An Anonymous Sealed-bid Electronic Auction Based on Ring Signature

Hu Xiong, Zhiguang Qin, and Fagen Li
(Corresponding author: Hu Xiong)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
No.4, Section 2, North Jianshe Road, Chengdu, 610054, China (Email: xionghu.uestc@gmail.com)
(Received Oct. 08, 2007; revised Mar. 28, 2008; and accepted May 30, 2008)

Abstract

Privacy and anonymity have become two factors of increasing importance in auction protocol. This paper provides an efficient sealed-bid electronic auction protocol based on the technique of ring signature and verifiable technique of encryption key chain. The peculiar characteristics of our protocol are non-repudiation of bidders but preserving their anonymity and allowing the auctioneer to determine the wining bid without revealing the losing bid. Our protocol has additional characteristics such as public verifiability, unforgeability, correctness and fairness.

Keywords: Anonymity, encryption key chain, non-repudiation, privacy, ring signature, sealed-bid auction

1 Introduction

1.1 Backgrounds

Electronic auctions are fundamental parts of the electronic commerce technology. They are not only widespread mechanisms selling goods, but have also been shown applicable to task assignment, scheduling, or finding the shortest path in a network with selfish nodes [2]. To date, many researchers have studied and published various outstanding auction protocols [1, 2, 6, 16]. As there are a variety of auction styles such as English, Dutch, Sealed-bid, Vickery, and M+1, etc., whose rules are quite different, each protocol has distinctive goals and decision strategies depending on its own style. Our target among the auction styles is to design an efficient Sealed-bid auction in which a bidder commits his bid with which he is willing to pay on the items without disclosing of the bidding price then, after the bidding session, the auctioneer opens the received bids and declares the highest bid as the winning price and the winner who sent the highest bid.

1.2 Related works

From the previous researches, we have figured out there exist two problems which can deteriorate the security of the auction.

One is to identify the winner explicitly by the auctioneer alone. Otherwise, the winner can repudiate his bidding since he feels the winning price is too high to buy the items even if he cast at the winning price. In addition, a bidder can conspire with other bidders to decrease the winning price by not engaging in the winner identification. So the auctioneer must have the ability to authenticate real or equivalent identity of the winner without its assistance. Reference [16]treated non-repudiation as a mandatory requirement. But it does not meet anonymity so that these protocols raise privacy problem. In other references [1, 6, 8], they seemed to be anonymous in that only the indices of the winner are revealed to the auctioneer at the end of protocol. However, inevitably the auctioneer must perform supplementary communications with the winner, namely who is placed in the winning indices, to confirm the fact that he committed the winning bid.

The other problem is the bid privacy, which is a frequently desired characteristic in auction schemes. It refers to the confidentiality of losing bids even after the auction ended. The privacy issues of the sealed-bid auction protocol are listed in Table 1 for comparison [14, 19]. Franklin and Reiter [5] were among the first researchers to address electronic auction with bid privacy. They covered many problems such as secret sharing, digital cash and multicasts as well as their own primitive technique called verifiable signature sharing. Their protocol successfully prevents a single auctioneer from altering a bid or throwing an auction to a single bidder. Unfortunately, their protocol also results in disclosing all bids to all auctioneers after the auction is closed. Kikuchi et al. [7] attempted to deal with such problems through secret sharing techniques, but Sako [12] pointed out that several problems still remain in their work. Felix [2] proposed a security model in which bidders themselves jointly compute the auction outcome so that any subset of bidders is incapable

Table 1: Privacy issues of the sealed-bid auction protocol

Technique	Auctioneer(s)	Hidden bids of losers	Opener of bids
Verifiable signature sharing [5]	Distrusted	No	Auctioneer(s)
Secret sharing [2, 7]	Trusted	Yes/No	Auctioneer(s)
(Distributed)public-key crypto [11, 12]	Trusted	Yes	Auctioneer(s)
Convertible undeniable signature [13]	Distrusted	Yes	Bidder
Homomorphic encryption [1, 3, 17]	Distrusted	Yes	Auctioneer(s)
Hash chaining [16]	Distrusted	Yes	Bidder
Verifiable encryption [14, 15, 19]	Distrusted	Yes	Auctioneer(s)

of revealing private information. The main drawbacks implied by their setting are low resilience and relatively high computational and communication complexity. In addition, the flaw of convertible undeniable signature and hash chaining technique is that all bidders have to take part in the protocol during opening bids. Distributed public-key crypto technique [18] is quite efficient, but it is not fair to all bidders and auctioneer agents. A bidder has to rely on uncertain evidence that more than a threshold of auctioneer agents is honest. Therefore, the construction of an efficient, anonymous and non-repudiable sealed-bid auction is of great interest in the field of cryptography.

Definition 1. *Anonymous and non-repudiable auction is that the bid is committed to the auctioneer anonymously, however the winner can be explicitly identified without bidder's aid at the end of the auction.*

Definition 2. *Sealed-bid auctions are that each bidder seals his bid and submits it before a set time, after that time the bids are opened and the winning price and winner are determined according to a pre-defined auction rule preserving the loser's bids unknown.*

The main goal of this paper is to propose a winner-identifiable anonymous auction protocol based on the ring signature [10], that is to say, the auctioneer can authenticate the real identity of the winner at the end of the protocol without additional interactions with the winning bidder even though all the bidders bid anonymously. On the other hand, this sealed-bid auction method also enjoys bid privacy and public verifiability based on encryption key chain [14, 15, 19], which is claimed to have achieved strong bid privacy efficiently.

1.3 Outline of Paper

Hereinafter, this paper is organized as follows: The next section explains the definition of sealed-bid auction and ring signature. The proposed sealed-bid auction protocol is given in Section 3. The security and efficiency of our protocol is discussed in Section 4. Finally, the conclusions are given in Section 5.

2 Definition

2.1 Auction Rules

Informally, a sealed-bid auction consists of two phases of execution. The first is a bidding period (bidding phase), during which bidders can choose bids from a set of biddable values and submit sealed bids to the auctioneer. At certain point the bidding period is closed, thus initiating the second phase (opening phase) in which the bids are opened and the winner is determined and possibly announced. In general, the rule by which the winner is determined can be publicly known as deterministic rule. For convenient, however, we assume that this rule dictates that the highest bidder be chosen as the winner.

In order for an auction protocol to provide both security and efficiency, we take into account the following requirements:

- Anonymity: Nobody including the authority can identify the losing bidders even after the opening phase.

  Non-repudiation:Auctioneer can verify that bidders followed a protocol to cast their bids and no bidder can repudiate his bid. No malicious bidder can disrupt the auction with an unmannered bid without being detected.

- Unforgeability: Nobody can impersonate a certain bidder.

- Correctness: If every party acts honestly, the correct winning price and winner are determined according to the auction rules.

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

- Fairness: All bids should be fairly dealt with.

- Bid privacy: The scheme should conceal all bids except for the winning bid. This property is desired in order to keep losers' privacy.

- Public verifiability: Anybody can publicly verify that a winning bid is the highest value of all bids and publicly confirm whether a winner is valid or not.

- Efficiency: The protocol should be efficient from the viewpoints of computation and communication.

2.2 Ring Signature

The notion of ring signature was introduced in 2001 by Rivest and Shamir[10]. Ring signature is a digital signature that specifies a set of possible signers, whose main purpose is to provide anonymity for the signer, by making it impossible to determine who among the possible signers is the actual one. But the unconditional anonymity of ring signature provides chances for the criminals. Instead the similar notion group signatures [4] have the demerit that the group manager has the absolute power in revoking the signer's identity.

We assume that each possible signer B_i is associated with a public key y_i and the corresponding secret key is denoted as s_i. A ring signature scheme consists of the following two-tuple (Sign and Verify):

- **Sign**$(m_0, y_1, y_2, \cdots, y_n, s_i)$ which produces a ring signature σ for the message m_0, given the public keys $\{y_1, y_2, \cdots, y_n\}$ of the n ring members, together with the secret key s_i of the i-th member (who is the actual signer).
- **Verify**(m_0, σ) which accepts a message m_0 and a signature σ (which includes the public keys of all the possible signers), and outputs either *true* or *false*.

3 Protocol

3.1 Preliminaries

The notations used in this paper are briefly described in Table 2. Let $B = \{B_1, \cdots, B_n\}$ be a set of n bidders who take part in an auction and offer a price, and AM be Auction Manager who holds an auction and manages a Bulletin Board System (BBS). Let T be a trusted third party who resolves the dispute and revokes the malicious bidder with AM, and $VE_T(x)$ be the verifiable encryption of x with T's public key. A Naccache-Stern encryption algorithm is used [9]. We assume that these two authorities T and AM do not collude together. The role of AM is to manage the participants of auction through administrating the BBS, and prepare for the auction. T plays a part in dissolving the dispute and revoking the malicious bidder with AM's cooperation.

$W = \{\omega_1, \cdots, \omega_l\}$, where $\omega_1 > \cdots > \omega_l$, be a set of l biddable prices, from which each bidder must choose his bid and submit it during the bidding period. In the auction, the highest bidder, i.e., the bidder whose bid has the highest index will be determined as the winner.

The following parameters are used in the protocol. Let p and q be large primes such that $q|p-1$. Given g^x, where g is the generator of a prime-order sub-group of Z_p^*, it is hard to compute x. Let $H : \{0,1\}^* \rightarrow Z_q$ denote an ideal collision resistant cryptographic hash function. Suppose $\{x\}_{y_i}$ is the discrete logarithm based encryption function of x with the public key y_i, where $s_i = \log_g y_i$ is the decryption key to invert it. We assume that the encryption function is semantically secure in order not to reveal any information of bids.

This anonymous, public verifiable sealed-bid auction protocol consists of initial, pre-bidding, bidding and opening phases that are described in detail as follows.

3.2 Initial Phase

Bidder B_i chooses $r_i \in_R Z_q^*$ and computes $p_i = g^{r_i} \bmod p$, then sends (y_i, p_i) to AM while keeping the corresponding s_i and r_i secret. AM registers bidder $B_i (1 \leq i \leq n)$ as the participants of auction with bidder's personal information (y_i, p_i) and publishes it with public parameters such as $\{p, q, H, VE, SE_k\}$ on the BBS.

Step 1: B_i chooses $L = \{y_1, y_2, \cdots, y_d\}$ where $(d \leq n, i \in [1, d])$ from BBS, and chooses h_i as the key of symmetric cryptosystem $SE_k()$. Then B_i computes $\{h_i, L\}_{y_{AM}}$ and sends it to AM through an anonymous connection (such as onion router and Mixnets).

Step 2: AM computes $\{h_i, L\}_{y_T} \leftarrow \{[\{h_i,\ L\}_{y_{AM}}]_{s_{AM}}\}_{y_T}$ and sends it to T.

Step 3: T computes $\{h_i, L\} \leftarrow [\{h_i, L\}_{y_T}]_{s_T}$ and gets $\{p_1, \ldots, p_d\}$ from BBS according to $L(= \{y_1, \ldots, y_d\})$. Then T chooses $r_T \in_R Z_q^*$ and computes $\{p_1^{r_T}, p_2^{r_T}, \cdots, p_d^{r_T}\}$. After that, T computes $Encode(r_T, L) = \{r_T\}_{y_1}, \cdots, \{r_T\}_{y_d}$ and $\alpha_i = SE_{h_i}([Encode(r_T, L)]_{s_T}, [p_1^{r_T}, p_2^{r_T}, \cdots, p_d^{r_T}]_{s_T})$. Finally, T sends α_i to AM and keeps $\{h_i, r_T\}$ secure.

Step 4: AM chooses $r_{AM} \in_R Z_q^*$ and keeps $\{h_i,\ r_{AM}\}$ secure. Then AM computes

$$\begin{aligned} \beta_i &= SE_{h_i}([z_{r_T}]_{s_T}, [z_{r_{AM}}]_{s_{AM}}) \\ &= SE_{h_i}([Encode(r_T, L)]_{s_T}, [Encode(r_{AM}, L)]_{s_{AM}}) \end{aligned}$$

and sends it to B_i through an anonymous connection. B_i can compute $r_T = Decode(z_{r_T}, s_i, L)$ and $r_{AM} = Decode(z_{r_{AM}}, s_i, L)$.

3.3 Pre-bidding Phase

Step 1: Bidder B_i chooses his secret share $s_{i,j}$ for price ω_j, where its corresponding public key is $y_{i,j} = g^{s_{i,j}}$. Additionally, $s_{i,j}$ is encrypted as $\alpha_{i,j} = VE_T(s_{i,j})$ by the public key of trusted third party T. $\alpha_{i,j}$is recoverable by T and can be verified as a correct encryption of the secret committed in $y_{i,j}$ by zero knowledge proof of equality of logarithms. Let $m_{i1} = \{(y_{i,1}, \alpha_{i,1}), \cdots, (y_{i,l}, \alpha_{i,l})\}$. Then, B_i generates ring signature on m_{i1} as follows:

1) Choose randomly $\alpha \in_R Z_q$ and compute $c_{k+1} = H(m_{i1}, g_i^{\alpha} \bmod p)$;
2) For $j = k+1, \cdots, d, 1, \cdots, k-1$, choose randomly $e_j \in_R Z_q$ and compute $c_{j+1} = H(m_{i1}, g_j^{e_j}(p_i^{r_{AM} r_T} y_j)^{c_j} \bmod p)$;
3) Compute $e_k = \alpha - (r_i r_{AM} r_T + s_i) c_k \bmod q$;

Table 2: Notation of parameters

B_i	bidder who has its own secret key s_i and public key y_i $(1 \leq i \leq n)$
T	Trusted Third Party(TTP) who has its own secret key s_T and public key y_T
AM	Auction Manager who has its own secret key s_{AM} and public key y_{AM}
$VE_T(x)$	verifiable encryption of x with T's public key
p, q	primes s.t. q|p-1
$[x]_{s_i}$	DLP-based signature on x using secret key s_i
$\{x\}_{y_i}$	DLP-based encryption on x using public key y_i
$SE_k()$	DES-based symmetric encryption system
$L = \{y_1, \cdots, y_n\}$	n public key of corresponding bidders
$Encode(x, L)$	$Encode(x, L) = z_x = [\{x\}_{y_1}, \cdots, \{x\}_{y_n}]$
$Decode(z_x, s_j, L)$	$Decode(z_x, s_j, L) = [z_x(j)]_{s_j} = [\{x\}_{y_j}]_{s_j} = x$
$H : \{0,1\}^* \rightarrow Z_q$	an ideal cryptographic hash function
$W = \{\omega_1, \cdots, \omega_l\}$	a set of l prices which can be chosen by bidders
$Yes, No \in \{0,1\}$	Predetermined description for indicating bidder's intention
$V_{i,j}$	Encrypted bids of bidder B_i with price ω_j
$v_{i,j}$	Decrypted bids of bidder B_i with price ω_j
S_j, Y_j	Decryption and encryption key at price ω_j
$s_{i,j}, y_{i,j}$	Secret and public key share of bidder B_i at price ω_j

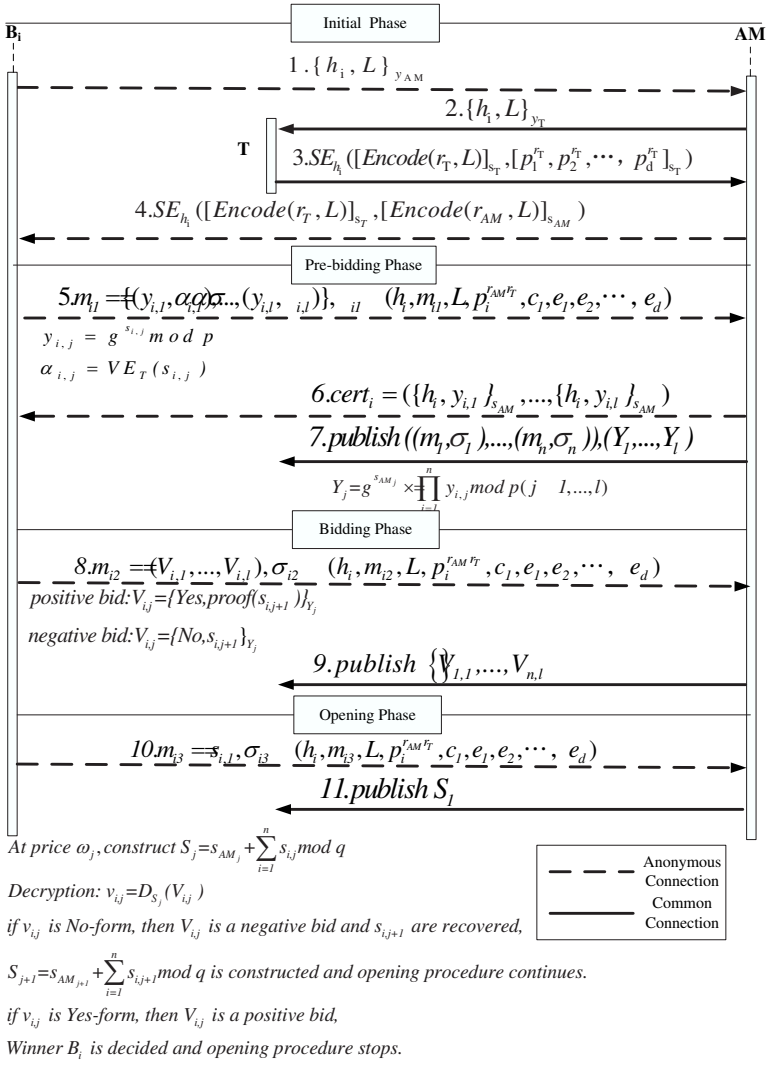

Figure 1: Auction procedure based on ring signature and encryption key chain

4) Return $\sigma_{i1} = (h_i, m_{i1}, L, p_i^{r_{AM} r_T}, c_1, e_1, e_2, \cdots, e_d)$.

B_i sends (m_{i1}, σ_{i1}) to AM through an anonymous connection.

Step 2: AM verifies the ring signature of m_{i1} and the correctness of encryption. The procedure of the verification of the signature can be described as follows:

1) $p_i^{r_{AM} r_T}$ checking: AM decrypts $SE_{h_i}([Encode(r_T, L)]_{s_T}, [p_1^{r_T}, p_2^{r_T}, \cdots, p_d^{r_T}]_{s_T})$ to get $\{p_1^{r_T}, p_2^{r_T}, \cdots, p_d^{r_T}\}$ and computes $\{(p_1^{r_T})^{r_{AM}}, (p_2^{r_T})^{r_{AM}}, \cdots, (p_d^{r_T})^{r_{AM}}\}$. Checking whether $p_i^{r_{AM} r_T} \in \{(p_1^{r_T})^{r_{AM}}, (p_2^{r_T})^{r_{AM}}, \cdots, (p_d^{r_T})^{r_{AM}}\}$, if so, do next step; otherwise, return "Reject".

2) Verify the ring equation: For $j = 1, 2, \cdots, d$, computes

$$c_{j+1} \leftarrow H(m_{i1}, g_j^{e_j} (p_i^{r_{AM} r_T} y_j)^{c_j} \bmod p),$$

If $c_{d+1} = c_1$, then return "Accept" else return "Reject".

If this ring signature is accepted, then AM computes $cert_i = (\{h_i, y_{i,1}\}_{s_{AM}}, \cdots, \{h_i, y_{i,l}\}_{s_{AM}})$ and sends it to B_i through an anonymous connection.

For $1 \le j \le l$, AM randomly chooses s_{AM_j} and computes $Y_j = g^{s_{AM_j}} \times \prod_{i=1}^{n} y_{i,j} \bmod p$, where Y_j is the encryption-key corresponding the bidding price ω_j, and its corresponding decryption-key S_j is denoted as $S_j = s_{AM_j} + \sum_{i=1}^{n} s_{i,j} \bmod q$. Key generation is illustrated in Table 3 for the case of 3 bidders and 6 biddable prices, that is to say, $n = 3$ and $k = 6$. Finally AM publishes $\{(m_{11}, \sigma_{11}), \cdots, (m_{n1}, \sigma_{n1}), (Y_1, \cdots, Y_l)\}$ in the BBS.

3.4 Bidding Phase

Step 1: If B_i is not willing to pay ω_j, $V_{i,j} = \{No, s_{i,j+1}\}_{Y_j}$. If B_i is willing to pay ω_j, $V_{i,j} = \{Yes, proof(s_{i,j+1})\}_{Y_j}$ where $proof(s_{i,j+1})$ is a transcript for zero knowledge of $s_{i,j+1}$. Bid format is illustrated in Table 4 (supposing there are 3 bidders and 6 biddable prices, thus $n = 3, l = 6$, and $\omega_1 > \omega_2 > \cdots > \omega_6$). Then B_i lets $m_{i2} = \{V_{i,1}, \cdots, V_{i,l}\}$ as his bid and computes its ring signature $\sigma_{i2} = \{h_i, m_{i2}, L, p_i^{r_{AM} r_T}, c_1, e_1, e_2, \cdots, e_d\}$. Finally, B_i sends $\{m_{i2}, \sigma_{i2}\}$ to AM through an anonymous connection.

Step 2: After verifying the correctness of the ring signature, AM publishes all bids $\{V_{1,1}, \cdots, V_{n,l}\}$ in BBS.

3.5 Opening Phase

Step 1: Bidder B_i lets $m_{i3} = s_{i,1}$ and computes its ring signature $\sigma_{i3} = \{h_i, m_{i3}, L, p_i^{r_{AM} r_T}, c_1, e_1, e_2, \cdots, e_d\}$ to AM through an anonymous connection.

Step 2: If B_i opens no messages or this check failed, AM runs the dispute protocol, after which B_i is identified and removed from the auction. After verifying the correctness of the ring signature, AM calculates and publishes $S_1 = s_{AM_1} + \sum_{i=1}^{n} s_{i,1} \bmod q$, the first decryption key for the bids at price ω_1. If no "Yes" bid is found at this price, decryption key S_2 for ω_2 can be constructed and opening procedure continues. Similarly the opening procedure can go on along the encryption key chain until a "Yes" bid is found as a winning bid and the key chain is broken. Figure 1 illustrates the auction procedure.

3.6 Dispute Protocol

If B_i cheats or simply crashes, AM invokes the dispute protocol, which is two-party protocol between AM and T for resolving the dispute. At the beginning of this protocol, AM sends (m_{i1}, σ_{i1}) to T, where $m_{i1} = \{(y_{i,1}, \alpha_{i,1}), \cdots, (y_{i,l}, \alpha_{i,l})\}$. Then T will check the correctness of the ring signature and confirm B_i's deviation. The loss of registration information and sending irregular messages can be considered as the deviation. If the confirmation is true, T and AM performs the dispute protocol as follows:

1) T computes $(s_{i,1}, \cdots, s_{i,l})$ by decrypting $\{\alpha_{i,1}, \cdots, \alpha_{i,l}\} = \{VE_T(s_{i,1}), \cdots, VE_T(s_{i,l})\}$ and sends it to AM;

2) AM sets $s_{AM_j} = s_{AM_j} + s_{i,j}$ and continues the opening procedure. Then AM gets r_{AM} according to h_i and sends it to T;

3) T gets r_T according to h_i and computes $\{p_1^{r_{AM} r_T}, \cdots, p_d^{r_{AM} r_T}\}$;

4) T identifies the malicious bidder by comparing $p_i^{r_{AM} r_T}$ with $\{p_1^{r_{AM} r_T}, \cdots, p_d^{r_{AM} r_T}\}$.

Note that $(y_1, p_1), \cdots, (y_n, p_n)$ are published as the participants' personal information in the initial phase. As a result, the malicious bidder can be revoked. And then, AM can exclude the malicious bidder B_i from bidder's list in the BBS and continue the opening bids.

4 Analysis

The security and efficiency of auction protocol is analyzed in this section. It will be shown that the protocol is fair, publicly verifiable and achieves unconditional privacy, anonymity, correctness, and soundness.

4.1 Security Analysis

Anonymity: If nobody can match p_i along with $p_i^{r_{AM} r_T}$ without knowing r_{AM} and r_T, our protocol is unconditionally bidder-ambiguous.

Table 3: Encryption key generations

	AM	B_1	B_2	B_3	Encryption key
ω_1	$y_{AM_1} = g^{s_{AM_1}}$	$y_{1,1} = g^{s_{1,1}}$	$y_{2,1} = g^{s_{2,1}}$	$y_{3,1} = g^{s_{3,1}}$	$Y_1 = y_{AM_1} \times y_{1,1} \times y_{2,1} \times y_{3,1}$
ω_2	$y_{AM_2} = g^{s_{AM_2}}$	$y_{1,2} = g^{s_{1,2}}$	$y_{2,2} = g^{s_{2,2}}$	$y_{3,2} = g^{s_{3,2}}$	$Y_2 = y_{AM_2} \times y_{1,2} \times y_{2,2} \times y_{3,2}$
ω_3	$y_{AM_3} = g^{s_{AM_3}}$	$y_{1,3} = g^{s_{1,3}}$	$y_{2,3} = g^{s_{2,3}}$	$y_{3,3} = g^{s_{3,3}}$	$Y_3 = y_{AM_3} \times y_{1,3} \times y_{2,3} \times y_{3,3}$
ω_4	$y_{AM_4} = g^{s_{AM_4}}$	$y_{1,4} = g^{s_{1,4}}$	$y_{2,4} = g^{s_{2,4}}$	$y_{3,4} = g^{s_{3,4}}$	$Y_4 = y_{AM_4} \times y_{1,4} \times y_{2,4} \times y_{3,4}$
ω_5	$y_{AM_5} = g^{s_{AM_5}}$	$y_{1,5} = g^{s_{1,5}}$	$y_{2,5} = g^{s_{2,5}}$	$y_{3,5} = g^{s_{3,5}}$	$Y_5 = y_{AM_5} \times y_{1,5} \times y_{2,5} \times y_{3,5}$
ω_6	$y_{AM_6} = g^{s_{AM_6}}$	$y_{1,6} = g^{s_{1,6}}$	$y_{2,6} = g^{s_{2,6}}$	$y_{3,6} = g^{s_{3,6}}$	$Y_6 = y_{AM_6} \times y_{1,6} \times y_{2,6} \times y_{3,6}$

Table 4: Bids and decryption key generations

	B_1	B_2	B_3	Decryption key
ω_1	$\{s_{1,2}\}_{Y_1}$	$\{s_{2,2}\}_{Y_1}$	$\{s_{3,2}\}_{Y_1}$	$S_1 = s_{AM_1} + s_{1,1} + s_{2,1} + s_{3,1}$
ω_2	$\{s_{1,3}\}_{Y_2}$	$\{s_{2,3}\}_{Y_2}$	$\{proof(s_{3,3})\}_{Y_2}$	$S_2 = s_{AM_2} + s_{1,2} + s_{2,2} + s_{3,2}$
ω_3	$\{s_{1,4}\}_{Y_3}$	$\{s_{2,4}\}_{Y_3}$	Random bid in correct form	B_3 and AM must collude to recover S_3
ω_4	$\{s_{1,5}\}_{Y_4}$	$\{proof(s_{2,5})\}_{Y_4}$	Random bid in correct form	B_3 and AM must collude to recover S_4
ω_5	$\{proof(s_{1,6})\}_{Y_5}$	Random bid in correct form	Random bid in correct form	B_2, B_3 and AM must collude to recover S_5
ω_6	Random bid in correct form	Random bid in correct form	Random bid in correct form	All participants must collude to recoverS_6

In the ring signature generation procedure, e_k is computed by bidder B_i according to $e_j(j = 1, \cdots, k-1, k+1, \cdots, d)$, which are chose randomly from Z_q. For the determinate m_i and $p_i^{r_{AM} r_T}$, $e_1, e_2, \cdots, e_d$ have q^d possible values, whereas c_1 is determined according to m_i and $e_1, e_2, \cdots, e_d$. Therefore, it is impossible to determine who among the possible signers the actual one is. Under the circumstance that nobody can match $p_i^{r_{AM} r_T}$ along with p_i, actual signer won't be found even if all private keys are leaked because ring signature are unconditionally anonymous.

Non-repudiation: No bidder can deny he had submitted his bid.

Despite the bidders send their bids to AM through anonymous connection, all bidders have generated ring signature on their bids. So the malicious bidder cannot conceal his own identity. During the Dispute protocol, T can compute $p_i^{r_{AM} r_T}$ and identify the malicious bidder by comparing it with $\{p_1^{r_{AM} r_T}, \cdots, p_d^{r_{AM} r_T}\}$, where r_{AM} and r_T are generated and kept secure in the Initial phase by AM and T respectively.

Unforgeability: In our protocol nobody can impersonate any other bidder to make a bid.

If an outside attacker wants to forge other participant's bid, it must gain r_{AM} and r_T by decrypt $Encode(r_T, L)$ and $Encode(r_{AM}, L)$, that is to say, this attacker must be one member in $L = \{y_1, y_2, \cdots, y_d\}$. So anyone out of L cannot forge the ring signature because they cannot gain r_{AM} and r_T. Furthermore, if participant B_i in L wants to forge B_k's bid, it must know r_k (which is generated in Initial phase and only knew by B_k) to generate c_1 satisfying the ring equation during the ring signature generating procedure. So no bidder can pretend to be other bidders due to the unforgeability of bidder's ring signature.

Correctness: The winning bid is indeed the highest bid.

In the opening phase, an honest bidder B_i publishes $s_{i,1} = \log_g y_{i,1}$ so that $S_1 = \log_g Y_1$ can be reconstructed. So the encryption key chain starts correctly and the bids at ω_1 can be opened. The bids of the honest bidder B_i with all the biddable prices are generated as follows:

1) At a price ω_j that is higher than his evaluation, the bid is $s_{i,j+1}$ satisfying $y_{i,j+1} = g^{s_{i,j+1}}$.

2) At a price ω_j that is equal to his evaluation, the bid is $E_{Y_j}(proof(s_{i,j+1}))$.

3) At a price ω_j that is lower than his evaluation, the bid is a random value. Otherwise, bids are opened and the decrypted bids are $s_{i,j+1} = \log_g y_{i,j+1}$ for $i = 1, 2, \cdots, n$. So $S_{j+1} = \log_g Y_{j+1}$ can be reconstructed, that is to say, the encryption key chain extends correctly one step downward and the bids at ω_{j+1} can be opened. After the opening phase, AM and all bidders can be convinced that the winner satisfies all conditions. As a result, AM and bidders cannot get any information of bids lower than the winning bid unless all of them collude.

Robustness: Malicious cheating and crashing can be recovered.

The auctioneer can continue the protocol by eliminate cheating bidders through the execution of the dispute protocol, that is, cheaters cannot make any corruption at all.

Fairness: It is illustrated that before the opening phase, no bids are revealed.

Opening bids require the first decryption key S_1 that is shared among all bidders and the AM. Therefore,

Table 5: Computation and communication cost (exponentiations) of our protocol

Computational cost of a bidder(exponentiations)	$4l + 3d + 1$
Bid length	$1024bits$
Communication cost of a bidder	$1024(3l + 7d + 7)bits$

no one can disclose any information of bids unless all bidders open their shares $s_{1,1}, \cdots, s_{n,1}$ after confirming that the bidding procedure is closed.

Bid Privacy: All bidding prices except the winning price is not revealed to anyone including the AM.

If the bidder B_i with his bid ω_i is the winner, he does not disclose $s_{i,j+1}$ but $proof(s_{i,j+1})$. Therefore, AM cannot get any information of S_{j+1} and decrypt the subsequent bids.

Public verifiability: It is public verifiable that the price of the successful bid is higher than any other bids.

In our protocol, anyone can simulate the procedure to open bids using the information on the BBS. Since all the information necessary to decide the auction result is published on the BBS, anyone can verify the auction result. These decryption keys are available after the execution of opening phase, since they are published by AM during the opening phase.

4.2 Efficiency Analysis

In our protocol, the round complexity between a bidder and the auctioneer is only four (initial phase, pre-bidding phase, bidding phase and the beginning of the opening phase). In order to calculate efficiency, the parameter l and $d(d \leq n)$ are used to denote the number of biddable prices and the number of public keys in the generation of ring signature respectively. The efficiency of ring signature depends on d, the number of ring members. The computation and communication of ring signature will increase with the expansion of the length of d. But it is also obvious that with the increasing of d's length, the anonymous scope will become more and more wide. In addition, integer length of 1024 bits is assumed for all the cryptographic primitives. Table 5 demonstrates the computation and communication efficiencies of the bidder.

5 Conclusions

In this paper, we proposed an anonymous sealed-bid auction protocol based on the ring signature and verifiable encryption. First, one achievement of our protocol is non-repudiation of bidders while reserving its anonymity. Second, any information about the bid price will not be leaked except the final winning bidder. Third, our protocol is quite efficient since a bidder takes a part only at the beginning. We believe that this low complexity makes our proposed protocol fit in a large scale auction with respect to both the number of bidders and possible available prices.

Acknowledgments

This work was supported by the High Technology Research and Development Program of China(No. 2006AA01Z428) and the National Natural Science Foundation of China(No.60673075). The authors are grateful to the anonymous reviewers for valuable comments.

References

[1] M. Abe, and K. Suzuki, "M+1-st price auction using homomorphic encryption," *Public Key Cryptography*, vol. 72, pp. 115-124, 2002.

[2] F. Brandt, "How to obtain full privacy in auctions," *International Journal of Information Security*, vol. 5, no. 4, pp. 201-216, 2005.

[3] F. Brandt, and T. Sandholm, "Efficient privacy-preserving protocols for multi-unit auctions," *Financial Cryptography and Data Security: 9th International Conference (FC 2005)*, pp. 298-312, Roseau, Springer-Verlag, 2005.

[4] D. Chaum, and E. Heyst, "Group signatures," *Eurocrypt '91*, pp. 257-265, 1991.

[5] M. K. Franklin, M. K. Reiter, and E. Jernigan, "The design and implementation of a secure auction service," *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 302-312, 1996.

[6] A. Juels, M. Szydlo, and A Two-Server, "Sealed-bid auction protocol," *Financial Cryptography*, pp. 72-86, 2002.

[7] H. Kikuchi, M. Harkavy, and D. TYGAR, "Multi-round Anonymous Auction Protocols," *Special Issue on Internet Technology and Its Applications*, pp. 62-69, 1998.

[8] H. Lipmaa, N. Asokan, and V. Niemi, "Secure vickrey auctions without threshold trust," *Financial Cryptography*, pp. 87-101, 2002.

[9] D. Naccache, and J. Stern, "A New public key cryptosystem based on higher residues," *ACM Conference on Computer and Communications Security*, pp. 59-66, 1998.

[10] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," *Asiacrypt '01*, pp. 552-565, 2001.

[11] D. Rolli, M. Conrad, D. Neumann, and C. Sorge, "Distributed ascending proxy auction: A cryptographic approach," *Wirtschaftsinformatik*, vol. 48, no. 1, pp. 7-15, 2006.

[12] K. Sako, "An auction protocol which hides bids of losers," *Public Key Cryptography*, pp. 422-432, 2000.

[13] K. Sakurai, and S. Miyazaki, "A bulletin-board based digital auction scheme with bidding down strategy," *International Workshop on Cryptographic Techniques and E-Commerce*, pp. 180-187, 1999.

[14] D. Shih, H. Huang, D. C. Yen, "A secure reverse vickrey auction scheme with bid privacy," *Informaction Sciences*, vol. 176, no. 5, pp. 550-564, 2006.
[15] D. Shih, C. Cheng, and J. Shen, "A secure protocol of reverse discriminatory auction with bid privacy," *ICMB*, pp. 52, 2007.
[16] K. Suzuki, K. Kobayashi, and Hikaru Morita, "Efficient sealed-bid auction using hash chain," *ICISC*, pp. 183-191, 2000.
[17] K. Suzuki, and M. Yokoo, "Secure generalized Vickrey auction using homomorphic encryption," *Proceedings of 7th FC Conference*, LNCS 2742, pp. 239-249, Springer-Verlag, 2003.
[18] C. A. Waldspurger, T. Hogg, B. A. Huberman, J. O. Kephart, and W. S. Stornetta, "Spawn: A distributed computational economy," *IEEE Transactions on Software Engineering*, vol. 18, no. 2, pp. 103-117, 1992.
[19] Y. Watanabe, and H. Imai, "Reducing the round complexity of a sealed-bid auction protocol with an off-line TTP," *ACM Conference on Computer and Communications Security*, pp. 80-86, 2000.

Hu Xiong is a Ph.D. candidate in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. He received his MS degree in Mathematics from University of Electronic Science and Technology of China, 2004. His research interests include: information security and cryptography.

Zhiguang Qin is a professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC). He received his Ph.D. degree from UEST in 1996. His research interests include: network computing and information security.

Fagen Li received his Ph.D. degree in Cryptography from Xidian University, Xi'an, P.R. China in 2007. He is now a lecture in the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, P.R. China. His recent research interests include cryptography and network security.