is each 1. $\leftrightarrow$ means both-direction communication, $\rightarrow$ means one-way direction., and $B_j \Rightarrow A_i$ means the one-way untappable channel from B_j *to* A_i.

Table 6 ***The communication complexity***

	Phase	Pattern	Round	Volume
[OM00]	Bidding (a random number)	$B_j \rightarrow C$	*b*	*O(m)*
	Bidding (a bid)	$B_j \rightarrow C$	*b*	*O(m)*
	Bidding (a bid vector)	$B_j \rightarrow C$	*b*	*O(m)*
	Opening (key)	$B_j \rightarrow C$	*b*	*O(m)*
	Opening (price)	$B_j \rightarrow C$	*b*	*O(m)*
[AS02-2]	Bidding (commit)	$B_j \rightarrow BB$	*b*	*O(m)*
	Bidding (Proof)	$B_j, A_i \leftrightarrow BB$	*3b*	*O(m)*
	Bidding (Secret Share)	$B_j \Rightarrow A_i$	$b \times a$	*O(m)*
	Opening	$A_i \leftrightarrow BB$	$a \times m$	*O(b)*
Our scheme	Registration (ID)	$B_j \rightarrow A_i$	*b*	*O(m)*
	Bidding/Opening	$B_j \rightarrow BB$	$b \times (b/2) \times (b/4) \times \ldots$	*O(m)*

6. CONCLUSIONS

In e-auction, it is very important how to use the price decision for the winner. The problem of the price decision has an influence on efficiency of communication and computation complexity in e-auction. In this paper, we concentrate on the efficiency of e-auction in aspect of communication and computation complexity. For efficiency of e-auction, we use tournament opening–method. Also, the tournament opening-method can play a role as mix-net anonymous channel. So, our scheme can keep anonymity and security on the winner as well as loosing bidders. Moreover, the used tournament opening-method contributes to be decreased the computation and communication complexity.

ACKNOWLEDGEMENT

The first author was partly supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Head of Researchers : Prof. Hiroto Yasuura, System LSI Research center, Kyushu University) of the Ministry of Education, Science and Culture (MEXT) and by the 21st Century COE Program 'Reconstruction of Social Infrastructure Related to Information Science and Electrical Engineering'. Also, this paper was studied by the Core University Program (Sponsors: Japan Society for the Promotion of Science, and Korea Science and Engineering Foundation).

REFERENCES

[KHT98] H.Kikuchi, M.Harkavy and J.D.Tygar, "Multi-round Anonymous Auction Protocols", Proceeding of Third USENIX Workshop on Electronic Commerce, pp61-74, 1998

[NPS99] M.Naor, B.Pinkas and R.Summer, "Privacy Preserving Auctions and Mechanism Design", Proceeding of ACM conference of E-commerce, pp129-139, 1999

[OM00] K.Omote and A.Miyaji, "An anonymous auction protocol with a single non-trusted center binary trees", Information security workshop-Proc. of ISW2000, LNCS 1975, Springer-Verlag, pp108-120, 2000

[LKM01] B.C.Lee, K.J.Kim and J.S.Ma, "Efficient Public Auction with One-Time Registration and Public Verifiability", Indocrypt 2001.

[OM01] K.Omote and A.Miyaji, "An Anonymous Sealed-bid Auction with a Feature of Entertainment", Transactions of Information Processing Society of Japan, Vol.42, No.8, Aug. 2001

[BS01] O.Baudron and J.Stern, "Non-interactive Private Auctions", Proc. of Financial Cryptography 2001, 2001

[AS02-1] M.Abe and K.Suzuki, "M+1-st Price Auction using Homomorphic Encryption", Proc. of Public Key Crytpography 2002, LNCS 2274, pp.115-124, 2002

[AS02-2] M.Abe and K.Suzuki, " Receipt-Free Sealed-Bid Auction", ISC2002, LNCS2433, pp191-199,2002

[Bra02] F.Brandt, "Secure and Private Auctions without Auctioneers", Technical Report FKI-245-02, Feb. 2002

[JS02] A.Juels and M.Szydlo, "A Two-Server, Sealed-Bid Aucion Protocol", Proc. of Financial Cryptography 2002, 2002

[CLK03] X.Chen, B.C.Lee and K.G.Kim, "Receipt-free Electronic Auction Schemes Using Homomorphic Encryption" The International Conference on Information Security and Cryptology 2003, pp 275- 290, 2003