A New English Auction Scheme Using The Bulletin Board System*

Cheng-Chi Lee[§] Min-Shiang Hwang[‡] Chih-Wei Lin[¶]

Department of Management Information Systems[‡]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

Department of Computer & Communication Engineering[§]
Asia University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.

Department of Information Management[¶]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

September 23, 2008

*Responsible for correspondence: Prof. Min-Shiang Hwang (Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C., Email: mshwang@nchu.edu.tw)

A New English Auction Scheme Using The Bulletin Board System

Abstract

The concept of group signature was first introduced by Chaum and van Heyst. They allowed individual members in a group to create signatures on behalf of the group. In this paper, we shall propose a new English auction scheme based on this concept by using the bulletin board system (BBS). The proposed scheme can satisfy the requirements of an ideal of English auction scheme as in Introduction.

Keywords: Auction, Discrete Logarithm, Group Signature, Security.

1 Introduction

A group signature scheme allows a member in the group to create a signature on the message on behalf of the group. The validity of the signature should be able to be verified, and the identity of the creator (signer) should be kept secret. Only the group manager has the authority to identify the creator.

In 1991, Chaum and van Heyst [3] introduced the concept of group signature and proposed their scheme. There are four requirements to be met in their scheme.

1. **Unforgeability:** only a group member can create a signature on the message on behalf of the group.

2. **Anonymity:** the validity of the group signature can be verified. However, nobody can reveal the identity of the signer except the group manager.

3. **Unlinkability:** no one (but the group authority) can link what two different group signature issued by the same group member.

4. **No framing:** no group member can masquerade another member to sign a message.

Chen and Pedersen [4] improved the Chaum et al. scheme and concealed the identity of the signer by using the Cramer et al.'s [20] protocol. However, in the Chen-Pederson scheme, the signer has to sign twice so that the signer identification can be done. Besides, Pedersen [19] also offered a general group signature scheme that could convert any digital signature into a group signature. So far, a wide variety of group signatures [2, 18, 19, 21] have been proposed.

Lee and Chang [15] proposed a novel group signature scheme based on the discrete logarithm [6, 8, 9]. Their scheme proves to be more efficient than those in [3, 4] in terms of communication. However, Joye et al. [11] reported that their not satisfy the requirement of unlinkability. In this paper, we shall propose a new English auction scheme based on the Lee-Chang group signature by bringing in the bulletin board system (BBS). Although the Lee-Chang group signature does not satisfy the requirement of unlinkability of the group signature, their scheme can be extend to be suitable for our new English auction scheme. The drawback of the Lee-Chang group signature cannot destroy our new English auction scheme. On the contrary, we can apply this property to our new English auction scheme.

Recently, electronic auction has been receiving more and more attention in the world of electronic commerce [1]. Electronic auction can be either sealed-bid auction or public auction. In public auction, also known as the English auction, all the bid values are clearly published, but nobody can reveal the identity of any bidder except the auctioneer. Each bidder can offer prices again and again that are higher than ever. When no more bids are called, the highest price is the winning price. Finally, the bidder who cast the winning price is the winner in this auction. However, in sealed-bid auction [5, 7, 10, 12, 13], the bid values cannot be revealed until the open stage.

An ideal of English auction procedure should satisfy the requirements in the following [14, 16, 17]:

- **Unforgeability:** Nobody can forge a valid bid and pass the verification equation.
- **Anonymity:** Nobody can identify the bidder from a bid.
- **No framing:** Nobody can masquerade a bidder to bid.
- **Traceability:** The winner cannot deny his/her winning bid after the winner decision and announcement stage.
- **Fairness:** All bidders have the same power in the auction.
- **Verifiability:** The validity of a bid can be publicly verified.
- **Unlinkability among different auctions:** When a bidder is making bids in two or more auctions, nobody can derive any bid in one auction from another bid in another auction.
- **Linkability in an auction:** Everybody knows it when some bidder has made many bids in an auction.
- **Efficiency of bidding:** The computation and communication cost is lowest.
- **One-time registration:** All bidders only have to register manager with the once before participating in the auction rounds.
- **Easy revocation:** The manager can easily revoke the power of a bidder.
- **Two independent authority's powers:** There is no single authority who can break anonymity.

Up to now, the English auction has received only limited attention. Based on Camenisch and Stadler's [2] group signature, the signature of knowledge reveals the identity of the bidder. In this paper, we shall propose a new English auction scheme to achieve the above requirements based on the Lee-Chang group signature.

This paper is organized as follows. In Section 2, we shall briefly review the Lee-Chang group signature. Then, we shall propose a new English auction scheme based on the Lee-Chang group signature in Section 3. Next, we shall analyze the English auction scheme in Section 4. Finally, the conclusion will be in Section 5.

2 Review of the Lee-Chang Scheme

In this section, we shall introduce the Lee-Chang scheme. The group signature scheme, based on the discrete logarithm problem, was proposed in 1997. The Lee-Chang scheme procedures are as follows. Let p and q be two large primes such that $q|p-1$, and let g be an element of order q in $GF(p)$.

There are four phases in this scheme: *creation of the group, signing and verification, identification of the signer* and *renewal of the signer's identity.* In the first phase, the group manager gathers a group of participants. In the second phase, only a group member can create a valid signature on behalf of the group. The phase is for the group manager to identify the signer when necessary. Finally, in the fourth phase, the group manager will give a new identify to a signer when his/her identity have been revealed.

Creation of the Group: Each user U_i chooses a private key x_i and computes the corresponding public key as $y_i \equiv g^{x_i} \bmod p$. The group manager GM has a private key x_{GM} and a public key $y_{GM} \equiv g^{x_{GM}} \bmod p$. If the user U_i wants to participate in a group, he/she has to propose a request with his/her information and y_i to group manager GM for registration. When the group manager accepts the request, he/she issues $(r_i,\, s_i)$ to the user U_i secretly.

$$\begin{aligned} r_i &\equiv g^{-k_i} DH_i \bmod p, \\ s_i &\equiv k_i - r_i x_{GM} \bmod q, \end{aligned}$$

where k_i is a random number, $\gcd(k_i, q) = 1$, and $DH_i \equiv g^{x_i k_i} \bmod p$. The user can verify $(r_i,\, s_i)$ by the verification equation:

$$g^{s_i} y_{GM}^{r_i} r_i \equiv (g^{s_i} y_{GM}^{r_i})^{x_i} \bmod p.$$

If the equation holds, then $(r_i,\, s_i)$ is valid.

Signing and Verification: When a user wants to create a signature on a message m on behalf of the group, he/she randomly chooses a number $t \in_R Z_p^*$ and computes

$$\begin{aligned} \alpha_i &= g^{s_i} y_{GM}^{r_i} \bmod p, \\ r &= \alpha_i^t \bmod p, \\ h(m) &= r x_i + t s \bmod p, \end{aligned}$$

and then publishes $(h(m),\, r,\, s,\, r_i,\, s_i)$. Everyone can verify the validity of the signature through the verification equation as follows:

$$\begin{aligned} \alpha_i &\equiv g^{s_i} y_{GM}^{r_i} \bmod p, \\ DH_i &\equiv \alpha_i r_i \bmod p, \end{aligned}$$

and check

$$\alpha_i^{h(m)} \equiv r^s DH_i^r \bmod p.$$

If the above equation holds, it is a valid signature.

Identification of the Signer: If other group members want to know the identity of the signer, they must go through the GM. First, the GM

chooses a random number $a \in_R Z_p^*$ and computes

$$\begin{aligned} r_{GM} &\equiv (gy_i)^a \bmod p, \\ s_{GM} &\equiv a - r_{GM}k_i \bmod q, \end{aligned}$$

and then sends $(r_{GM},\ s_{GM})$ to the verifier. The verifier checks it by computing

$$\begin{aligned} \beta_i &\equiv gy_i \bmod p, \\ \delta_i &\equiv \alpha_i DH_i \bmod q, \end{aligned}$$

and

$$r_{GM} \equiv \beta_i^{s_{GM}} \delta_i^{r_{GM}} \bmod p.$$

If the above equation holds, then the signer can be successfully identified.

Renewal of the Signer's Identity: The GM will secretly give a new identify $(r_i',\ s_i')$ to a group member when the old identity of the group member has been revealed. After that, the old identity $(r_i,\ s_i)$ will no longer be valid. The new pair $(r_i',\ s_i')$ is computed as follows:

$$\begin{aligned} r_i' &\equiv g^{-k_i'} DH_i' \bmod p, \\ s_i' &\equiv k_i' - r_i' x_{GM} \bmod q, \end{aligned}$$

where k_i' is a random number, $\gcd(k_i', q) = 1$, and the $DH_i' \equiv g^{x_i k_i'} \bmod p$.

3 The Proposed English Auction Scheme

In this section, we shall apply the above group signature to our new English auction scheme. The procedures of the English auction include bidder registration, bidding, and winner decision and announcement. In the above group signature, the user and the GM play the roles of the bidder and the auction manager AM, respectively. The bidder registration procedure is similar the creation of the group in the group signature, the bidding procedure is similar to the signing and the verification phase of the group signature. Finally, the procedure of winner decision and announcement is similar to the opening of the signature and the identification of the signer.

In our English auction scheme, we disperse the power of the auction manager to the registration manager RM in order for the anonymity of the bidders. Under such circumstances, only AM and RM can cooperate to identify the bidder. Note that RM or AM alone cannot identify the bidder. In our scheme, the registration manager RM knows the correspondence between a bidder's identity and the bidder's registration key. The auction manager AM creates and handles the auction.

AM and RM have private keys x_{AM} and x_{RM} as well as their corresponding public keys $y_{AM} \equiv g^{x_{AM}} \bmod p$ and $y_{RM} \equiv g^{x_{RM}} \bmod p$, respectively. The detail procedures of the new English auction scheme are as follows.

3.1 Bidder Registration

The bidder B_i randomly chooses a private key x_i and computes the corresponding public key $y_i \equiv g^{x_i} \bmod p$, and then B_i secretly sends his/her information and y_i to RM for registration. When RM accepts the registration request, he/she computes

$$Y_i \equiv (y_i)^{x_{RM}} \equiv (y_{RM})^{x_i} \bmod p$$

for all bidders, computes $Y_{RA} \equiv (y_{AM})^{x_{RM}} \bmod p$, and publishes them on RM's BBS (ie. Table 1) in a shuffled way.

Note that the BBS is a read-only site where only RM can write. In the meantime, RM maintains a database of the bidders' information as Table 2 shows.

AM gets the list of all the Y_i of n valid bidders from RM's BBS, then AM

Table 1: RM's BBS.

g, p, q, y_{RM}, Y_{RA}
Y_2
Y_1
Y_3
$\vdots$
Y_n

Table 2: The database of the bidders' information

User name	Public key	Round key
Alice	y_1	Y_1
Bob	y_2	Y_2
Coral	y_3	Y_3
$\vdots$	$\vdots$	$\vdots$

computes the auction key Y_{A_i}

$$Y_{A_i} \equiv (Y_i)^{x_{AM}} \equiv (Y_{RA})^{x_i} \bmod p,$$

where

$$Y_{RA} \equiv (y_{AM})^{x_{RM}} \equiv (y_{RM})^{x_{AM}} \bmod p,$$

for each valid bidder through the RM's public key. After that, AM computes the certificate, $(r_i,\, s_i)$, and α_i for the valid bidders and publish them on AM's BBS (see Table 3) in a shuffled way, where

$$\begin{aligned} r_i &\equiv y_{RM}^{k_i} DH_i \bmod p, \\ s_i &\equiv k_i - r_i x_{AM} \bmod q, and \\ \alpha_i &\equiv y_{RM}^{s_i} Y_{RA}^{r_i} \bmod p. \end{aligned}$$

Here, k_i is a random number, $\gcd(k_i, q) = 1$ and $DH_i \equiv (Y_i^{k_i}) \equiv (g^{x_i x_{RM}})^{k_i} \bmod p$. Note that the parameters of the valid bidders published on RM's BBS and AM's BBS can only be read. Only AM can edit them.

Table 3: AM's BBS

y_{AM}, Y_{RA}
r_3, s_3, α_3, DH_3, Y_{A_3}
r_1, s_1, α_1, DH_1, Y_{A_1}
r_2, s_2, α_2, DH_2, Y_{A_2}
$\vdots$
r_i, s_i, α_i, DH_i, Y_{A_i}
$\vdots$
r_n, s_n, α_n, DH_n, Y_{A_n}

3.2 Bidding

Suppose a bidder B_i wants to participate in this auction. B_i executes the following steps.

Step 1: The bidder computes his/her round key as

$$Y_i \equiv (y_{RM})^{x_i} \equiv (y_i)^{x_{RM}} \bmod p$$

and checks whether the round key is listed on RM's BBS. If it is not listed, he/she complains to RM.

Step 2: The bidder computes his/her auction key as

$$Y_{A_i} \equiv (g^{x_{RM}x_{AM}})^{x_i} \equiv (Y_{RA})^{x_i} \bmod p$$

and checks whether the auction key is listed on AM's BBS. If it is not listed, he/she complains to AM.

Step 3: The bidder finds own certificate $(r_i,\ s_i)$ and α_i by using his/her auction key on AM's BBS. He/she uses $(r_i,\ s_i)$ to create a signature on his/her bid m_i. He/she chooses random a number $t \in_R Z_p^*$ and computes

$$r \equiv \alpha_i^t \bmod p,$$

and find s such that

$$m_i \equiv rx_i + ts \bmod q.$$

Finally, (m_i, r, s, r_i, s_i) is a bid that can be verified by everyone.

Step 4: The verifier can check the verification equation with the knowledge of α_i and DH_i from AM's BBS.

$$\alpha_i^{m_i} \equiv r^s DH_i^r \bmod p. \quad (1)$$

3.3 Winner Decision and Announcement

Assume that B_j's bid m_j is the highest bid at the end of the bidding procedure. Here, AM and RM will cooperate to find and publish the winner B_j's identity as follows.

Step 1: AM announces that $(m_j, r, s, r_j, s_j, DH_j)$ is the winning bid.

Step 2: AM publishes k_j^{-1}, which everyone can verify to make sure whether the winning bid was from a legal bidder or not by looking into RM's BBS.

$$(DH_j)^{k_j^{-1}} \equiv Y_j \bmod p.$$

Step 3: RM shows B_j is the winner that has $y_j \equiv (Y_j)^{x_{RM}^{-1}} \bmod p$.

4 Analysis of Our English Auction Scheme

Our English auction scheme can satisfy the requirements as follows.

- **Anonymity:** In our scheme, we use RM and AM to jointly support the bidders with anonymity. RM or AM alone cannot identify the any bidder. The bidder sends *name* and y_i to RM in the registration phase. RM computes Y_i for each bidder through y_i and posts it on his/her BBS in a shuffled way. Next, AM posts (r_i, s_i) for each bidder on AM's BBS in a shuffled way. Consequently, nobody knows the identity of a bidder except RM and AM working together.

- **Traceability:** RM and AM can jointly trace the winner. So, after the winner decision and announcement stage, the winner cannot deny submitting the winning bid.

- **No framing:** In our scheme, the bidder cannot disguise as another bidder to bid because he/she cannot get the private key x_i of another bidder.

- **Unfrogeability:** In an auction, the bidder must create a legal signature on his/her bid when he/she wants to bid. Only a legal bidder can pass the verification equation because he/she has a valid private key x_i.

- **Fairness:** No bidder can deny his/her bidding because every bid has a signature on it.

- **Verifiability:** Every bidder can confirm the validity of any signature by the computing verification Equation (1).

- **Unlinkability among different auctions:** For each auction, RM and AM generate new x_{RM} and k_i for the event and each bidder, respectively, and therefore nobody can know the bids of the same bidder among different auctions.

- **Linkability in an auction:** The bidder can use $(r_i,\ s_i)$ to bid many times until he/she gets identified. Although all the bidders get to know that somebody has bid many times, they cannot know the identity of the bidder.

- **Efficiency of Bidding:** The bidder can repeatedly use his/her $(r_i,\ s_i)$ to bid until the end of this auction round. All he/she has to do is compute a signature s on the bid when he/she wants to bid in the auction.

- **One-time Registration:** Each bidder only executes the registration procedure once with RM. RM saves the identity of each bidder in the database. If the bidders want to participate in the auction, he/she can find Y_i and (r_i, s_i) on RM's BBS and AM's BBS, respectively.

- **Easy Revocation:** We can easily revoke the bidder as RM and AM respectively delete the corresponding Y_i and (r_i, s_i) on their BBS.

- **Two independent authority's powers:** Only AM and RM can cooperate to identify the bidder. That is to say, there is no single authority who can break anonymity.

Our proposed scheme applies the BBS based on the Lee-Chang group signature. In addition, our scheme can satisfy the requirements of an ideal of English auction scheme as in Introduction.

5 Conclusions

In this paper, we have proposed a new English auction scheme based on the group signature by employing the BBS. Our scheme can satisfy the requirements set up for an ideal electronic English auction.

References

[1] E. David and R. Azoulay-Schwartz and S. Kraus, "Semiparametric identification and estimation in multi-object, English auctions," *Journal of Econometrics*, vol. 141, pp. 84–108, Nov. 2007.

[2] J. Camenisch and M. Stadler, "Efficient group signature scheme for large groups," in *Advances in Cryptology, Crypto'97*, pp. 410–424, Lecture Notes in Computer Science, 1997.

[3] D. Chaum and E. Heyst, "Group signatures," in *Advances in Cryptology, Eurocrypt'91*, pp. 257–265, Lecture Notes in Computer Science, 1991.

[4] L. Chen and T. P. Pedersen, "New group signature," in *Advances in Cryptology, Eurocrypt'94*, pp. 171–181, Lecture Notes in Computer Science, 1994.

[5] E. David and R. Azoulay-Schwartz and S. Kraus, “Bidding in sealed-bid and English multi-attribute auctions,” *Decision Support Systems*, vol. 42, pp. 527–556, Nov. 2006.

[6] T. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[7] M.K Franklin and M.K.Reiter, “The design and implementation of a secure auction service,” *IEEE Transactions on Software Engineering*, vol. 22, no. 3, pp. 302–312, 1996.

[8] Min-Shiang Hwang and Ting-Yi Chang, “Threshold Signatures: Current Status and Key Issues,” *International Journal of Network Security*, vol. 1, no. 3, pp. 123–137, 2005.

[9] Min-Shiang Hwang and Cheng-Chi Lee, “Research Issues and Challenges for Multiple Digital Signatures,” *International Journal of Network Security*, vol. 1, no. 1, pp. 1–7, 2005.

[10] Min-Shiang Hwang, Eric Jui-Lin Lu, and Iuon-Chung Lin, “Adding timestamps to the secure electronic auction protocol,” *Data & Knowledge Engineering*, vol. 40, no. 2, pp. 155–162, 2002.

[11] M. Joye, Narn-Yih Lee, and Tzonelih Hwang. “On the security of the lee-chang group signature scheme and its derivatives,”. Technical Report TR-99-7, Departement of Electrical Engineering, TamKang University, 1999.

[12] Hiroaki Kikuchi, Michael Hakavy, and Doug Tygar, “Multi-round anonymous auction protocols,” *IEICE Transactions on Information and Systems*, vol. E82-D, no. 4, pp. 769–777, 1999.

[13] M. Kudo, “Secure electronic sealed-bid auction protocol with public key cryptography,” *IEICE Transactions on Fundamentals*, vol. E81-A, no. 1, pp. 20–27, 1998.

[14] B. Lee, K. Kim, and J. Ma, “Efficient public auction with one-time registration and public verifiabiltiy,” in *Proceedings of Indocrypt2001*, pp. 16–20, Madras, Chennai, India, 2001.

[15] W. B. Lee and C. C. Chang, "Efficient group signature scheme based on the discrete logarithm," *IEE Proceedings - Computer Digital Technology*, vol. 145, no. 1, pp. 15–18, 1998.

[16] K. Nguyen and J. Traoré, "An online public auction protocol protecting bidder prvacy," in *Proceedings of Australasian Conference on Information Security and Privacy, ACISP2000*, pp. 427–442, 2000.

[17] K. Omote and A. Miyaji, "A practical English auction with one-time registration," in *Proceedings of Australasian Conference on Information Security and Privacy, ACISP2001*, pp. 221–234, 2001.

[18] S. Park, S. Kim, and D. Won, "ID-based group signature," *Electronics Letters*, vol. 33, no. 19, pp. 1616–1617, 1997.

[19] H. Petersen, "How to convert any digital signature scheme into a group signature scheme," in *Security Protocol Workshop*, pp. 177–190, Paris, 1997.

[20] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols," in *Advances in Cryptology, Crypto'94*, pp. 174–187, Lecture Notes in Computer Science, 1994.

[21] Yuh-Min Tseng and Jinn-Ke Jan, "Improved group signature scheme based on discrete logarithm problem," *Electronics Letters*, vol. 35, no. 1, pp. 37–38, 1998.