International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-4, April 2013

Modified Group Signature in Online Auction System

Aayush Agarwal, Rekha Saraswat

Abstract— Group Signature scheme allows members of a group to sign messages on behalf of the group, such that the resulting signature does not reveal the identity of the signer. Signatures can be verified with respect to a single group public key. In case of dispute, only a designated group manager, because of their special property, is able to open signatures, and thus reveal the signer's identity. Its applications are widespread used, especially in e-commerce such as e-cash, e-voting and e-auction. On the other hand, Internet is an open environment, and the unsecured environment can obstruct the development of e-commerce. Therefore, Internet must have some protocol to prevent the important message from impersonating and modifying. Recently, online auction has been receiving more and more attention in the world of electronic commerce, hence, the security and efficiency of online auction is more and more important. This paper proposes a new scheme for conducting secure and anonymous online auctions using a modified type of group signature. Our scheme solves the problems of the existing auction schemes and has following characteristics: unforgeability, anonymity, unlinkability, exculpability, coalition-resistance, verifiability, robustness, traceability, revocation, one-off registration, unskewability and unblockability. Our scheme has comparable efficiency to the existing schemes for the enhanced security and privacy it provides.

Index Terms— anonymity, authenticated encryption, E-auction, group signature.

I. INTRODUCTION

Online auctioning is now widely accepted as one of the premiere means to do business on the web. English auctions are the most common type of online auction employed by Internet auctioneers (e.g., eBay [15] and uBid [16]). Such auctions are used to sell various items from real estate to football tickets. An English auction allows one seller to offer an item for sale. Many potential buyers then submit bids for the item attempting to outbid each other. The winner is the bidder with the highest bid after a given time-out period where no bid higher than the current highest bid has been made. The winner must pay the seller an amount equal to the winning bid. Since the participants are not physically present in an online auction, there exist many security concerns and opportunities for people to cheat. For example, a bidder might repudiate having made a bid or the seller doesn't deliver the item. The timing of events in English auctions is much more critical than sealed bid auctions. As a result, this presents some unique security risks. An English auction requires a real-time link between the bidders and the Auctioneer. Frequent price quotes are issued to update bidders regarding the current highest bid. As bidders base their decisions on this information, its timeliness directly influences the auction. A corrupt Auctioneer could disadvantage certain bidders by delaying this information or by speeding up (skewing) the clock in order to close the auction early. Furthermore, the speed and ease of the bid submission process is significant, especially when an auction is nearing its end. A malicious Auctioneer could selectively block bids based on bidder identity and/or bid value.

The concept of group signatures was introduced by (Chaum and van Heyst, 1991). A group signature scheme allows members of a group to sign messages on behalf of the group, such that the resulting signature does not reveal the identity of the signer. Signatures can be verified with respect to a single group public key. Only a designated group manager is able to open signatures, and thus reveal the signer's identity [8]. Due to these unique security characteristics, group signature schemes have recently been used as the basis for auction protocols.

This paper presents a scheme for conducting online English auctions in a secure and anonymous manner. The new scheme solves the problems of the existing proposals while maintaining all of their features. In this approach, member of a group can sign a message on the behalf of the group. Then bidders who participate in auction protocol can verify the signature and post their bid. In the end of the bidding process, the winner is announced who the highest has bid. In case of any discrepancy, the group manager identifies that who has signed the message. But there is also an option for bidders to identify that cheated member as group manager can also cheat. Bidders can identify in only that case if the number of bidders are more than half to agree to reveal the identity.

The paper is organized as follows:

- Section 2 describes the fundamental and security issues of online English auctions.
- Section 3 describes the component of our scheme.
- Section 4 describes the auction protocol.
- Section 5 describes the informal security analysis of this scheme.
- Section 6 describes the efficiency of this new procedure.
- Section 7 describes some concluding remarks.

II. FUNDAMENTALS OF ONLINE AUCTIONS

There are four main activities in online English auction:

Initialization – The Auctioneer sets up the auction and advertises it i.e., type of good being auctioned, starting time, etc.

Registration – In order to participate in the auction, bidders must first register with the Auctioneer.

Bidding – A registered bidder computes his/her bid and submits it to the Auctioneer. The Auctioneer checks the bid received to ensure that it conforms to the auction rules.

Manuscript published on 30 April 2013.
* Correspondence Author (s)
Aayush Agarwal*, Information Technology, CDAC, Noida, India.
Rekha Saraswat, Computer Applications, CDAC, Noida, India.

Winner Determination – The Auctioneer determines the winner according to the auction rules.

1. ***Expiration Time*** - The auction closes at a predetermined expiration time.
2. ***Timeout*** - The auction closes when no bids higher than the current highest bid are made within a predetermined timeout interval.
3. ***Combination of Expiration and Timeout*** - The auction closes when there is a timeout after the expiration time.

III. SECURITY ISSUES IN ONLINE AUCTIONS

The core security requirements for an English auction include:

Unforgeability – Only valid group members are able to sign the message on behalf of the group.

Verifiability - There must be publicly available information by which all parties can be verified as having correctly followed the auction protocol. This should include evidence of registration, bidding and proof of the winner of the auction.

Exculpability - Neither the Auctioneer nor a legitimate bidder can forge a valid signature of an auctioneer or group member.

Coalition-resistance - No coalition of bidders can frame an innocent bidder by fabricating a bid.

Robustness - The auction process must not be affected by invalid bids or by participants not following the correct auction protocol.

Anonymity - The bidder-bid relationship must be concealed so that no bidder can be associated or identified with the bid they submit.

One-time registration - Registration is a one-off procedure, which means that once a bidder has registered, they can participate in future auctions held by the Auctioneer.

Unlinkability – Deciding whether two different valid signatures were computed by the same group member is computationally hard.

Traceability - Once a bidder has submitted a bid, they must not be able to repudiate having made it. Otherwise if a bidder wins and does not want to pay, they might deny that they submitted the winning bid. In this event the identity of the bidder who submitted the bid in question can be revealed.

Same for the auctioneer, if they block the bids or speed up the clock, then they also been identified by the group manager.

Revocation - Malicious auctioneer can be easily revoked from all future auctions.

English auctions are open bid and the timely nature of the auction process therefore raises several further concerns. Due to the flexibility of closing rules for English auctions this introduces the following unique requirements:

Unskewability - The Auctioneer must not be able to alter the auction timing. For example, speed up its clock in an attempt to close the auction early, or slow the auction down to keep the bidding process active beyond the official timeout.

Unblockability - The Auctioneer cannot selectively block bids based on bid amount or the identity of the bidder.

Conditional bid cancellation - In online auctions using an expiration time, it is common for the auction to continue for days or weeks. In this situation a bidder might be reluctant to make such an open ended bid. Therefore depending on the closing rule and the stage of the auction it is desirable to allow bidders to conditionally cancel bids. Note that bidders should not be able to cancel bids when an auction is in a timeout stage and cancellation must only be done in strict accordance with the Auctioneer's bid cancellation policy [17].

IV. COMPONENT OF OUR SCHEME

The auction has three parties:

A ***Bidder***, who is interested in buying an item from a seller in an English auction,

A ***Group Member*** **(GM)**, who organizes the auction proceedings, accepts bids and determines the winner according to whoever has submitted the highest bid. To participate in an auction, a bidder presents his/her real identity to GM. GM issues the bidder with a token that allows him/her to register.

An ***Auction Manager*** **(AM),** who are responsible for the registration of all group member, providing the membership certificate and helps in revealing the identity of the group member who has signed the message.

V. GROUP SIGNATURES

All the group members must register themselves to an auction manager and got his/her membership certificate. Then they are able to sign the message for bidding process using group signature.

All the bidders, who want to participate in an auction process can verify the signature whether it comes from right source.

To join an auction, a bidder must first register with GM (who plays the role of a group member in a group signature scheme). Once registered, a bidder can participate in the auction by applying their bids.

After the closing of bidding process, the winner is announced based on the highest bid.

In case, when bidders feel that some discrepancy had happen in the bidding process as group member does not update their bid or by speeding up (skewing) the clock in order to close the auction early, they request the manager to reveal the identity that who has done it. In this approach, it is also possible for the bidders to identify the identity of the signer of the message as the keys used by the group manager are transferred to the bidders. But this will only happens if more than half bidders are agreed to open the identity. After this, all the keys used by the group members and group managers are changed for the next auction protocol.

VI. THE AUCTION PROTOCOL

This section describes the auction protocol. A high level view of the protocol is given in Figure 1. This auction protocol is based on the Tseng and Jan scheme for group signature with some modifications. This scheme is used for online auction [11].

This approach includes five steps: initiation, signing, verification, identification and revealed by bidders.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

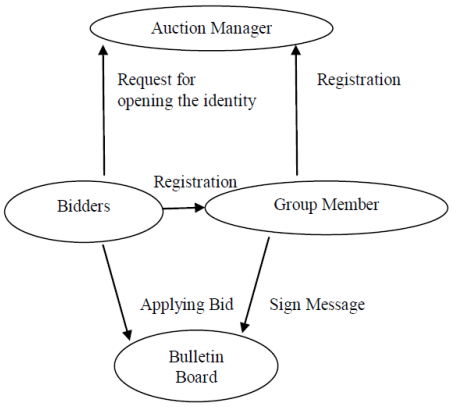

FIGURE 1. View of the Auction Protocol.

A. *Initiation Phase:*

Let p and q be large prime numbers such that q|p-1, and let g be a generator with order q in GF (p). Each group member U (i) selects the secret key x (i) and computes the public key $y_i = g^{x(i)} \bmod p$. The auction manager T has the secret key x (t) and the public key $y(t) = g^{x(t)} \bmod p$. For each group member U (i), the auction manager randomly chooses an integer k (i) in Z^*_q and compute $r(i) = g^{-k(i)}.y(i)^{k(i)} \bmod p$ and $s(i) = k(i)-r(i).x(t) \bmod q$. Then auction manager sends (r (i), s (i)) to the group member U (i) secretly. After receiving (r (i), s (i)), U (i) may verify the validity by checking the equation $g^{s(i)}.y(t)^{r(i)}.r(i) = (g^{s(i)}.y(t)^{r(i)})^{x(i)} \bmod p$.

B. *Signing Phase:*

U (i) wants to sign message m, first, U (i) selects two random numbers a and b in Z*q and computes {A,B,C,D,E} using (r (i), s (i)) as:

$A = r(i)^a \bmod p$,
$B = s(i)-b \bmod q$,
$C = r(i).a \bmod q, r_i s_i$
$D = g^a \bmod p$ and
$E = g^{a.b} \bmod p$

Secondly, U (i) chooses a random number t and computes $k(i) = D^B.y(t)^C.E \bmod p$ and $R = k(i)^t \bmod p$. Then, U (i) solves the congruence relation $h(m) = R.x(i) + t.S \bmod q$ for S. The group signature for message m is {R, S, h (m), A, B, C, D, E}. This message is the advertisement of the auction protocol mentioning price of the product, starting time, ending time etc.

C. *Verification Phase:*

Any bidder can verify the group signature by using the following steps:

1. Compute $k(i) = D^B.y(t)^C.E \bmod p$,
2. Compute $DH(i) = k(i).A \bmod p$ and
3. Check the congruence relation $k(i)^{h(m)} = DH(i)^R.R^S \bmod p$.

If the above relation holds, then the signature is valid. Now the bidders participate in the bidding process can apply their bid according to the rules. For this, bidders must register themselves to the group member who start that bidding process by giving their details and based on that bidders got their ID's.

D. *Identification Phase:*

In this phase, the bidder who has the highest bid announced as the winner and has to pay the money as the bid. If they repudiate that he/she has not apply the bid, group member will identify based on their details saved in the group member accounts.

E. *Revealing Phase:*

In the case of dispute (group member did not update the bid or skewing up the clock), the signature must be opened to reveal the identity of the signer. Because the auction manager has access to the (r (i), s (i), k (i)) of each member U (i), the auction manager can acquire the (r (i), s (i), k (i)) of U (i) satisfying the equation $D^B.y(t)^C.E = D^{k(i)} \bmod p$ for i=1 to n, where n is the number of group members. So the auction manager can determine the signer.

There is also a possibility for bidders to identify the identity of the signer that has signed the message if they thought that manager can also cheat. In this case, bidders must vote for their revealing request and if more than half votes are added, then (r (i), s (i), k (i)) will provided to the bidders and by $D^B.y(t)^C.E = D^{k(i)} \bmod p$ equation, they will able to identify. After this, secret and public keys of the group member and auction manager will change so that in future nobody can reveal without permission.

VII. SECURITY ANALYSIS AND EFFICIENCY

This section provides an informal security analysis of the online English auction scheme presented in this paper based on the characteristics described in Section 2.

Unforgeability - Only group members that are members of the group are able to sign messages on behalf of the group. This is due to the unforgeability of the underlying group signature.

Anonymity – No bidder can identify that who has submit the bid as only the bid are shown to everyone. So the bidder-bid is concealed.

Unlinkability – Deciding if two signatures {R, S, h (m), A, B, C, D, E} and {R', S', h (m)', A', B', C', D', E'} were generated by the same group member is not possible.

Exculpability - Neither a bidder nor the member of the other group, can sign on behalf of the valid group member. This is because the secret key x (i), associated to user i is computationally hidden from all others.

Verifiability - All bids (including signatures) are posted to the public bulletin, therefore all parties can verify the auction outcome.

Robustness - Invalid bids will not be posted to the bulletin board. Moreover, malicious bidders will be revoked from the system, and thus cannot affect the auction outcome.

Traceability – Auction Manager is always able to open a valid signature and, identify the signer of the bid.

Revocation - Bidders can be easily revoked from the future auctions if they have broken the auction rules.

One-time registration - Once a bidder has received a identity, they are free to participate in future auctions.

Unskewability - The Auctioneer is not being able to alter the auction timing as if bidders feel that there is some problem with the timing process, they are able to request to reveal the identity of the signer.

Unblockability - A bidder must submit his/her bids to group member, who post the bid on the bulletin board. If they tries to block a bid, then there bid will not be posted to the bulletin board which will indicate that something happens wrong. In this case bidder will request for identify the group member or vote for them.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Conditional bid cancellation - Bidders can conditionally cancel bids by sending a CANCEL message to group member as long as the auction is not in a timeout stage.

VIII. EFFICIENCY

This section discusses the efficiency considerations of the new scheme. First of all our scheme has an enhanced set of security requirements that are much more comprehensive. Furthermore, our scheme clearly has the most efficient revocation method. In addition, we have the most practical one-time registration procedure. We include the procedure that third party (verifier) can also identify the signer of the message by the keys used by the auction manager. In this case after revealing the identity, all the keys of auction manager and group member will be changed. This provides the extra security as there is no chance to cheat for group member or auction manager.

IX. CONCLUSIONS

This paper presented a scheme for conducting secure and anonymous online English auctions. Such a scheme is vital for protecting the security and anonymity of participants who engage in online auctioning. The timeliness of information and verifiability of the Auctioneer's actions is critical in an online English auction. We have shown that the existing "secure" English auction schemes are inadequate for the task. In direct contrast, our scheme solves all of the problems of the existing schemes and has a more comprehensive set of security requirements. We use a group signature to protect the identities of bidders. Bidders can also be able to identify the signer of the message. One time registration process will help the bidders to bid in the future anytime as they are given the unique ID. The scheme has comparable efficiency to the existing proposal for its enhanced security and privacy characteristics. The efficiency and security of the scheme rests with the underlying group signature scheme used. Our approach offers the client flexibility in choosing from any group signature scheme.

REFERENCES

1. D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In V. Atluri, B. Pfitz-mann, and P. D. McDaniel, editors, ACM Conference on Computer and Communications Security, ACM, 2004.
2. G.Ateniese, J.Camenisch, M.Joye, and G.Tsudik, "A Pracical and provably secure coalition-resistant group signature", in Advances in Cryptology 2000.
3. Q.L.Xu . A Modified Threshold RSA Digital Signature Scheme. Chinese Journal of Computer, 2000.
4. J. Camenisch, "Efficient and generalized group signatures", in Advances in Cryptology, EuroCrypto 1997.
5. Sun Huihui, Chen Shaozhen. An Efficient Forward Secure Group Signature Scheme With Revocation. JOURNAL OF ELECTRONICS, 2008
6. J. Camenisch and M.Stadler, "Efficient group signature scheme for large groups", in Advances in Cryptology, Crypto 1997.
7. J. Camenisch and M. Michels, "Separability and efficiency for generic group signature schemes". In M. Wiener, editor, Advances in Cryptology, CRYPTO 1999.
8. D. Chaum and E. Heyst, "Group Signatures", in Advances in Cryptology, Eurocrypt, 1991.
9. L. Chen and T.P. Pedersen, "New Group Signatures", in Advances in Cryptology, Eurocrypt 1994.
10. R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of rsa functions. In Advances in Cryptology, 1996.
11. Yuh-Min Tseng and Jinn-Ke Jan, "Improved Group Signature scheme based on discrete logarithm problem," IEE Electronics Letters, vol. 35, no. 1, pp. 37-38, 1999.
12. M.K. Franklin and M.K. Reiter, "The design and implementation of a secure auction service", IEEE Transactions on Software Engineering, 1996.
13. G. Tsudik, G. Ateniese, "Some open issues and new directions in group signatures", in Advances in Cryptology Crypto 1999.
14. G. Tsudik and G. Ateniese, "Quasi-efficient revocation of group signatures", in To Appear in Financial Cryptography, 2002.
15. www.ebay.com
16. www.ubid.com
17. Jarrod Trevathan and Wayne Read, "SECURE ONLINE ENGLISH AUCTIONS", School of Mathematical and Physical Sciences James Cook University.
18. M. Harkavy, H. Kikuch and J.D. Tygar, "Electronic auction with private commerce", in Proceedings of the 3rd USENLX Workshop on Electronic Commerce, August 1998.
19. Fangguo Zhang and Kwangjo Kim, "Security of A New Group Signature Scheme", IEEE TENCON'02
20. E. Petrank J. Kilian, "Identity Escrow", in Advances in Cryptology Crypto 1998.
21. Zulfikar Amin Ramzan, "Group Blind Digital Signatures: Theory and Applications" in Advances in Cryptology 1999.
22. Trevathan, J., Ghodosi, H. and Read, W. "Design Issues for Electronic Auctions", in *2nd International Conference on E-Business and Telecommunication Networks*, 2005.

Mr. Aayush Agarwal received his B.Tech in IT from G.B.T.U Lucknow, Uttar Pradesh, India in 2010.Currently, he is doing M.Tech in IT from C-DAC Noida(Affiliated to G.G.S.I.P.U New Delhi), India. He is working on the project **"Group Signature Scheme for Online Bidding".** His interest areas are Cryptography and Network Security, Operating Systems, and DBMS.

Ms Rekha Saraswat is a Sr. Lecturer in CDAC, Noida (Affiliated to G.G.S.I.P.U New Delhi), India. She has 10 years of expertise in the field of teaching. Her area of interests are Computer networks, Object oriented software engineering and Operating system.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)