Privacy-preserving 1-n-p Negotiation protocol

Sumit Chakraborty, Sushil Kumar Sharma and Asim Kumar Pal
Fellow, MIS, Indian Institute of Management Calcutta
Miller College of Business, Ball State University
MIS, Indian Institute of Management Calcutta
{surya2004678@yahoo.co.in, ssharma@bsu.edu, asim@iimcal.ac.in}

Abstract

In this paper, we have designed an electronic market where a buyer negotiates with n suppliers to procure p types of items within a given time frame. A privacy preserving 1-n-p negotiation protocol has been developed based on secure group communication and secure multiparty computation. The suppliers submit their bids. The objective is to label the bids as winning or losing so as to minimize the buyer's cost with the constraint that the buyer obtains all items in required quantity. The negotiation process has two distinct phases – Pre-bid and Final bid. During pre-bid phase, the suppliers singly or jointly bid for a combination of items. The privacy requirements considered are: a) Pre-bid: forward and backward privacy and anonymity of the winner in each pre-bid cycle. b) Final bid: anonymity of the losers and traceability of the winners.

1.0 Introduction

The rapid expansion of global market, the explosive growth of information and communication technologies, aggressive competition and the changing economic and social conditions have triggered tremendous opportunity to conduct business electronically. Electronic market operations like e-auctions, e-negotiations and e-procurement have become common business transactions today. However, lack of privacy and trust in coordination mechanisms is one of the most serious threats for digital business. The sharing of information is important for efficient coordination of operational processes in the e-market. But, the agents operating in the electronic market are often reluctant to disclose sensitive strategic information since the information can be revealed to the competitors. Privacy is a critical issue for multi-party negotiation in electronic market where a group of decision-making agents try to reach an agreement by disclosing minimum possible information [10]. The research in this field has focused on various aspects of e-market: coordination mechanisms, economic modeling, buyer-seller behavior, the preservation of privacy, winner determination maximizing revenue and efficiency, payment determination, dynamic pricing strategy, information flow and bidding languages [7].

Negotiation is a means through which a group of decision-making agents communicate and compromise and try to reach a mutually beneficial agreement in the electronic market. The agents exchange information in the form of offers, counter-offers and arguments and search for a consensus. Auction is a form of price negotiation that enables efficient allocation of resources in the electronic market [2]. Negotiation can take a more complex form as combinatorial auction and combinatorial reverse auction wherein the main challenge is to determine the winning bid. Combinatorial auction is an event wherein multiple goods are available and bidders can submit bids for bundles of the goods [16]. This typically requires the solution of one or more difficult optimization problems.

Let us consider the case of online combinatorial reverse auction in an electronic market wherein the suppliers bid instead of the buyers and prices are bid down instead of up. There are two types of online reverse auctions – *sealed bid* and *open bid*. Jap addressed some critical issues of online reverse auction [13]. In sealed bid auction, the suppliers reveal their bottom line bids. In open-bid reverse auction, the suppliers bid sequentially and can view their competitors' bids and respond in real time. Sealed bid reverse auctions have no price visibility. Open bid reverse auctions have full price visibility for the bidders. But, The dynamic bidding process and the fast response to competitor's bids creates pressure on the suppliers. Open bid reverse auctions may generate more cost savings and appear more opportunistic to the buyers. But**,** the strategic private information of the suppliers is disclosed to their competitors; the suppliers are often reluctant to share such critical information in competitive market. Advanced negotiation protocols should overcome these limitations of electronic market. Privacy is a crucial factor for the design of electronic market. There are many works on the design of privacy preserving auctions protocols such as one-sided auction including English auction, Vickrey auction, sealed bid auction [5,11], double auction [8], multi-unit auctions

1530-1605/08 $25.00 © 2008 IEEE

[6] and combinatorial auction [12]. However, not much research has been pursued regarding the privacy issues of reverse auction. In this paper, we have designed a model of electronic market where a buyer negotiates with n suppliers to procure p types of items within a given time frame. A privacy preserving 1-n-p negotiation protocol has been developed based on secure group communication and secure multiparty computation. The paper is organized as follows. Section 2 describes the model of an electronic market. Section 2.1 presents the privacy model. Section 3 describes the 1-n-p negotiation protocol. Section 4 presents the key management protocols for secure group communication alongwith an example. Section 5 discusses the secure computation for winner determination. Section 6 describes open issues and concludes the paper.

2.0 A model of electronic market

Let us consider following model of an e-market.

- A group of suppliers: S_1, $S_2 \ldots S_9$; S_1 and S_2 merge together.
- A set of resource to be procured by a buyer B : i_1,i_2,i_3
- A set of bundle: (i_1,i_2), (i_1,i_2,i_3) and (i_3).
- A set of subgroups of the suppliers for the first negotiation cycle: $sg_1(S_1, S_2, S_3)$, $sg_2(S_4, S_5, S_6)$ and sg_3 (S_7,S_8,S_9); these three subgroups are competing over the item sets (i_1,i_2), (i_1,i_2,i_3) and (i_3) respectively.
- A set of winners for the first prebidding cycle: S_3,S_6, S_8 over the item sets (i_1,i_2), (i_1,i_2,i_3) and (i_3).
- The buyer (B) is responsible for group access control and key management. In particular, B securely distributes keys to the group of the suppliers for secure group communication and maintains the user-key relation. $K_{1\text{-}9}$ is the group key (K_g) shared by all the suppliers. B can send common private message to all the suppliers of the group encrypting the message with this group key.
- K_{123}, K_{456}, K_{789} are subgroup keys of the sub groups sg_1 (S_1,S_2,S_3), sg_2 (S_4,S_5,S_6) and sg_3 (S_7,S_8,S_9) respectively. B can send a private message (e.g. the best offer for a specific bundle) to a subgroup encrypting with the relevant subgroup key. The privacy of a subgroup is protected through subgroup key.
- $K_1, \ldots, K_9$ are individual keys of the suppliers $S_1,S_2,\ldots,S_9$ respectively. B sends a private message to a supplier by encrypting the individual key. The distribution of symmetric keys for secure group communication is shown in figure 1.

2.1 Privacy

In this section, we have proposed a privacy model for the e-market. A supplier does not want that its bidding information is disclosed to other suppliers. Even, the buyer should not know the bid of the losing suppliers. On the other side, the buyer does not want to reveal its optimal total procurement cost (for the entire set of items) to the suppliers. Thus, privacy is an important issue for both sides : the buyer and the suppliers. The negotiation process has two phases - Prebid and final bid [15].

Prebid phase : *Anonymity* is an important issue for prebidding phase. Nobody should be able to identify a bidder from a bid. Even, the buyer should not be able to identify the winners of any prebidding cycle. The privacy of the losing suppliers should be preserved in the same way. The value of winning prebid of minimum cost for each subgroup should be disclosed to the members of that particular subgroup only by the buyer. This critical information should not be disclosed to other subgroups. Privacy should be ensured at three different levels of communication – individual, subgroup and group. To ensure *backward* and *forward privacy*, a new member of a subgroup / group should not be able to decrypt the earlier communication and a leaving member should not be allowed to decrypt the future communication. The shared keys must be updated for every change of membership and redistributed to all authorized members of a subgroup in time. A supplier should not be able to submit prebid as part of more than one subgroups at a time. A supplier can participate in more than one subgroups; submit bids; get the information of pattern of bidding and can utilize this knowledge of bidding pattern in future negotiation processes. The information is strategic for both the buyer and the suppliers. So, the buyer imposes restrictions on the bidding process of a supplier through forward and backward privacy; the supplier cannot control the price of several subgroups simultaneously. Similarly, a supplier should not be able to access information on bids for more than one subgroups at a time.

Final bid phase : Traceability of the winning bids corresponding to the optimal path and a*nonymity* of the losing bids are the key privacy issues of final bidding phase. In other words, the buyer should be able to trace the winning suppliers correctly. The only information that should be disclosed is the information required to carry out the transactions i.e. the winning bidders and the buyer should learn the selling prices and the buyer should be able to trace the winner's identity. The privacy of the optimal combinations of final winning bid is important for the buyer. The optimal cost at which the buyer procures a set of items should not be disclosed to the suppliers. On the other side, the

anonymity of the losing bids should be preserved simultaneously.

Let us consider an example [16]. A buyer requires five different types of items. The suppliers have submitted bids against 10 subgroups - {1}, {2}, {3}, {4}, {5}, {1,2}, {1,3,5}, {1,4}, {2,5} and {3,5}. These are the subgroups, which have survived the pre-bid phase. It is required to construct a search tree (Figure 2.0) on the basis of the winning final bids of these ten subgroups. The search tree has a total of seven paths, each path comprising all the items of supply. Since each path specifies a combination of bids, there will be identical number of paths irrespective of the way the search tree is constructed. The ultimate objective is to find out the optimal cost path from this tree. Let, the optimal path consists of the subgroups {1,2},{3,5}and {4} which is decided based on minimum cost of the total supply. The buyer should be able to identify the winners of these three subgroups and should know the values of corresponding final bid. On the other side, the information of the losing bids corresponding to the subgroups {1},{2},{3},{5},{1,4},{2,5} and {1,3,5} should not be disclosed to the buyer or any other supplier.

The other assumptions and requirements for are as follows :

1. All the agents involved in the negotiation process are assumed to be semi-honest.
2. An agent should be able to manage several negotiation processes concurrently. The protocol supports concurrency, which can reduce the duration of negotiation process among the agents.
3. The buyer commits its demand d_i for item i to the suppliers and cannot alter the value of its demand during the negotiation process.
4. A supplier can submit bids against all possible combinations of required items; each combination forms a subgroup of the suppliers. But, a supplier cannot submit bids for more than one subgroups at a time.

3. 1-n-p negotiation protocol

Agents: A buyer (B) and n suppliers (S). The buyer negotiates with the suppliers for p number of items.
Input : The buyer announces its requirements and each supplier submits bids.
Output: Optimum combinations of bids

---

1. The buyer announces its order proposals.
2. The buyer registers each supplier as it joins the group of all suppliers and distributes individual, subgroup and group keys. Initial subgroups of the suppliers are formed depending on the combination of items each supplier intends to supply. All the suppliers together form a group.
3. The buyer interacts with its registered suppliers, standardizes attributes of required items and calls for *prebid*.
4. *Prebid phase* : Each supplier submits a prebid. This phase consists of a number of prebid rounds. In a prebid round each supplier submits its bid for its combination of item. The buyer finds the minimum cost bid for each subgroup securely for each prebidding cycle (section 5.1). The buyer informs through multicast each member of all the subgroups the minimum cost bid for the corresponding subgroup. The suppliers can change their subgroups or merge or split or leave driven by their competitive bidding strategies and the buyer executes key management protocols accordingly for efficient secure group communication (section 4). The prebid phase terminates because of a pre-fixed time deadline. At this phase, there is no commitment from any supplier.
5. At the end of prebid phase, the winning bid of each subgroup gets preaccepted and others get prerejected. The buyer announces its expectation for each subgroup and calls for *final bid* from the suppliers. At the final bidding phase, each bid is a commitment given by the supplier. Each supplier submits *final bid* for the combination of items according to the subgroup it belonged to the last prebidding cycle. At the final bid, no supplier can change its subgroup.
6. The buyer finds out the optimum combination of winning bids using combinatorial optimization algorithm (section 5.2); sends *accept* message to the winning suppliers and *rejects* others.

4.0 Key management at prebid phase

Many emerging multi-cast based applications like 1-n-p negotiation require a secure group communication model, which ensures authenticity, confidentiality and integrity of the messages [3,14]. The combinatorial nature (i.e. p factor) demands the execution of the key management protocols following various types of strategies of bidding of the suppliers. Let us consider the case of the supplier S_5 in figure 1. When it joins the group, B distributes K_5, K_{456} and $K_{1\text{-}9}$ to S_5. Suppose, S_5 in not the winner of the subgroup (i_1,i_2,i_3) at the first prebidding cycle. Now, it has following strategic options to compete for the next bidding cycle.

Strategy 1 revise price: The first option for S_5 is to revise the previous bid for items (i_1,i_2,i_3) if possible.

Strategy 2 change of subgroup: The second strategy is to leave the old sub group, join a new sub group and submit offer against a new item set (say, i_3) without revising prebid. This new offer may be more competitive and there is a chance of S_5 to win the bid for this new item set. Suppose, S_5 departs from the old sub group sg_2 and wants to join a new subgroup sg_3. B should replace the subgroup keys K_{456} and K_{789} with K_{46} and K_{5789} respectively. Thus, S_5 can not access any future communication of the subgroup sg_2. Also, S_5 cannot access any past communication of the subgroup sg_3. The rekeying process has been shown in figure 3.

Strategy 3 Leave : If S_5 wants to regret and departs from the group (S_1–S_9), the keys K_{456} and $K_{1\text{-}9}$ should be replaced with keys K_{46} and $K'_{1\text{-}9}$ respectively. Now, B encrypts $K'_{1\text{-}9}$ with K_{123}, K_{46} and K_{789} separately; encrypts K_{46} with K_4 and K_6 separately and then multicasts these encrypted keys (figure 3).

Strategy 4 Split: Two or more suppliers merge and form a sub-group to satisfy the demand of the buyer but may fail to compete effectively as a single sub-group. In our example, S_1 and S_2 can supply items i_1 and i_2 respectively. Initially, they merge and submit a bid for a combination of items i_1 and i_2 but fail to become the winner of subgroup sg_1. So, S_1 and S_2 have decided to get splitted and form two or more new subgroups : sg_1' and sg_1''. For the next bidding cycles, S_1 and S_2 will submit bids for items i_1 and i_2 respectively. Now, the key management strategy of B should be as follows to ensure forward and backward privacy : B should generate new subgroup keys K' and K'' for the new splitted subgroups sg_1' and sg_1''. B should also generate new individual keys K_1' and K_2' for S_1 and S_2 respectively and delete old individual key K_1. If the splitted subgroups already exist, B should replace the old subgroup keys with new subgroup keys. This ensures backward privacy. Here, sg_1' and sg_1'' are two new subgroups. So, there is no requirement of replacement of old subgroup keys. B should replace old subgroup key of the merged subgroup if the subgroup is not empty. It ensures forward privacy. Since, S_3 remains the member of the subgroup sg_1 after the split of S_1 and S_2; so the old subgroup key K_{123} should be replaced with K'_{123}. B should delete the old subgroup key of merged subgroup if the subgroup is empty after the split. The subgroup sg_1 is not empty after the split of S_1 and S_2, so there is no requirement of the deletion of old subgroup key K_{123}.

Strategy 5 Merge : A supplier may not be able to satisfy the total demand of a buying agent. Two or more suppliers may merge and form a sub-group to satisfy the demand of the buyer. For example, S_3 belongs to subgroup sg_1 and S_9 belongs to subgroup sg_3. S_3 can supply items (i_1 and i_2) and S_9 can supply item i_3. Now, S_3 and S_9 have decided to merge so that they can compete and submit bids against total requirement of B i.e. items i_1,i_2 and i_3. There exists a subgroup sg_2 for this combination of items (i_1,i_2 and i_3). Now, the key management strategy of B should be as follows to ensure forward and backward privacy: B should generate new subgroup key for the merged subgroup if it is a new subgroup. In our example, sg_2 is not a new subgroup. It already exists. But, the individual keys of S_3 and S_9 should be replaced by a common individual key K_{39}B should replace old subgroup key of the merged sub-group if the sub-group already exists. Here, the old sub-group key of sg_2 i.e. K_{456} should be replaced by a new sub-group key K_{34569}. It ensures backward privacy since S_3 and S_9 will not be able to access past communications of the subgroup sg_2. B should delete old subgroup keys if the subgroups are empty after the merger. This is not applicable for our example since after merger, S_1 and S_2 belongs to sg_1 and S_7 and S_8 belongs to sg_3. B should replace old subgroup keys if the subgroups are not empty after the merger. In other words, the subgroup key of sg_1 and sg_3 i.e. K_{123} and K_{789} should be replaced by K_{12} and K_{78} respectively.

Theorem : The key management protocols preserve the forward and backward privacy at prebid phase.

Proof : In case of 1-n-p protocol, a centralized key management approach has been followed where the buyer acts as the group controller and is responsible for generation and distribution of keys, membership identification, authentication and access control.

Forward privacy: To prevent the suppliers who have already left the negotiation table from accessing future communications of a group, all keys along the path from the leaving point to the root node of the key tree should be changed. In case of a change of subgroup within a group, only old subgroup key is replaced with a new subgroup key. This ensures forward privacy.

Backward privacy: To prevent a new supplier from accessing past communications, all keys along the path from the joining point to the root node of the key tree are changed. In case of a change of subgroup within a group, only old subgroup key is replaced with a new subgroup key. This ensures backward privacy. The new member of a subgroup should not get access to corresponding past bidding history, which is strategic information of the old members of a subgroup. From the data of past bidding process, the new member may get some idea of the competitive bidding process and adjust its bid accordingly. This issue is crucial when the suppliers of a subgroup submit the final prebid and get pre-accepted message for the next bidding cycle. The new member should not get any privilege or competitive advantage. Duration of membership of a

sub-group is also an important factor. The buyer imposes restrictions on the bidding process of a supplier through forward and backward privacy; the supplier cannot control the price of several subgroups simultaneously. Similarly, a supplier should not be able to access information on bids for more than one subgroups at a time. Thus, the key management protocols satisfy the privacy requirement of pre-bid phase.

5.0 Secure computation for winner determination

5.1 Winner determination at prebid phase

For 1-n-p negotiation problem, the suppliers submit their bids at prebid phase alongwith its subgroup key. The buyer correlates each bid to a specific subgroup through the subgroup key; computes the minimum cost bid of each subgroup for each prebidding cycle without knowing any individual bid value and informs the winning bid value to the suppliers of each sub-group through multi-cast. So, it is required to execute private minimum estimation protocol for each subgroup for each prebidding cycle. The following section describes a privacy preserving minimum estimation protocol based on the concept of mixnet.
Agents: A group of DMAs and Bob.
Input : Each DMA_i holds a value v_i.
Output: Bob finds out the minimum value without revealing individual value.

---

1. Bob generates a public key (K) and sends it to all DMAs. It does not disclose the private decryption key.
2. Each DMA computes and sends $E_k(v_i)$ to a mixnet.
3. The mixnet shuffles the encrypted messages so that the DMA-value relationship is lost and sends the shuffled messages to Bob.
4. Bob finds the minimum of values.

A mixnet consists of multiple independent mix-servers and enables a group of senders to send their messages anonymously [1,4]. In step 3, a mixnet protocol should be used for the shuffling of encrypted messages [9]. The DMA-value relationship is lost by the mixing service. So, Bob cannot identify the original owner of a value. On the other side, each value is encrypted with the encryption key of Bob. So, the mixnet servers cannot get the idea of any values. There is risk of disclosure if Bob colludes with all the mixnet servers and all the servers behave dishonestly.

5.2 Winner determination at final bid

Agents : A group of suppliers and the buyer.
Input: Each supplier submits its final bid (b^f_i).
Output: The optimal combination of winning final bids, which minimize the procurement cost of the buyers subject to the constraint that the buyer gets each item of desired quantity.

---

1. The buyer generates a public key (e.g. group key) and sends it to all the suppliers. It does not disclose the private decryption key.
2. Each supplier (S_i) generates a unique tag k_i ; encrypts (b^f_i., tag(k_i); k_{sg}) with the encryption key of the supplier and sends the encrypted message to a mixenet. k_{sg} is the subgroup key of S_i ; it helps the buyer to identify a bid for a specific subgroup.
3. The mixnet shuffles the encrypted messages received from all the suppliers and sends the shuffled messages to the buyer. The buyer decrypts the encrypted messages.
4. The buyer computes the minimum cost bid i.e. the winning final bid of each subgroup. Next, the buyer computes the optimum combination of final winning bids using combinatorial optimization algorithm. The buyer makes a list (L) of tags of the optimum final winning bids and sends the list to each supplier.
6. If a supplier (S_i) can identify its tag in the list (L), it reveals its final bid to the buyer and the buyer verifies this information.

Theorem: At final bidding phase, the protocol ensures *traceability* of the winning bids corresponding to the optimal path and a*nonymity* of the losing bids simultaneously.

Proof: The mixnet can not get any idea of the final bids of the suppliers since the suppliers encrypt their final bids with the group key. Only, the buyer can decrypt the messages. The mixnet shuffles the encrypted messages so that the buyer cannot identify the owner of the messages. The buyer can trace the winning suppliers through their tags. The protocol also preserves the anonymity of the losing bids since the losing suppliers do not disclose their identity to the buyer. The computational framework of final bidding phase is shown in figure 7.0. This is a two-stage computation process. At 1st stage, the winning bid of each subgroup is computed and other bids are rejected. At 2nd stage, a combinatorial optimization algorithm is applied on the winning final bids of all the subgroups in order to find out the optimal path. The bids corresponding to the optimal path are accepted and the

losing bids are rejected. The heuristic search algorithm can be applicable for winner determination [16].

Correctness is a desirable property for the computation of this phase – the winners should be determined correctly. We have assumed that the trust in determination of the winners is distributed to the buyer and the suppliers. All the agents are assumed to be semi-honest. So, they follow the protocol correctly; the suppliers submit correct bid and the buyer determines the winners correctly. All the bidders should be treated equally and all the bids should be evaluated in a fair way.

6.0 Conclusions

The communication complexity of 1-n-p negotiation protocol depends on various factors - number of bidding rounds in prebid phase, number of subgroups, number of suppliers and the key management approach for secure group communication. There are three different approaches of key management in secure group communication - centralized, decentralized and distributed [14]. In this paper, we have assumed a centralized approach wherein a single entity i.e. the buyer acts as the group controller. In decentralized approach, a set of subgroup controllers are used to manage change of membership of each subgroup. In case of distributed key management, the group key can be generated in a contributory way by all the members of a group. But, such type of interaction among the suppliers may not be feasible in 1-n-p negotiation protocol. Moreover, the buyer may not want to trust the suppliers in generation and access control of the keys. So, the decentralized and distributed approaches are not suitable for 1-n-p negotiation model. The computation and communication complexity of various types of centralized key management approaches for secure group communication are discussed in [14].

In 1–n-p negotiation protocol, a buyer selects the potential supplier strategically to minimize operational cost under the constraints that it obtains each item of required amount in time. On the other side, a supplier tries to maximize its revenue under its capacity constraints. It selects the potential buyers and submits final bids accordingly. This is a flexible mechanism wherein a supplier can get enough scope to compete efficiently before final selection/rejection. It can submit bids for all possible combinations; it can change its subgroup or merge or split during prebid phase independently and can boost its revenue. Thus, this fair exchange protocol protects individual interests of both the suppliers and the buyers. The protocol enables an agent to manage several negotiation processes in parallel and reduces the duration of negotiation process. The negotiation process has two distinct phases – prebid and final bid. The buyer and the suppliers get enough scope for the adjustment of price. The negotiation mechanism reduces the situations of decommitment of the agents. In this paper, we have considered a simple approach of key management for secure group communication. This approach may not be scalable for large dynamic group because cost increases linearly with the group size. It would be interesting to explore appropriate key management approach for large dynamic group.

References

[1] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yaoo, "Providing receipt freeness in mix-net based voting protocols", Proceedings of sixth International Conference on Information Security and Cryptology, Seoul, 2003.

[2] C. Boyd and W. Mao., "Security issues for electronic auctions", Technical report of Hewlett Packard, HPL-2000-90.

[3] C.K. Wong, M. Gouda and S.S. Lam, "Secure group communications using key graph", IEEE/ACM Transactions on Networking, 18(1), 2000.

[4] D.Chaum "Elections with unconditionally secret ballots and disruption equivalent to breaking RSA", Advances in Cryptology, Eurocrypt'88, LNCS 330, Springer, pp. 177 – 182.

[5] F. Brandt, "Fundamental aspects of privacy and deception in electronic commerce", Doctoral dissertation, Institute für Informatik der Technischen Universität München, 2003.

[6] F. Brandt and T. Snadholm, "Efficient privacy-preserving protocols for multi-unit auctions", In Proceedings of the International Conference on Financial Cryptography and Data Security (FC-05), LNCS 3570. Springer 2005.

[7] G.Anandalingam, R.W.Day and S.Raghavan, "The landscape of electronic market design" Management Science, Volume 51, No. 3, March 2006, pp. 316 –327.

[8] J. Ha, J. Zhou and S. Moon, "A robust auction protocol based on a hybrid trust model", Proceedings of ICISS'05, LNCS 3803, Springer Verlag, 2005, pp. 77-90.

[9] J. Groth, "A verifiable secret shuffle of homomorphic encryptions", Proceedings of Public Key Cryptography, LNCS 2567, Springer Verlag 2003, pp. 145 – 160.

[10] J.Kalvenes and A.Basu, "Design of robust business-to-business electronic marketplace with guaranteed privacy", Management Science, No. 11, November 2006, pp. 1721–1736.

[11] M. Naor, B. Pinkas and R. Sumner, "Privacy preserving auctions and mechanism design", First ACM conference on electronic commerce ACM Press, 1999, pp. 129 -139.

[12] M. Yokoo and K. Suzuki, "Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions", Proceedings of 1st joint International Conference on Autonomous Agents and Multi-agents Systems, Bologna, Italy, 2002.

[13] S.D. Jap, "An exploratory study of the introduction of online reverse auctions", Journal of Marketing, 2003, 67, pp. 96-107.

[14] S. Rafaeli and D. Hutchinson, "A survey of key management for secure group communication", ACM Computing surveys, 2003, 35(3), pp. 309-329.

[15] S. Aknine, S. Pinson and M.F. Shakun, "An extended multi-agent negotiation protocol", International Journal on Autonomous Agents and Multi-Agent Systems, 2002, 8(1), pp. 5-45.

[16] T. Sandholm, "Algorithm for optimal winner determination in combinatorial auctions", Artificial Intelligence, 2002, 135, pp. 1-54.

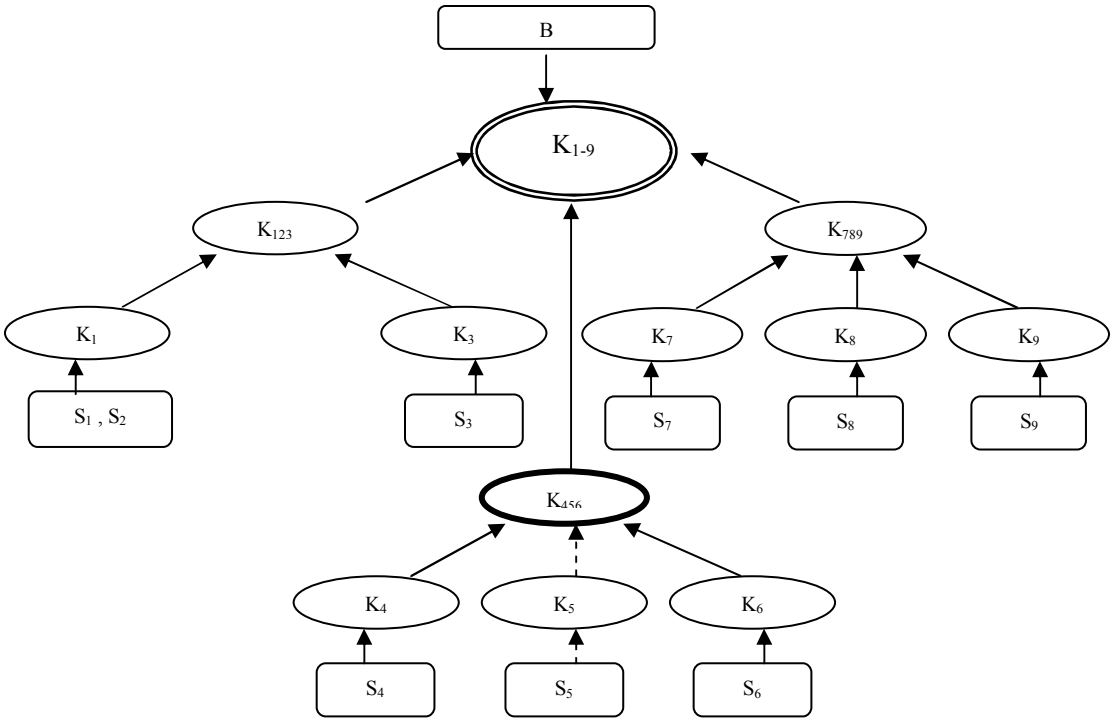

Figure 1. A model of electronic market

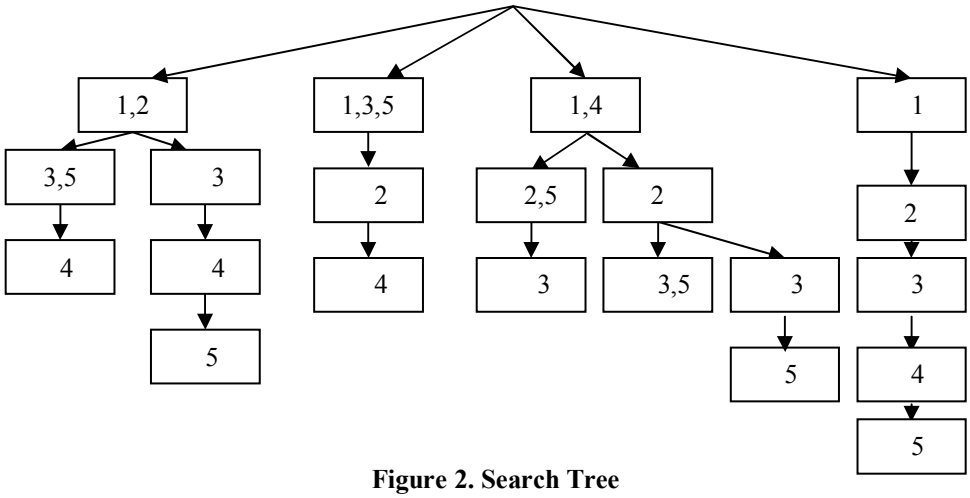

Figure 2. Search Tree

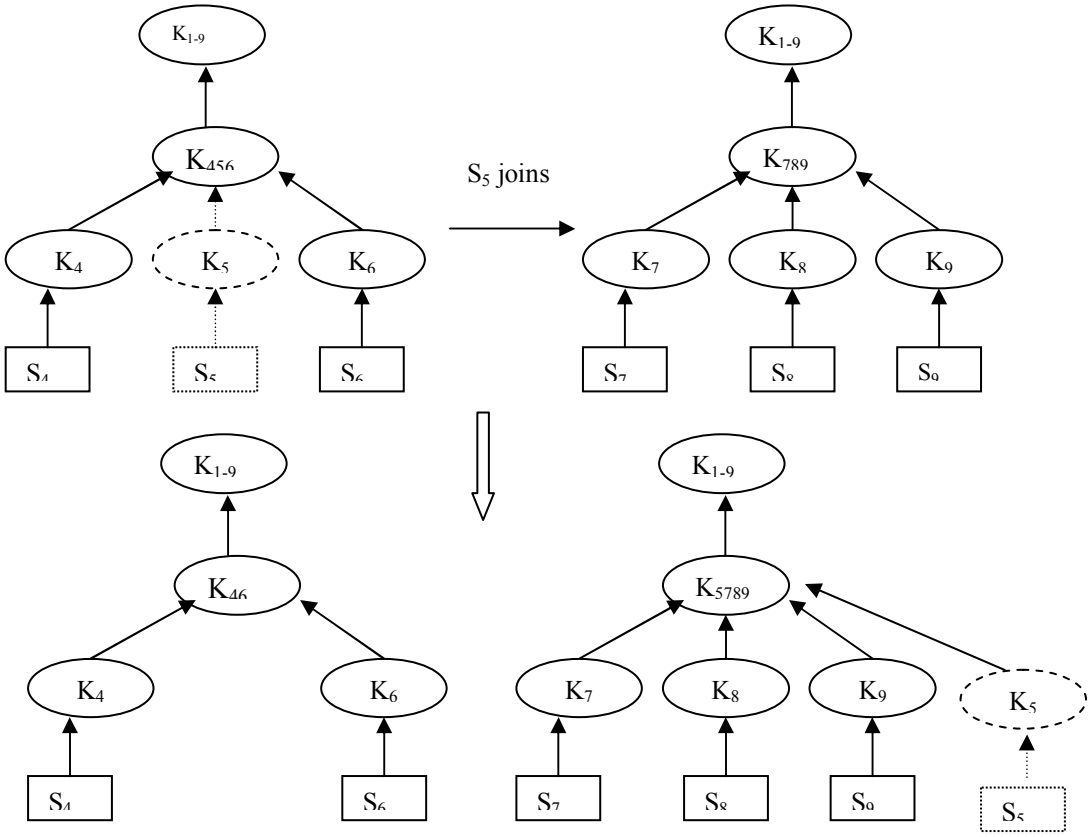

Figure 3. Change of Subgroup

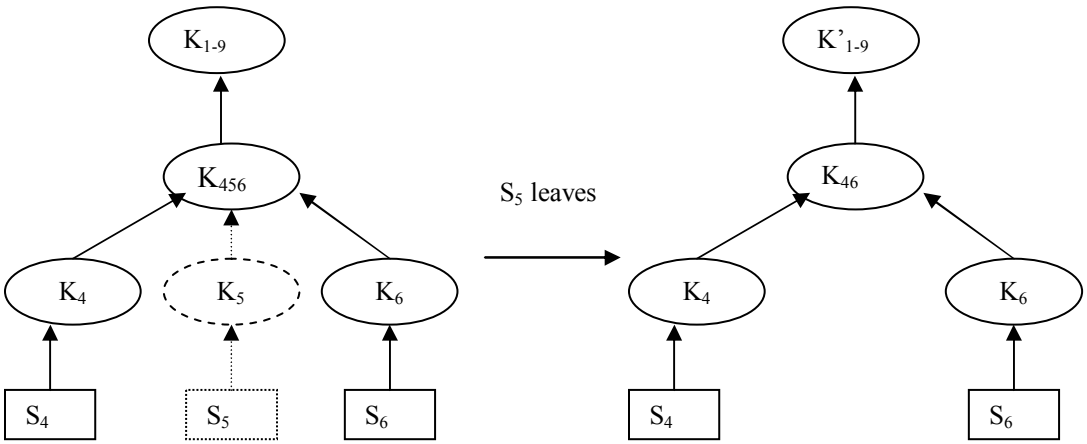

Figure 4. Key Management for leave from the group

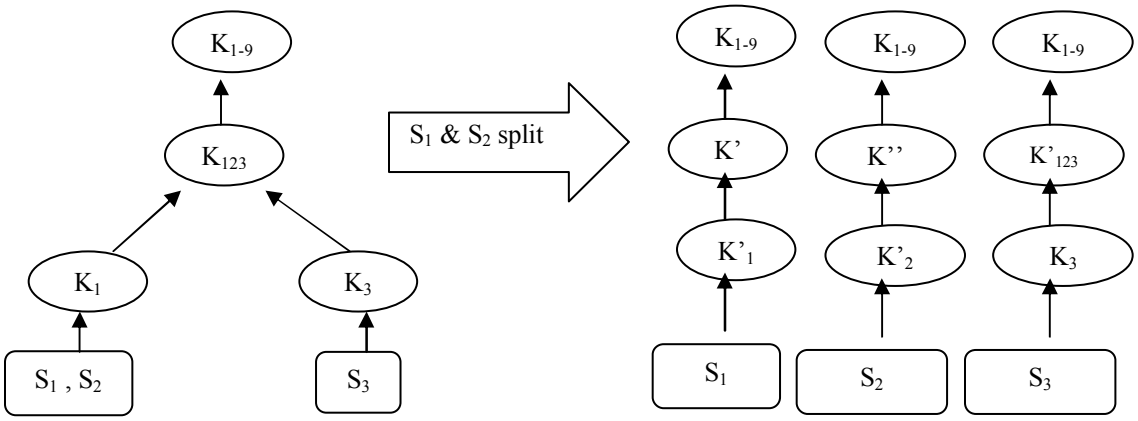

Figure 5. Key Management for Split

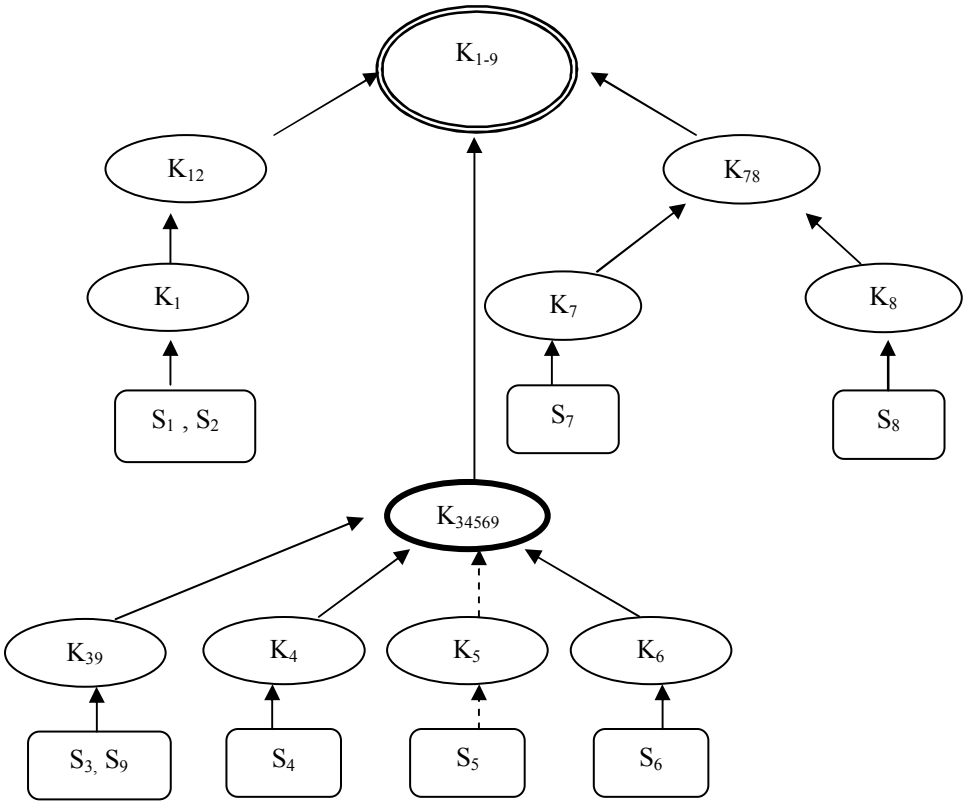

Figure 6. Key management for merger

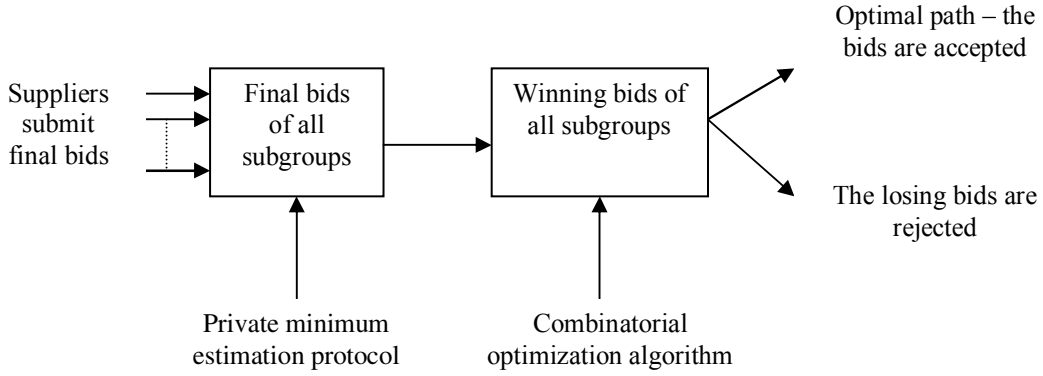

Figure 7. Computational framework for final bid