SCIS 2003 The 2003 Symposium on
Cryptography and Information Security
Hamamatsu,Japan, Jan.26-29,2003
The Institute of Electronics,
Information and Communication Engineers

Yet Another Strong Sealed-Bid Auctions

Wooseok Ham * tarzan92@icu.ac.kr

Kwangjo Kim * kkj@icu.ac.kr

Hideki Imai † imai@iis.u-tokyo.ac.jp

Abstract— In this paper, we propose two sealed-bid auction protocols that one is based on RSA problem and the other on Discrete Logarithm problem. The peculiar characteristics of new protocols are non-repudiation of bidders preserving their anonymity and the reduced computational complexity to $\mathcal{O}(n \log_2 P)$, where n and P denote the number of bidders and the number of possible bidding prices, respectively. Our protocols have additional characteristics such as privacy, publicly verifiability, fairness and walk-awayness. We claim that this low complexity is preferable in a large scale auction.

Keywords: Sealed-bid auction, RSAP, DLP, non-reputation, anonymity, hash function

1 Introduction

On-line auction is an efficient method to buy and sell the items on the Internet. In the cryptographic literature, auction is also an attractive topic for the researchers to design a secure and practical protocol employing cryptographic primitives. To date, many researchers have studied and published various and outstanding auction protocols [1, 3, 4, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17]. As there are a variety of auction styles such as *English, Dutch, Sealed-Bid, Vickrey, and M+1, etc.*(refer to [2] for details) 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 *Sealed-Bid auction* in which a bidder commits his bid with which he is willing to pay on the items without disclosure 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.

1.1 Motivations

From the previous researches, we have figured out there exist two problems which can deteriorate the security and efficiency 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 casted 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 his assistance. Some works[9, 10, 16] treated non-repudiation as a mandatory requirement. But, [16] does not meet anonymity so that these protocols raise privacy problem. [9] cannot resolve tie-breaking which compromises non-repudiation. In others [1, 4, 7, 10, 11, 12, 15, 17], they seems 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.

Definition 1.1 *Anonymous and non-repudiable auction* is the bid is committed to the auctioneer anonymously, however,the winner is explicitly identified without bidder's aid at the end of the auction.

The other problem is *to reduce the computational complexity to the size* $\log P$ in the winner resolution, where P is the number of possible bidding prices. Abe and Suzuki have stated this issue as well in [1]. If the complexity of an auction protocol is proportional to $\log P$, the protocol is able to achieve much higher efficiency as the bid range increases. Naor, Pinkas and Sumner [12] introduced a protocol proportional to $\log P$ in a rough estimation, but a bidder's *on-line* communication load is very high to proceed bit by bit oblivious transfer.

1.2 Our results

Following the rule of sealed-bid auction, we suggest winner-identifiable anonymous auction protocols; that is to say, the auctioneer knows identity of the winner at the end of the protocol run without additional interactions with the winning bidder. Thus the winner cannot repudiate the fact of his bidding although he bid anonymously. Furthermore, the complexity is roughly $\mathcal{O}(n \log_2 P)$, where n is the number of bidders. We propose two auction protocols: one is based on RSA Problem(hereinafter, RSAP) and the other is Discrete Logarithm Problem(hereinafter, DLP).

* International Research center for Information Security (IRIS) Information and Communications University (ICU) 58-4, Hwaam-dong, Yuseong-gu, Daejeon, 305-732, Korea.

† Institute of Industrial Science, Univ. of Tokyo, Meguro-ku, Tokyo, 153-8505, Japan.

1.3 Organization

In Section 2, we examine related works in brief. Section 3 explains our model, assumptions and requirements as preliminaries for the rest of our paper. Section 4 describes our proposed protocol based on RSAP in detail and Section 5 gives a protocol based on DLP. The security and performance aspects of the proposed protocols are discussed in Section 6. We finalize this paper with conclusion and further works in Section 7.

2 Related Works

Recently, lots of works employing different cryptographic primitives have been done in the secure auction area. Here, we limit our observation on the previous works to *Sealed-bid* auction only for simplicity.

Franklin and Reiter [6] presented a sealed-bid auction protocol based on threshold secret sharing of bidding price. Their scheme also used verifiable signature sharing to prohibit a bidder from repudiating but doesn't protect the privacy of losers and losing bidders. Naor, Pinkas and Sumner [12] proposed privacy preserving auction with secure function evaluation and proxy oblivious transfer, which is improved by Juels and Szydlo [7] to address security bleaches by introducing verifiable proxy oblivious transfer. However, the scheme is not publicly verifiable. Cachin [4] used homomorphic encryption with the Φ-hiding assumption and an oblivious third party. The main problem of this scheme is that it cannot resolve the winning price except the winner, and also doesn't support non-repudiation. Suzuki, Kobayashi and Morita [16] proposed an efficient scheme adopting distribution of hash chain results to auctioneers. But, for anonymity, each bidder should register to a registration center and get a suitable pseudonym from the center. Kikuchi, Harkavy and Tygar[9] explored the property of polynomial interpolation. Interpolation with the winning polynomial results in the identity of the winner. However, their scheme cannot resolve tie-breaking and increases the number of auctioneers proportional to the possible bidding range.

$(M+1)$ auction schemes proposed by Abe and Suzuki [1] and Kikuchi [10] can be converted to fit in sealed-bid auction with small variation. However, Abe and Suzuki's scheme seems to be inefficient in a sense that it makes use of bidder's several proofs and mixing. Kikuchi's protocol addressed non-repudiation, but, as in [9], large number of auctioneers are necessary for the wide range of bidding prices.

3 Sealed-Bid Auction

3.1 Our model and Assumptions

We focus on sealed-bid auction which can be modelled as consisting of three main phases: BID, Opening and Announcement. There are n bidders($= B_1, \ldots, B_n$), one master auctioneer(A_M), and m sub-auctioneers($= A_1, \ldots, A_m$). The role of master auctioneer is to organize each auction run and announces the bid result(*i.e.*, the winner and the winning price) at the end of the protocol run. He receives bids from bidders in a predetermined form (BID phase) and distributes the bids to m sub-auctioneers for the selection of the winning price and winner(s) (Opening phase) then publishes the result(Announcement phase). The channels between master auctioneer and sub-auctioneers are supposed to be secure and reliable, which means all messages transferred between two entities finally reach to the communicating party without compromising. We suppose that auctioneers doesn't collude each other and misbehave. Our scheme is based on a public key cyrptosystem, namely every entity has its own secret key(SK) and public key(PK). Here, note that PK and SK of A_M are not static keys but ephemeral keys. He reveals SK after the bid. Bidding price(Bp) is denominated as a binary string of size m. Each sub-auctioneer represents each bit in bidding price, *i.e.*, bidders have 2^m possible bid choices and there is m sub-auctioneers. Notice that we allow a sub-auctioneer to know a little information such as bid statistics at his position.

$\mathcal{KG}$ is the key generation algorithm that takes a random string 1^k as an input, where k is a security parameter, and returns a *key* pair depending on the underlying encryption system. $\mathcal{H}$ is a collision resistant one-way hash function which takes an arbitrary string and outputs a uniformly distributed random string of a fixed size. Symbol $\|$ denotes concatenation of two strings through this paper. $\mathsf{DSig}^{\mathsf{n}}_{\mathsf{X}}(\cdot)$ is the digital signature generated by entity X_n on $(\cdot)$ using his static secret key.

3.2 Requirements

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

Privacy Losing bidders and bids should be kept in secret even to the auctioneer except the winning bid and the winner.

Anonymity No one can identify the bidder and the bidding price from a bid.

Non-repudiation The winner cannot repudiate his bidding at the winning price.

Publicly Verifiability Any one can verify the winning price and the winner which are decided correctly.

Fairness The protocol run is terminated in the predefined period and all accepted bids is dealt with in a fair way.

Walk-Awayness A bidder doesn't need to do any other action after bidding.

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

Definition 3.1 If a sealed-bid auction accomplishes all requirements listed above, we say a *strong sealed-bid auction.*

4 Proposed Protocol 1

4.1 Initialization

This protocol is based on RSA problem. n is a composite number subject to $n = pq$, where p and q are sufficiently large distinct primes and Euler phi function $\phi(n) = (p-1)(q-1)$. We suppose that all bidders and auctioneers have the key generation algorithm $\mathcal{KG}$. Master auctioneer calls $\mathcal{KG}$ and receives his RSA key tuple (n_A^M, e_A^M, d_A^M), where each term denotes a modulus, public and secret keys, respectively. $d_A^M(= SK)$ is kept in safe. m sub-auctioneers execute $\mathcal{KG}$ and each sub-auctioneer gets his own key tuple (n_A^j, e_A^j, d_A^j) on the condition that $n_A^M < n_A^1 < \ldots < n_A^m$. PK set of all auctioneers $\mathsf{PKS} = \{(n_A^M, e_A^M), (n_A^1, e_A^1), \ldots, (n_A^m, e_A^m)\}$ is announced in public by master auctioneer before the bid runs. Each bidder B_i obtains his RSA key tuple (n_B^i, e_B^i, d_B^i) from $\mathcal{KG}$, where $n_B^i < n_A^M$. PK of each bidder, (n_B^i, e_B^i), is publicly known. In order to protect our protocol against unexpected system failure in any sub-auctioneer, we may adopt key distribution method working in a threshold manner among auctioneers.

4.2 BID Phase

The i-th bidder B_i carries out the following steps to commit his bid:

B1. Gets PKS.

B2. Decides his bidding price $\mathsf{Bp} = (b_m \ldots b_1) \in_R \{0,1\}^m$.

B3. Executes the following B–Compute algorithm:

```
Algo. B–Compute (PKS, $d_B^i$, Bp)
$EID \leftarrow [\mathcal{H}(ID_B^i \| Seq)]^{d_B^i} \bmod n_B^i$
$\sigma_M^i \leftarrow [ID_B^i \| EID]^{e_A^M} \bmod n_A^M$
$\sigma_0^i \leftarrow \sigma_M^i$
for $1 \le j \le m$
   if $b_j = 1$ then
      $\sigma_j^i \leftarrow [\sigma_{j-1}^i + 1]^{e_A^j} \bmod n_A^j$
      $S_j^i \leftarrow \mathcal{H}(\sigma_{j-1}^i \| e_A^j)$
   else
      $\sigma_j^i \leftarrow [\sigma_{j-1}^i]^{e_A^j} \bmod n_A^j$
      $S_j^i \leftarrow \mathcal{H}(\sigma_{j-1}^i)$
$S_M^i \leftarrow \mathcal{H}(\sigma_M^i \| \sigma_m^i \| Seq)$
Returns $(\sigma_m^i, S_M^i, S_m^i, \ldots, S_1^i)$.
```

B4. Sends $(\sigma_m^i, S_M^i, S_m^i, \ldots, S_1^i)$ to A_M.

Seq is the unique number of the participating auction, which works as a nonce to ensure uniqueness. Notice that b_1 is the least significant bit(LSB) in Bp and computed from LSB in B–Compute algorithm. Whenever a bit in Bp equals 1, PK of the sub-auctioneer at that place is powered to the previous result. S_j^i will play a role of indicator to verify whether or not the bid is committed at this bit. The communication between a bidder and master auctioneer occurs just *once* to transfer the encoded bid tuple.

4.3 Opening Phase

When the bidding time is over, master auctioneer closes the bidding session and collaborates with sub-auctioneers to resolve the winner and the winning price. Only auctioneers communicate according to the order in this phase. Observing the following steps, each sub-auctioneer A_j publishes the winning bit b_j^W (1 *or* 0) and transfers returned results to A_{j-1}. Running steps are as follows:

O1. A_M publishes all (σ_m^i, S_M^i) with $\mathsf{DSig}_\mathsf{A}^\mathsf{M}(\mathcal{H}(\sigma_m^1 \| S_M^1 \| \ldots \| \sigma_m^n \| S_M^n))$.

O2. A_M distributes all S_j^i to each A_j, for $1 \le i \le n$.

O3. A_j publishes all received S_j^i with $\mathsf{DSig}_\mathsf{A}^\mathsf{j}(\mathcal{H}(S_j^1 \| \ldots \| S_j^n))$.

O4. A_M transfers $(\beta_m^1(= \sigma_m^1), \ldots, \beta_m^n(= \sigma_m^n))$ to A_m.

O5. From A_m to A_1, each sub-auctioneer A_j runs A–Resolution algorithm and forwards the returned value to the next sub-auctioneer A_{j-1} at the end of the algorithm:

```
Algo. A–Resolution ($d_A^j$, $(\beta_j^i, \ldots, \beta_j^n)$,$(S_j^1, \ldots, S_j^n)$)
 for $1 \le i \le n$
     $\beta_{j-1}^i \leftarrow ([\beta_j^i]^{d_A^j} - 1) \bmod n_A^j$
     $S_j^{i'} \leftarrow \mathcal{H}(\beta_{j-1}^i \| e_A^j)$
 if any $S_j^i = S_j^{i'}$ then announces $b_j^W = 1$
 else $b_j^W = 0$
   for $1 \le i \le n$
     $\beta_{j-1}^i \leftarrow \beta_{j-1}^i + 1$
 Publishes $\mathsf{DSig}_\mathsf{A}^\mathsf{j}(\mathcal{H}(\beta_{j-1}^1 \| \ldots \| \beta_{j-1}^n \| 1\ or\ 0))$
 Returns $(\beta_{j-1}^1, \ldots, \beta_{j-1}^n)$.
```

O6. A_1 transfers all β_0^i subject to $S_1^i = S_1^{i'}$, if $b_1 = 1$; otherwise, computes $S_1^{i'} \leftarrow \mathcal{H}(\beta_0^i)$ for $1 \le i \le n$, then sends all β_0^i subject to $S_1^i = S_1^{i'}$ to A_M.

Note that the order of opening is consecutive from the m-th sub-auctioneer to the 1st sub-auctioneer. In A–Resolution algorithm, the j-th sub-auctioneer first decrypts all bids and examines if at least one bidder bid at the j-th bit by matching $S_j^{i'}$ to S_j^i which is delivered from A_M in advance. Provided that bidders and auctioneers work correctly, at least one β_0^i that is sent to A_M will have the identical form of σ_M^i in BID phase. In terms of the signature scheme, several provably secure signature schemes (refer to [14] for details) could be a candidate to sign the message in our protocol. The last concatenated bit (1 *or* 0) in $\mathsf{DSig}_\mathsf{A}^\mathsf{j}$ is the winning bit b_j^W announced by the j-th sub-auctioneer. $\mathsf{DSig}_\mathsf{A}^\mathsf{j}$ in A–Resolution algorithm will be an evidence when any disputes happens related to auctioneers's malfunctioning. We assume that all digital signatures are generated using the signer's static private key.

Note that a few trivial modifications and policies can enhance performance of our algorithm. These points will be discussed in the full paper.

4.4 Announcement Phase

In this phase, A_M performs alone the following steps to officially announce the winning bid and authenticate the winner(s):

A1. Aggregates all winning bits announced by each sub-auctioneer, $\mathsf{Bp}^{\mathsf{Win}} = (b_m^W \dots b_1^W)$.

A2. Decrypts all β_0^i received from the 1st sub-auctioneer, $\beta_M^i \leftarrow \left[\beta_0^i\right]^{d_A^M} \bmod n_A^M$, and extracts (ID_B^i, EID) from β_M^i.

A3. Gets PK of ID_B^i from the public key repository and computes $\beta_m^{i'}$ using β_M^i as σ_m^i in B–Compute algorithm taking PKS and $\mathsf{Bp}^{\mathsf{Win}}$ as inputs.

A4. Verifies winner(s): $\mathcal{H}(ID_B^i \| Seq) \overset{?}{=} EID^{e_B^i} \bmod n_B^i$ and $S_M^i \overset{?}{=} \mathcal{H}(\beta_M^i \| \beta_m^{i'} \| Seq)$.

A5. Announces the winner(s) ID_B^W and $\mathsf{Bp}^{\mathsf{Win}}$ with $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{M}}$ on them and publishes his ephemeral secret key d_A^M together.

At A2, note that β_0^i is identical to σ_M^i in BID phase.

5 Proposed Protocol 2

5.1 Initialization

This protocol makes use of the intractability of discrete logarithm problem. Each bidder B_i has his static key tuple $(p, g, x_B^i, y_B^i (= g^{x_B^i}))$. A_M and every A_j execute $\mathcal{KG}$ and receive their ephemeral key tuple $(p, g, x_A^M, y_A^M (= g_1^{x_A^M}))$ and $(p, g, x_A^j, y_A^j (= g^{x_A^j}))$, respectively. x and y denote SK and PK, on each. These tuples match to the ElGamal encryption[5] setting, although we don't make use of ElGamal encryption through the paper. Here, another constraint is given in generating secret keys of all entities: $\gcd(SK, \phi(p)) = 1$. This policy should be embedded in $\mathcal{KG}$ beforehand. Note that auctioneers' keys are not static but ephemeral. $\mathsf{PKS} = \{y_A^M, y_A^m, \dots, y_A^1\}$ and all PK of bidders, y_B^i, are published as in our protocol 1. We regard PK of bidder represents his identity assuming PK_B is certified by the certification authority(CA), *i.e.* $PK_B = ID_B$.

When the above initialization is completed, BID, Opening, and Announcement phases are almost same as in our protocol 1. Hence, we just describe main steps without further details. Notice that some small variations in algorithms and steps are made.

5.2 BID Phase

In order to bid, a bidder B_i performs the following steps:

B1. Gets PKS.

B2. Decides his bidding price $\mathsf{Bp} = (b_m \dots b_1) \in_R \{0,1\}^m$.

B3. Executes the following B–Compute algorithm:

```
Algo. B–Compute (PKS, $x_B^i$, Bp)
  $a, b \in_R \mathbf{Z}_p^*$
  $\tau_B^i \leftarrow (Seq + x_B^i)/a$
  $\sigma_M^i \leftarrow \left[y_A^M\right]^a$
  $\alpha_B^i \leftarrow g^b$
  $\sigma_0^i \leftarrow \sigma_M^i$
  for $1 \leq j \leq m$
    $\delta_j^i \leftarrow \left[y_A^j\right]^b$
    if $b_j = 1$ then
      $\sigma_j^i \leftarrow (\sigma_{j-1}^i + 1)\delta_j^i$
      $S_j^i \leftarrow \mathcal{H}(\sigma_{j-1}^i \| \delta_j^i)$
    else
      $\sigma_j^i \leftarrow \sigma_{j-1}^i \delta_j^i$
      $S_j^i \leftarrow \mathcal{H}(\sigma_{j-1}^i)$
  $S_M^i \leftarrow \mathcal{H}(\sigma_M^i \| \sigma_m^i \| \tau_B^i \| \alpha_B^i \| Seq)$
  Returns $(\sigma_m^i, \tau_B^i, \alpha_B^i, S_M^i, S_m^i, \dots, S_1^i)$.
```

B4. Sends $(\sigma_m^i, \tau_B^i, \alpha_B^i, S_M^i, S_m^i, \dots, S_1^i)$ to A_M.

5.3 Opening Protocol

O1. A_M publishes all $(\sigma_m^i, \tau_B^i, \alpha_B^i, S_M^i)$ with $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{M}}$ $(\mathcal{H}(\sigma_m^1 \| \tau_B^1 \ \| \alpha_B^1 \| S_M^1 \| \dots \| \sigma_m^n \| \tau_B^n \| \alpha_B^n \| S_M^n))$.

O2. A_M distributes all (S_j^i, α_B^i) to each A_j, where $1 \leq i \leq n$.

O3. A_j publishes all received (S_j^i, α_B^i) with $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{j}}$ $(\mathcal{H}(S_j^1 \| \alpha_B^1 \| \dots \| \ S_j^n \| \alpha_B^n))$.

O4. A_M transfers $(\beta_m^1 (= \sigma_m^1), \dots, \beta_m^n (= \sigma_m^n))$ to A_m.

O5. From A_m to A_1, each sub-auctioneer A_j runs A–Resolution algorithm and forwards the returned value to the next sub-auctioneer A_{j-1} at the end of the algorithm:

```
Algo. A–Resolution ($x_A^j, (\beta_j^1, \dots, \beta_j^n), ((S_j^1, \alpha_B^1),$
    $\dots, (S_j^n, \alpha_B^n)))$
  for $1 \leq i \leq n$
    $\lambda_j^i \leftarrow \left[\alpha_B^i\right]^{x_A^j}$
    $\beta_{j-1}^i \leftarrow (\beta_j^i / \lambda_j^i) - 1$
    $S_j^{i'} \leftarrow \mathcal{H}(\beta_{j-1}^i \| \lambda_j^i)$
  if any $S_j^i = S_j^{i'}$ then announces $b_j^W = 1$
  else $b_j^W = 0$
   for $1 \leq i \leq n$
    $\beta_{j-1}^i \leftarrow \beta_{j-1}^i + 1$
  Publishes $(\lambda_j^1, \dots, \lambda_j^n)$ and $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{j}}$ $(\mathcal{H}(\beta_{j-1}^1$
     $\| \lambda_j^1 \ \| \dots \| \beta_{j-1}^n \ \| \lambda_j^n \| 1 \ or \ 0))$
  Return $(\beta_{j-1}^1, \dots, \beta_{j-1}^n)$.
```

O6. A_1 transfers all β_0^i subject to $S_1^i = S_1^{i'}$, if $b_1 = 1$; otherwise, computes $S_1^{i'} \leftarrow \mathcal{H}(\beta_0^i)$, where $1 \leq i \leq n$, and sends all β_0^i subject to $S_1^i = S_1^{i'}$ to A_M.

5.4 Announcement Protocol

A1. Aggregates all announced winning bits by each sub-auctioneer, $\mathsf{Bp}^{\mathsf{Win}} = (b_m^W \dots b_1^W)$.

A2. Computes $\beta_m^{i'}$ using β_M^i as σ_m^i in B–Compute algorithm taking PKS, λ_j^i and $\mathsf{Bp}^{\mathsf{Win}}$ as inputs.

A3. Verifies winner(s): $S_M^i \overset{?}{=} \mathcal{H}(\beta_M^i \| \beta_m^{i'} \| \tau_B^i \| \alpha_B^i \| Seq)$.

A4. Announces the winner(s) $ID_B^W (= \left[{\beta_M^i}^{(\tau_B^i / x_A^M)} \right] / g^{Seq} = g^{x_B^i})$ and $\mathsf{Bp}^{\mathsf{Win}}$ with $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{M}}$ on them and publishes his ephemeral secret key x_A^M together.

We claim that our two protocols can be extended to other public key cryptosystems with small modifications.

6 Evaluation

In this section, we give justifications on the requirements as stated before to show that our schemes are secure and efficient. We represents our proposed protocol 1 as P1 and protocol 2 as P2, respectively.

6.1 Security

Privacy During Opening and Announcement phase, only winning σ_m^i takes off the exponent at the place of each auctioneer; otherwise, becomes a garbage value. So it is obvious that as far as at least one sub-auctioneer is honest, no one can learn any knowledge on losers' identities and bidding prices from the losing bids.

Anonymity Multiple encryptions with PK of sub-auctioneers in P1 randomize the bidder's identity. In P2, no information could be obtained from τ_B^i. Collision-free hash function makes sure no relationship between S_M^i and B_i as well.

Non-repudiation In Announcement phase of P1, the verification step A4 requires the winner's public key. This process seems to be equivalent to the verification of digital signature signed by the winner so that the winner cannot repudiate the fact of his bidding. In P2, non-repudiation is achieved by both the properties of hash function and Diffie-Hellman problem. Hashed value of correct $(\sigma_M^i, \sigma_m^i, \tau_B^i, \alpha_B^i, Seq)$ only maps to S_M^i and the one who knows x_B^i and a is able to compute τ_B^i.

From above security discussions, we can get:

Theorem 6.1 *Our proposed protocols,* P1 *and* P2 *are anonymous and non-repudiable sealed-bid auctions.*

Publicly Verifiability This is straightforward as SK of master auctioneer and $\mathsf{Bp}^{\mathsf{Win}}$ would be opened.

Fairness By checking the issuing time of $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{M}}$ issued by master auctioneer, fair termination can be observed. Fairness in the operations done by sub-auctioneers could be observed from the correctness of $\mathsf{DSig}_{\mathsf{A}}^{\mathsf{j}}$,$\mathsf{Bp}^{\mathsf{Win}}$ and published values. Any loser is able to claim, if $\mathsf{Bp}^{\mathsf{Win}}$ is lower than his bid.

Walk-Awayness This property is explicit in our protocols. The winner is identified by interactions among auctioneers only.

Table 1: Security comparison

	[10]	[12]	[16]	Our protocols
Privacy	△	O	△	O
Anonymity	O	O	X	O
Non-repudiation	X	X	O	O
Publicly Verifiability	X	X	O	O
Fairness	O	O	O	O
Walk-Awayness	X	X	O	O

From above discussions and our embedded system setting, we can induce the following security for the bidding message:

Theorem 6.2 *As far as $\mathcal{KG}$ works with a sufficient security parameter as input and $\mathcal{H}$ generates collision-free outputs, bidding messages in both* P1 *and* P2 *are secure.*

Proof(Sketch). Our two key generation algorithms are based on RSAP and DLP, respectively. We, in general, believe that an attacker bounded to the polynomial time has negligible probability($\leq \frac{1}{2^k}$, approximately) in solving those two hard problems given a sufficient security parameter. In addition, $\mathcal{H}$ with collision-free and one-way properties makes the attacker not to recover or find the original value from the output. So,we can conclude that our schemes are equivalent to those two hard problems and secure.

Security comparison with some sealed-bid auction protocols is shown in **Table 1**. For consistency, we consider 1st-price auction in [10] and method 2 in [16]. Note that [16] provides the privacy of bids not bidders.

6.2 Performance

Remind that P is the number of possible bid choices, n is the number of bidders and $m(= \log_2 P$, in our setting) is the number of auctioneers. We feel that $m = 20$(over than 1 million dollars) is enough for the general auctions.

6.2.1 Computation

In terms of computation, we ignore computation overhead of master auctioneer, since it is quite small and dominated by that of sub-auctioneers. A bidder's computation in BID phase also is not expensive as it can be performed in *off-line* and computed with a little consumption of resources under the current computing power. Main computation overhead takes place in each sub-auctioneer to resolve the winner and the winning price: n RSA decryptions and hashings with two digital signatures(P1) and n modular exponentiations, n modular divisions and hashings with two digital signatures(P2). These computations dominate that in master auctioneer. Consequently, we can represent our

Table 2: Performance comparison

	Computation (Opening)	Communication ($B_i \to A$)
[10]	$\mathcal{O}(P)$	$(P+t)\mathsf{M}$
[12]	$\mathcal{O}(n\log_2 P)$	$(\log_2 P+2)\mathsf{M}$
[16]	$\mathcal{O}(mnP)$	$m\mathsf{M}$
Our protocols	$\mathcal{O}(n\log_2 P)$	P1: $1\mathsf{M}+(\log_2 P+1)\mathsf{H}$ P2: $3\mathsf{M}+(\log_2 P+1)\mathsf{H}$

computational complexity as asymptotically $\mathcal{O}(n\log_2 P)$ with small constant.

Table 2 shows performance comparison of main computation and communication overhead of the various auction protocols.

6.2.2 Communication

Only *one* transmission from B_i to A_M is enough to finish bid commitment. Each sub-auctioneer has *one* communication with A_M and A_{j-1}, individually, except that A_m and A_1 have one more with A_M.

In communication comparison of **Table 2** , M and H denote the output size of modulo operation and hashing, respectively. For the sake of consistency, we set log operation with the base 2. In [10], t is is a number of faulty auctioneers. We concentrates on the communication, a bidder to an auctioneer only, since this is a main bottleneck in protocols. We regard all protocols are able to use a master auctioneer as a proxy to communicate with other auctioneers since it is more practical. Notice that [10] and [16] should encrypt the transferring messages in that case. We claim that the sizes of message from B_i to A_M in our protocols are not serious under the current network environment.

From the the above security and performance discussions, we can get:

Theorem 6.3 *Our proposed protocols,* P1 *and* P2*, are strong sealed-bid auctions.*

7 Conclusions

We proposed two secure and efficient sealed-bid auction protocols based on the intractability of RSAP or DLP with collision-free and one-way hash function. One of main achievements is non-repudiation of bidders keeping anonymity. Another one is computational reduction to the complexity of $\mathcal{O}(n\log_2 P)$ even if it's not the first scheme that works with this complexity, but in a different way. Furthermore, the inner communication and computation among auctioneers are not expensive. We believe that this low complexity makes our proposed protocols fit in a large scale auction with respect to both the number of bidders and possible choices.

Extension to the multi-functional auction will be studied as further work. As stated in [11], it is also interesting to reduce the computational complexity to $\mathcal{O}(\log_2 n\log_2 P)$.

References

[1] M.Abe and K.Suzuki, M+1-st Price Auction Using Homomorphic Encryption, *Proc. of Public Key Cryptography '02*, LNCS 2274, pp.115–124, 2002.

[2] C.Boyd and W.Mao, Security Issues for Electronic Auctions, Hewlett Packard, HP Technical Report HPL–2000–90, 2000.

[3] O.Baudron and J.Stern Non-interactive Private Auctions, *Proc. of Financial Cryptography '01*, LNCS 2339, pp.364–377, 2001.

[4] C.Cachin, Efficient Private Bidding and Autions with an Oblivious Third Party, *Proc. of 6th ACM conference on Computer and Communications Security*, pp.120–127, 1999.

[5] T.Elgamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *Proc. of Crypto '84*, LNCS 0196, pp.10–18, 1985.

[6] M.K.Franklin and M.K.Reiter, The Design and Implementation of a Secure Auction Service, *IEEE Trans. on Software Engineering*, 22(5), pp.302–312, 1996.

[7] A.Juels and M.Szydlo, A Two-Server, Sealed-Bid Auction Protocol, To appear in *Proc. of Financial Cryptography '02*, 2002.

[8] M.Harkavy, J.Tygar and H.Kikuchi, Electronic Auctions with Private Bids, *Proc. of 3rd USENIX Workshop on Electronic Commerce*, pp.61–74, 1998.

[9] H.Kikuchi, M.Harkavy and J.D.Tygar, Multi-round Anonymous Auction Protocols, *Proc. of 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pp.62–69, 1998.

[10] H.Kikuchi, (M+1)st-Price Auction Protocol, *Proc. of Financial Cryptography '01*, LNCS 2339, pp.291-298, 2001.

[11] H.Lipmaa, N.Asokan, and V.Niemi, Secure Vickrey Auctions without Threshold Trust, To appear in *Proc. of Financial Cryptography '02*, 2002.

[12] M.Naor, B.Pinkas, and R.Summer, Privacy Preserving Auctions and Mechanism Design, *Proc. of ACM conference on E-commerce*, pp.129–139, 1999.

[13] K.Peng, C.Boyd, E.Dawson and K.Viswanathan, Robust, Privacy Protecting and Publicly Verifiable Sealed-Bid Auction, *Proc. of ICICS '02*, LNCS 2513, pp.147–159, 2002.

[14] D.Pointcheval and J.Stern, Security Arguments for Digital Siganture and Blind Signatures, *Jouranl of Cryptology*, Vol.13, No.3, pp.361–396, 2000.

[15] K.Sako, An Auction Protocol Which Hides Bids of Losers, *Proc. of Public Key Cryptography '00*, LNCS 1751, pp.422-432, 2000.

[16] K.Suzuki, K.Kobayashi, and H.Morita, Efficient Sealed-bid Auction using Hash Chain, *Proc. of ICISC '00*, LNCS 2015, pp.183–191, 2000.

[17] S.G.Stubblebine and P.F.Syberson, Fair On-line Auctions Without Special Trusted Parties, *Proc. of Financial Cryptography '99*, pp.230–240, 1999.