Inf Syst Front (2009) 11:335–343
DOI 10.1007/s10796-008-9094-3

A secure e-auction scheme based on group signatures

Cheng-Chi Lee · Pi-Fang Ho · Min-Shiang Hwang

Published online: 20 May 2008

Abstract Recently, electronic auctions have been receiving more and more attention in the world of electronic commerce. The security and efficiency of electronic auctions are becoming important. We shall propose a securely sealed-bid auction scheme that uses our group signature scheme with the function of authenticated encryption. It can achieve the following goals: secrecy of bidding price, anonymity, verifiability, non-repudiation, and better performance.

Keywords E-auction · Electronic commerce · Group signature · Sealed-bid auction · Security

C.-C. Lee (✉)
Department of Computer & Communication Engineering,
Asia University, No. 500, Lioufeng Raod,
Wufeng Shiang, Taichung, Taiwan,
Republic of China
e-mail: cclee@asia.edu.tw

P.-F. Ho
Graduate Institute of Networking and Communication
Engineering, Chaoyang University of Technology,
168 Gifeng E Rd., Wufeng, Taichung Country,
Taiwan 413, Republic of China

M.-S. Hwang
Department of Management Information System,
National Chung Hsing University, 250 Kuo Kuang Road,
Taichung, Taiwan 402, Republic of China
e-mail: mshwang@nchu.edu.tw

1 Introduction

Due to Internet is now in widespread use, a lot of traditional businesses are implemented, especially electronic auction. Electronic auctions are a very popular trading method for determining a customer and the sale price (Hwang et al. 2002). The bidder can submit a bid anywhere and anytime through Internet. Generally, electronic auction can be classified into three types: English auction (Lee et al. 2001; Omote and Miyaji 2001) (and Dutch auction is also known as public bid auction), Dutch auction and sealed-bid auction (Chang and Chang 2003; Franklin and Reiter 1996; Kudo 1998). In English auction, each bidder casts his/her public bid on the product, and the bid must be higher than all bids in the previous round of bidding. After a round, the highest bid is adjusted upward until nobody submits a new bid in a given round. In Dutch auction, it is similar to English auction. Dutch auction begins with the highest bid, and then bids go down round after round until the first bidder decides to buy the product. In sealed-bid auction, all bids are sealed. All bidders submit their own bids to the auctioneer. After the deadline of the bidding, the auctioneer can open the bid and determines the winner. The difference between the public bid auction and the sealed-bid auction is that the one is multi-bidding auction and the other is single-bidding auction.

Recently, e-auction has been receiving a great deal of attention in the world of e-commerce. There are many e-auction schemes proposed (Chang and Chang 2003; Franklin and Reiter 1996; Harkavy et al. 1998; Hwang et al. 2002; Kawagoe 1996; Kikuchi et al. 1999; Sakurai and Miyazaki 1999; Kudo 1998; Lee et al. 2001; Liu et al. 2000; Omote and Miyaji 2001; Subramanian 1998). In

Subramanian (1998), Subramanian proposed a secure English auction scheme. It used the technique of public key cryptosystem to establish a secure transaction channel. It was claimed that the scheme ensured anonymity and security. However, Hwang et al. pointed out that Subramanian's auction scheme had a security flaw. The bid can be forged by a malicious auctioneer (Hwang et al. 2002). In Franklin and Reiter (1996), Franklin and Reiter proposed a sealed-bid auction protocol based on verifiable signature sharing (Franklin and Reiter 1995). It is used to prevent malicious bidders from canceling their bids. In Kawagoe (1996), Kawagoe proposed a secure sealed-bid auction protocol based on blind signature (Chaum 1982). It does not include time into their protocol. In Kudo (1998), a time server is used to carry out a sealed-bid auction protocol. In Omote and Miyaji (2001), Omote and Miyaji proposed a simple and efficient protocol that used the signature of knowledge to provide bidder anonymity. Later, Lee et al. (2001) pointed out that their scheme had a weakness that the Registration Manager (RM) or Auction Manager (AM) might not be honest.

In Kikuchi et al. (1999), proposed a multi-round anonymous auction protocol based on verifiable secret sharing (Rabin and Ben-Or 1989). The value of specific bids is kept secret even at the termination of the auction. In Liu et al. (2000), proposed a multi-round standard sealed bid auction scheme based on Shamir's threshold secret sharing (Shamir 1979). The scheme used the same model as that in Kikuchi et al. (1999). It can satisfy the following properties: secrecy of bidding price, validity, non-repudiation, and fast execution. In Chang and Chang (2003), proposed a simple and efficient method to ensure that the bidders can bid arbitrarily and anonymously. The anonymous auction scheme can act in English auction, Dutch auction, and sealed-bid auction. It is based on Fan et al.'s deniable authentication protocol (Fan et al. 2002).

In 1991, Chaum and van Heyst (1991) introduced the concept of group signature. 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. There are four properties to be met in group signature as follows:

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.

It is not hard to find the implicit relationship between the two distinct schemes, group signature and e-auction. The role of the signer in group signature scheme is played as the bidder in e-auction scheme. The role of the verifier in group signature scheme is played as the auctioneer in e-auction scheme. The role of the group manager in group signature scheme is played as the RM in e-auction scheme. Once the bidder casts his/her bid on the product, the auctioneer can verify the bid and open the bid to decide the winning bid. The RM can find the original identity of the winning bidder. As a result, the properties of group signature can be applied to e-auction scheme. In 2000, Nguyen and Traore' proposed an English auction scheme based on the group signature (Nguyen and Traoré 2000). Unfortunately, their scheme violates the anonymity and the difficulty of revoking the bidder is also shortcoming passed down from the signature.

In this paper, we propose a new group signature scheme with the function of authenticated encryption. Authenticated encryption is the digital signature with a message recovery function. It can combine the functions of digital signature and encryption (Lee and Chang 1995; Tseng et al. 2003). The signer may generate the signature for a message and only the specified receiver can recover and verify the message. This kind of new scheme can achieve authenticity, confidentiality, integrity and non-repudiation at the same time. It can produce a group signature and the ciphertext at the same time. The verifier (receiver) can check the validity of the group signature and recover the message simultaneously. What token has to be into account is that the receiver can recover the message. This kind of new group signature scheme is suitable for e-auction. We shall use our group signature scheme to design a secure sealed-bid auction scheme. Our e-auction scheme can find the winning bidder quickly in the opening phase. It can achieve the following properties (Liu et al. 2000; Zhang et al. 2000):

1. *Secrecy of bidding price:* the auctioneer must not know how much the bidders offer until the auction is completed. Otherwise, the auctioneer could possibly reveal information to bidders. Thus, the result of the bidding will be influenced.
2. *Anonymity:* all of the bidders' identities must be anonymous during the bidding.

3. *Verifiability:* everyone will be allowed to check the source and completion of a bid. However, nobody can submit a falsified bid to the auctioneer even if they are disguised as a legitimate bidder.
4. *Non-repudiation:* no one can repudiate his/her bid. Every bidder has a certificate to identify his/her bid.
5. *Performance:* the auction should support many bidders and efficiently find out the winner of this auction.

The rest of this paper is organized as follows: In Section 2, a new group signature scheme based on authenticated encryption is proposed. Next, we will propose our e-auction scheme based on our group signature scheme in Section 3. The analysis is described in Section 4. Finally, a summary is given in Section 5.

2 The proposed group signature scheme

2.1 The proposed scheme

Our group signature scheme involves three phases: the initiation phase, the signing and verification phase, and the identification phase. We describe our group signature scheme as follows.

- Initiation Phase:
  Let p and q be large primes 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 group 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 group manager randomly chooses an integer k_i in $Z_q{}^*$ and computes $r_i = y_i \cdot k_i - x_T \bmod q$ and $s_i = y_i{}^{k_i} \bmod p$. Next, the group manager sends (r_i, s_i) to the group member U_i directly. After receiving (r_i, s_i), U_i may verify the validity by checking the equation $s_i{}^{y_i} = (g^{r_i} \cdot y_T)^{x_i} \bmod p$.
- Signing and Verification Phase:
  In our scheme, we added a short message as a test. Thus, we called it M_{check}. U_i wants to sign the message $M_{original}$ by using the following steps:

  1. Compute $M = M_{check}||M_{original}$, where $||$ denotes the concatenation.
  2. U_i selects two random numbers R_1, R_2 in $Z_q{}^*$.
  3. Compute four parameters A, B, C, D as follows:

  $$A = x_i \cdot R_1 \cdot R_2 \bmod q, \tag{1}$$

  $$B = s_i^{R_1 \cdot R_2 \cdot y_i} \bmod p, \tag{2}$$

  $$C = M \cdot y_j{}^{-R_1 \cdot A \cdot h(B)} \bmod p, \textit{and} \tag{3}$$

  $$D = R_1 - r_i \cdot h(C) \bmod q. \tag{4}$$

  4. The group signature for message M is $\{A, B, C, D, M_{check}\}$.

  Receiver j can verify the group signature by using the following steps:

  1. Recover the message M as follows:

  $$M = C \cdot \left[g^{D\cdot A} \cdot y_T{}^{-h(C)\cdot A} \cdot B^{h(C)}\right]^{x_j \cdot h(B)} \bmod p. \tag{5}$$

  2. Check the following equation:

  $$M_{check} \overset{?}{=} head(M, s), \tag{6}$$

  where, $h(\cdot)$ is a collision-resistant hash function; M_{check} is a binary string with s bits; and $head(M, s)$ is a function which returns the first s bits of binary string M. If the above equation holds, the signature is valid.

- Identification Phase:
  In the case of a dispute, the signature must be opened to reveal the identity of the signer. As the group manager has access to the (y_i, k_i) of each member U_i, the group manager can acquire the (y_i, k_i) of U_i satisfying the equation $B = g^{A\cdot k_i \cdot y_i} \bmod p$ for $i = 1, 2, \cdots, n$, where n is the number of group members. So the group manager can determine the signer.

2.2 Security analysis

The security of our scheme is based on the difficulty of the discrete logarithm problem. In the following, we show that our scheme satisfies all the security properties.

- *Unforgeability and Exculpability:*

Attack 1: If an adversity wants to generate a valid group signature, he/she must have a valid membership (r_i, s_i) and the corresponding secret key x_i. We assume that he/she intercepts a valid membership (r_i, s_i) and tries to forge the group signature. First, he/she computes B by Eq. 2. Then, he/she must compute A, C and D by Eqs. 1, 3 and 4. Because he/she does not have the secret key x_i, he/she cannot forge a group signature making Eq. 5 holds.

Attack 2: An adversity does not have any information for forging group signature. If he/she can generate a signature $\{A, B, C, D, M_{check}\}$ that satisfy the checking Eqs. 5 and 6, and the verifier thinks the signature

$\{A, B, C, D, M_{check}\}$ is a valid group signature. There are four situations, we describe in the following:

(1) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects A, C, D. Then, he/she computes Eq. 5 by A, C, D and obtains the equation $(\triangle \cdot B^{h(C)})^{h(B)\cdot x_j} = \triangledown \bmod p$, where $\triangle$ and ∇ are integers, x_j is a secret key of the verifier V_j. The adversity must solve the congruence relation $(\triangle \cdot B^{h(C)})^{h(B)\cdot x_j} = \triangledown \bmod p$ for B. It is difficult to calculate the parameter B when we know $\triangle$, $\triangledown$ and C. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

(2) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects A, B, C. Then, he/she computes Eq. 5 by A, B, C and obtains the equation $\triangle^{x_j} \cdot g^{D\cdot\triangledown\cdot x_j} = \Phi \bmod p$, where $\triangle$, $\triangledown$ and Φ are integers, x_j is a secret key of the verifier V_j. The adversity must solve the congruence relation $\triangle^{x_j} \cdot g^{D\cdot\triangledown\cdot x_j} = \Phi \bmod p$ for D. It is difficult to calculate the parameter D when we know $\triangle, \triangledown, \Phi$ and g. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

(3) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects A, B, D. Then, he/she computes Eq. 5 by A, B, D and obtains the equation $C \cdot (\triangle \cdot \triangledown^{h(C)})^{x_j\cdot\Phi} = M \bmod p$, where $\triangle$, Φ and ∇ are the integers, x_j is a secret key of the verifier V_j. The adversity must solve the congruence relation $C \cdot (\triangle \cdot \triangledown^{h(C)})^{x_j\cdot\Phi} = M \bmod p$ for C. It is difficult to calculate the parameter C when we know $\triangle, \triangledown, \Phi$ and M. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

(4) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects B, C, D. Then, he/she computes Eq. 5 by B, C, D and obtains the equation $(\triangle \cdot *)^{x_j\cdot\Phi} = \triangledown \bmod p$, where $\triangle, \nabla, \Phi$ and $*$ are integers, x_j is a secret key of the verifier V_j. The adversity must solve the congruence relation $(\triangle \cdot *)^{x_j\cdot\Phi} = \triangledown \bmod p$ for A. It is difficult to calculate the parameter A when we know $\triangle, \nabla, \Phi$ and $*$. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

Attack 3: If the verifier V_j does not have any information for forging a group signature except his/her secret key x_j. If he/she can generate a signature $\{A, B, C, D, M_{check}\}$ that satisfies the checking Eqs. 5 and 6, and the verifier believes the signature $\{A, B, C, D, M_{check}\}$ is a valid group signature. There are four situations, we describe in the following:

(1) The verifier V_j chooses a message $M = M_{check}||M_{original}$ and randomly selects A, C, D. Then, he/she computes Eq. 5 by A, C, D and obtains the equation $\triangle^{h(B)} \cdot B^{h(B)\cdot *} = \triangledown \bmod p$, where $\triangle, \triangledown$ and $*$ are integers. The adversity must solve the congruence relation $\triangle^{h(B)} \cdot B^{h(B)\cdot *} = \triangledown \bmod p$ for B. It is difficult to calculate the parameter B when we know $\triangle$, $\triangledown$ and $*$. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

(2) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects A, B, C. Then, he/she computes Eq. 5 by A, B, C and obtains the equation $g^{D\cdot\triangle} = \triangledown \bmod p$, where $\triangle$ and $\triangledown$ are integers. The adversity must solve the congruence relation $g^{D\cdot\triangle} = \triangledown \bmod p$ for D. It is difficult to calculate the parameter D when we know $\triangle, \triangledown$ and g. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

(3) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects A, B, D. Then, he/she computes Eq. 5 by A, B, D and obtains the equation $C \cdot (\triangle \cdot \triangledown^{h(C)}) = M \bmod p$, where $\triangle$ and ∇ are integers. The adversity must solve the congruence relation $C \cdot (\triangle \cdot \triangledown^{h(C)}) = M \bmod p$ for C. It is not easy to calculate the parameter C when we know $\triangle, \triangledown$ and M. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

(4) An adversity chooses a message $M = M_{check}||M_{original}$ and randomly selects B, C, D. Then, he/she computes Eq. 5 by B, C, D and obtains the equation $\triangle^{A} = \triangledown \bmod p$, where $\triangle$ and $\triangledown$ are integers. The adversity must solve the congruence relation $\triangle^{A} = \triangledown \bmod p$ for A. It is not easy to calculate the parameter A when we know $\triangle$ and $\triangledown$. Based on the discrete logarithm problem, the adversity cannot forge the group signature that makes the checking equation holds.

- *Anonymity:*

Given a valid group signature $\{A, B, C, D, M\}$, it is hard for everyone but the group manager to identify the actual signer. All private information is protected by random parameters. Because a valid group signature $\{A, B, C, D, M\}$ just A and B have the relations about identity information. We discuss whether our scheme has anonymity by A and B.

Attack 1: Given a valid group signature $\{A, B, C, D, M\}$. The equation $A = x_i \cdot R_1 \cdot R_2 \bmod q$, therefore $g^A = g^{x_i \cdot R_1 \cdot R_2} = y_i^{R_1 \cdot R_2} \bmod p$, where R_1, R_2 are integers. If anyone has the integers R_1 and R_2 then he/she can computes y_i and finds out the identity of the actual signer. But R_1 and R_2 are unknown numbers and nobody can finds out the signer. To sum things up, our scheme has anonymity.

Attack 2: Given a valid group signature $\{A, B, C, D, M\}$. The equation $B = s_i^{R_1 \cdot R_2 \cdot y_i} = y_i^{k_i \cdot R_1 \cdot R_2 \cdot y_i} \bmod p$, where k_i, R_1 and R_2 are integers. In the same way, if anyone has the integer k_i, R_1 and R_2 then he/she can computes y_i and finds out the identity of the actual signer. But k_i, R_1 and R_2 are unknown. Therefore, the identity of actual signer cannot be discovered.

- *Unlinkability:*

Similar to anonymity, deciding if two signatures $\{A, B, C, D, M\}$ and $\{A', B', C', D', M'\}$ were generated by the same group member is not possible.

Attack 1: Given two valid group signatures $\{A, B, C, D, M\}$ and $\{A', B', C', D', M'\}$. If the two group signatures are generated by the same signer. First, anyone can compute $g^A/g^{A'} = g^{x_i \cdot R_1 \cdot R_2}/g^{x_i \cdot R'_1 \cdot R'_2} \bmod p$ and $B/B' = s_i^{R_1 \cdot R_2 \cdot y_i}/s_i^{R'_1 \cdot R'_2 y_i} = (g^{x_i \cdot R_1 \cdot R_2}/g^{x_i \cdot R'_1 \cdot R'_2})^{k_i \cdot y_i} \bmod p$. Then, he/she can compute $(g^A/g^{A'})^{k_i \cdot y_i} = B/B' \bmod p$ and check the equation holds or not. If the equation holds, the two valid group signature $\{A, B, C, D, M\}$ and $\{A', B', C', D', M'\}$ were generated by the same signer. But the integer k_i and y_i are unknown, hence, anyone cannot know where the two group signature were generated by the same signature or not.

- *Traceability:*

Because the group manager has access to the (y_i, k_i) of each member U_i, the group manager can acquire the (y_i, k_i) of U_i satisfying the equation $B = g^{A \cdot k_i \cdot y_i} \bmod p$ for $i = 1, \cdots, n$, where n is the number of group members. So the group manager can determine the signer.

2.3 Performance analysis

In the following, let us consider the performance of our proposed scheme. The performance evaluation of the proposed scheme mainly concerns the time complexity. For convenience, we assume some notations are used to analyze the computational complexity as follows:

1. T_h is the time for executing the one-way hash function $h(\cdot)$.
2. The amount of time to execute a modular exponentiation operation is T_{exp}.
3. T_{Nmul} is the time for multiplication with modulo N.

In our group signature scheme, the signer requires $2T_{exp} + 2T_h + 8T_{Nmul}$ to generate a group signature. The verifier requires $4T_{exp} + 2T_h + 6T_{Nmul}$ to verify the group signature.

3 The proposed e-auction scheme using our group signature

3.1 Our electronic auction model

Our electronic auction model comprises of three phases: bidder registration phase, bidding phase, and opening phase, and four participants: bidders, a RM, an AM and a identity manager (IM). In our model, we shall use public cryptosystems to ensure the security of transmission on a public channel and use the group signature technique to protect the private information. The responsibilities of these facilities are described as follows:

- Bidders: The user has the valid certificate that can bid goods on the Internet.
- RM: The registration manager is responsible for registering each bidder. Before bidding goods, the bidder must register and obtain his/her certificate from RM, first. After sending the certificate to the bidder, RM maintains the database of bidders' information in order to find the original identity of the winning bidder. Therefore, the RM has two functions: enabling bidders to bid, and revealing the identity of the bidder's originator.
- AM: All bidding goods must register to AM, firstly. Hence, AM must manage the information of goods. On the other hand, AM responds to managing the bids until the end of the bidding time. AM also responds to opening the bids. He/she finds the winning bid and opens it to provide bidders checking the validity.
- IM: AM responds to opening the bids, but, he/she can only finds the winning bid and does not know the identity of the winner. Hence, when AM finds the winning bid, then, he/she sends the winning bid to RM. RM can finds the identity of the winner. But RM requires too much time for finding the winner's

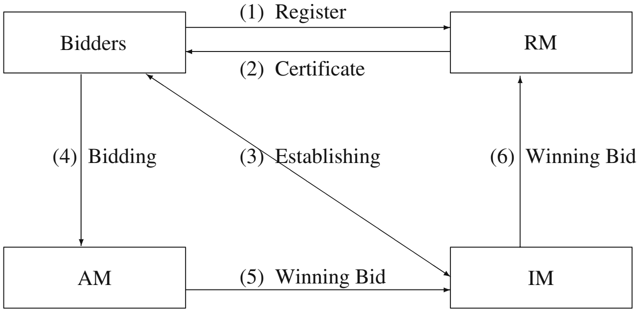

Fig. 1 The new e-auction protocol architecture

identity. In order to ameliorate the performance, we improved our group signature scheme. AM sends the winning bid and relative information to IM, then, IM processes it and sends the winning bid and the process information to RM. Finally, RM can find the winner's identity for a short time. Therefore, the function of IM helps RM find the winner's identity more quickly. The new e-auction protocol architecture is shown in Fig. 1.

3.2 Our electronic auction scheme

We shall introduce the proposed electronic auction protocol in this section. In Table 1, we list the abbreviations and notations used in our scheme.

The proposed scheme is composed of three phases, which are the bidder registration phase, the bidding phase and the winner's decision and announcement phase (opening phase). AM and RM have private keys x_{AM} and x_{RM} as well as their corresponding public key $y_{AM} = g^{x_{AM}} \bmod p$ and $y_{RM} = g^{x_{RM}} \bmod p$, respectively. Let p be a large prime and q equal to $p-1$ or a large prime factor of $p-1$. The details of our scheme's procedures are described as follows.

3.2.1 Bidder registration phase

Bidder B_i randomly selects a private key x_i and computes the corresponding public key $y_i = g^{x_i} \bmod p$. Then, B_i secretly sends his/her information ID_i and y_i to RM for registration. When RM accepts the registration request. RM computes the certificate (r_i, s_i) as follows:

$$r_i = y_i \cdot k_i - x_{RM} \bmod q,$$
$$s_i = {y_i}^{k_i} \bmod p,$$

where k_i is a random number and $\gcd(k_i, q) = 1$. Then, RM selects a random number RN_i and sends (r_i, s_i) and RN_i to the bidder B_i secretly. After receiving (r_i, s_i) and RN_i, bidder B_i can verify the certificate by the following congruence relation:

$$s_i^{y_i} = (g^{r_i} \cdot y_{RM})^{x_i} \bmod p.$$

If the above equation holds, then the certificate for bidder B_i is valid. The RN_i is a password, and RM can use it to find the identity of the winning bidder quickly. In the meantime, RM maintains a database of the bidders' information in Table 2.

Table 1 The notations used in the proposed scheme

Notations	Meaning
ID_i	A unique identity of each bidder, such as the identity card number
x_i	A private key of the bidder B_i
y_i	A public key of the bidder B_i
x_{RM}	A private key of the RM
y_{RM}	A public key of the RM
x_{AM}	A private key of the AM
y_{AM}	A public key of the AM
x_I	A private key of the IM
y_I	A public key of the IM
$h(\cdot)$	A one way hash function
RN_i	A linking value of the bidder B_i
GNO_i	A serial number of goods
GS	A group signature
$head(M, s)$	A function which returns the first s bits of binary string M
M	A message
T_i	A timestamp
P_i	A price of the bid
$\|\|$	An operator which concatenates two binary strings

Table 2 The database of the bidders' information in RM

Identity	Public key	Integer	Linking value
ID_1	y_1	k_1	RN_1
ID_2	y_2	k_2	RN_2
ID_3	y_3	k_3	RN_3
⋮	⋮	⋮	⋮

3.2.2 Bidding phase

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

1. The bidder sends his/her RN_i and GNO_i to IM. When receiving it, IM selects a random number d_i and computes $NO_i = GNO_i || d_i$. Then, IM signs NO_i and RN_i using x_I as $S = Sign_{x_I}[NO_i, RN_i]$ and sends S and NO_i to the bidder. Finally, IM maintains a database in Table 3. The bidder verifies the S by the public key y_I of IM. The bidder can check whether the RN_i of the decryption is equal to the bidder's RN_i. This step can prevent anyone from modifying the NO_i.
2. The bidder uses his/her certificate (r_i, s_i) and GNO_i to create a signature on his/her bid. First, he/she constructs $M = (GNO_i || T_i, NO_i, P_i)$, where P_i is the price of the bid, and T_i is the timestamp. Then, he/she selects two random numbers R_1 and R_2 in $Z_q{}^*$, and computes A, B, C, and D as follows:

$$A = x_i \cdot R_1 \cdot R_2 \bmod q,$$

$$B = s_i{}^{R_1 \cdot R_2 \cdot y_i} \bmod p,$$

$$C = M \cdot y_{AM}{}^{-R_1 \cdot A \cdot h(B)} \bmod p,$$

$$D = R_1 - r_i \cdot h(C) \bmod q.$$

   Finally, $\{A, B, C, D, GNO_i\}$ is a bid and the bidder sends it to AM.
3. When AM receives bids, he/she maintains a database in Table 4 until the opening phase.

Table 3 The database of the bidders' linking value in IM

Linking value	NO.
RN_1	NO_1
RN_2	NO_2
RN_3	NO_3
⋮	⋮

Table 4 The database of the bid information in AM

Serial numbers	Signature
1	$\{A_1, B_1, C_1, D_1, GNO_1\}$
2	$\{A_2, B_2, C_2, D_2, GNO_2\}$
3	$\{A_3, B_3, C_3, D_3, GNO_3\}$
⋮	⋮

3.2.3 Opening phase

When it is the end of the bidding procedure, AM, IM and RM will cooperate to find and publish the identity of winner B_w as follows.

1. AM recovers all messages using the following equation: $M_i = C_i \cdot [g^{D_i \cdot A_i} \cdot y_{RM}{}^{-h(C_i) \cdot A_i} \cdot B_i^{h(C_i)}]^{x_{AM} \cdot h(B_i)} \bmod p$ for $i = 1, 2, \cdots, n$. Then, AM finds the highest bid M_j and checks the congruence relation $GNO_j = head(M_j, s)$. If the above relations holds, then the signature is valid. The signature $\{A_j, B_j, C_j, D_j, GNO_j\}$ is the winning bid.
2. AM chooses a random number R_3 and computes $Q_j = x_{AM} \cdot R_3 \bmod q$ and $C'_j = M_j \cdot (C_j \cdot M_j^{-1})^{R_3} \bmod p$. Then, AM publishes $\{A_j, B'_j, Q_j, C_j, D_j, GNO_j\}$ and everyone can verify it by checking whether $M_j = C'_j \cdot [g^{D_j A_j} \cdot y_{RM}{}^{-h(C_j) A_j} \cdot B_j^{h(C_j)}]^{Q_j \cdot h(B_j)} \bmod p$ holds or not. In other words, everyone can check the bid which is highest.
3. AM sends the winning bid $\{A_j, B_j, C_j, D_j, GNO_j\}$ and NO_j to IM. Then, IM finds the corresponding password RN_j of NO_j by the Table 3.
4. IM sends the winning bid $\{A_j, B_j, C_j, D_j, GNO_j\}$ and RN_j to RM. When RM receivers it, he/she can find the corresponding ID_j, y_j and k_j of RN_j by the Table 2. Then, RM checks whether $B_j = g^{A_j \cdot k_j \cdot y_j} \bmod p$ holds or not. If the above holds, B_j that has identified ID_j is the winner. Finally, RM chooses a new password New_RN_j, and sends GNO_j and New_RN_j to the winner. When the

Table 5 The database of the bidders' information in RM

Identity	Public key	Integer	Linking value
ID_1	y_1	k_1	RN_1
ID_2	y_2	k_2	RN_2
ID_3	y_3	k_3	RN_3
⋮	⋮	⋮	⋮
ID_j	y_j	k_j	PW_j, New_RN_j
⋮	⋮	⋮	⋮

winner B_j receives it, he/she knows he/she is winning the bidding, and he/she must use New_RN_j to bid the next time. On the other hand, RM adds New_RN_j to the database in Table 5. Because B_j may use RN_j to bid many goods and in order to prevent this does not find the winner in the opening phase. RM must retain RN_j for a length of time until the above situation cannot occur again.

4 Analysis

The security analysis of the proposed e-auction protocol is similar to our group signature scheme in Section 2.2. Here, we shall analyze our e-auction protocol and check whether it can satisfy all of the requirements we brought up earlier.

1. *Secrecy of bidding price:* to protect the secrecy of the bidding phase, we use our group signature scheme with the function of authenticated encryption. It is guaranteed that no one can compute the previous value without the secret key of AM. Hence, only AM can compute the bidding price in the opening phase.
2. *Anonymity:* in our scheme, the bidder B_i generates a group signature to bid the goods. AM only can recover the message and check the validity but cannot know the identity of the bidder in the opening phase. After AM finds and opens the winner's bid, RM just can find the identity of the winner. Hence, nobody knows the identity of a bidder during the bidding.
3. *Verifiability:* anyone can verify the winning price and bid because it is published.
4. *Non-repudiation:* bidders cannot deny bidding and own bid prices because no one can find a random number k_j and ID_j to correspond with the checking equation.
5. *Performance:* the bidder can repeatedly use his/her (r_i, s_i) to bid. He/she just computes a signature GS on the bid when he/she wants to bid in the auction. In the opening phase, our scheme can find out the winner in a short time.

5 Conclusion

In this paper, we propose a new group signature scheme with the function of authenticated encryption. This kind of new scheme can achieve authenticity, confidentiality, integrity, and non-repudiation at the same time. It can produce a group signature and the ciphertext simultaneously. This new kind of group signature is suitable for e-auction.

Therefore, we used our group signature scheme to design an anonymous e-auction protocol. And the protocol is a securely sealed bid auction system. No one can discover any content of the bids before the bids are opened in the opening phase. It can achieve the following properties: secrecy of bidding price, anonymity, verifiability, non-repudiation, and performance.

References

Chang, C. C., & Chang, Y. F. (2003). Efficient anonymous auction protocols with freewheeling bids. *Computers & Security, 22*(8), 728–734.

Chaum, D. (1982). Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), *Advances in cryptology, CRYPTO'82* (pp. 199–203). New York: Plemum.

Chaum, D., & Heyst, E. (1991). Group signatures. In *Advances in cryptology, Eurocrypt'91* (pp. 257–265). Lecture Notes in Computer Science.

Fan, L., Xu, C. X., & Li, J. H. (2002). Deniable authentication protocol based on Diffie-Hellman algorithm. *Electronics Letters, 38*(14), 705–706.

Franklin, M. K., & Reiter, M. K. (1995). Verifiabe signature sharing. In *Advances in cryptology, EUROCRYPT'95* (pp. 50–63). Lecture Notes in Computer Science 921.

Franklin, M. K., & Reiter, M. K. (1996). The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering, 22*(3), 302–312.

Harkavy, M., Kikuch, H., & Tygar, J. D. (1998) Electronic auction with private commerce. In *Proceedings of the 3rd USENLX workshop on electronic commerce*, August.

Hwang, M.-S., Lu, E. J.-L., & Lin, I.-C. (2002). Adding timestamps to the secure electronic auction protocol. *Data & Knowledge Engineering, 40*(2), 155–162.

Kawagoe, T. (1996). Electronic auction mechanism. In *Proceedings of the symposium on information, Media'96* (pp. 75–82). August

Kikuchi, H., Hakavy, M., & Tygar, D. (1999). Multi-round anonymous auction protocols. *IEICE Transactions on Information and Systems, E82-D*(4), 769–777.

Sakurai, K., & Miyazaki, S. (1999). A bulletin-board based digital auction scheme with bidding down strategy. In *Proceedings of the international workshop on cryptographic techniques and E-commerce* (pp. 180–187). HongKong City University, July.

Kudo, M. (1998). Secure electronic sealed-bid auction protocol with public key cryptography. *IEICE Transactions on Fundamentals, E81-A*(1), 20–27.

Lee, B., Kim, K., & Ma, J. (2001). Efficient public auction with one-time registration and public verifiabiltiy. In *Proceedings of Indocrypt2001* (pp. 16–20). Chennai, India: Madras.

Lee, W.-B., & Chang, C.-C. (1995). Authenticated encryption schemes without using a one way function. *Electronics Letters, 31*(19), 1656–1657.

Liu, S., Wang, C., & Wang, Y. (2000). A secure multi-round electronic auction scheme. In *Proceedings of the EURO-COMM'2000* (pp. 330–334). Germany, May.

Nguyen, K., & Traoré, J. (2000). An online public auction protocol protecting bidder prvacy. In *Proceedings of Australasian conference on information security and privacy, ACISP2000* (pp. 427–442).

Omote, K., & Miyaji, A. (2001). A practical english auction with one-time registration. In *Proceedings of Australasian conference on information security and privacy, ACISP2001* (pp. 221–234).

Rabin, T., & Ben-Or, M. (1989). Verifiable secret sharing and multiparty protocols with honest majority. In *STOC'89* (pp. 73–85).

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*, 612–613.

Subramanian, S. (1998). Design and verification of a secure electronic auction protocol. In *IEEE 17th symposium on reliable distributed systems* (pp. 204–210).

Tseng, Y.-M., Jan, J.-K., & Chien, H.-Y. (2003). Authenticated encryption schemes with message linkages for message flows. *Computers and Electrical Engineering, 29*(1), 101–109.

Zhang, F., Li, Q., & Wang, Y. (2000). A new secure electronic auction scheme. In *Proceedings of the EUROCOMM 2000* (pp. 54–56). Germany, May.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, Republic of China in 2007. He is a Assistant Professor of Computer and Communication, Asia University, from 2007. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 30 articles on the above research fields in international journals.

Pi-Fang Ho received the B.S. degree in Information Management and M.S. in Graduate Institute of Networking and Communication Engineering from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2002 and in 2004. Her current research interests include cryptography, information security, and network security.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published over 100 articles on the above research fields in international journals.