Reducing the Round Complexity of a Sealed-Bid Auction Protocol with an Off-Line TTP *

Yuji Watanabe
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minatoku, Tokyo
106-8558, Japan
mue@imailab.iis.u-tokyo.ac.jp

Hideki Imai
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minatoku, Tokyo
106-8558, Japan
imai@iis.u-tokyo.ac.jp

ABSTRACT

We present a new sealed-bid auction protocol that allows an auctioneer to determine the winning bid in a universally verifiable way and simultaneously prevents not only bidders but also an auctioneer from getting any useful information of bids of losers. We make use of a trusted third party(TTP) but in an *optimistic* sense[1][2], i.e., the TTP takes part in the protocol only if one bidder cheats or simply crashes. Previous schemes[3][4] require the bidder's help during opening procedures. On the other hand, our protocol is quite efficient since a bidder takes part only at the beginning. More importantly, our scheme is robust against cheating bidders; i.e. any deviation of bidders cannot prevent the auctioneer from determining the auction. A stratified distributed encryption-key chaining mechanism and a verifiable encryption protocol are employed as building blocks. To the best of our knowledge, this work is the first construction of a universally verifiable bid-privacy preserving sealed-bid auction protocol with an off-line TTP.

1. INTRODUCTION

Electronic auctions are a fundamental part of the electronic commerce technology. A sealed-bid auction is one in which secret bids are issued for an advertised item, and once the bidding period closes, the bids are opened and the winner is determined according to some publicly known rule (e.g. the highest bidder wins).

In [5], Franklin and Reiter present a protocol for a sealed-bid auction. Their protocol uses a set of distributed auctioneers and features an innovative primitive called verifiable signature sharing[6]. 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 the all bids to all auctioneers after the auction is decided. Consequently, a corrupted auctioneer can derive detailed information about the bidder's strategy. This is a serious drawback : if an auctioneer can observe bidder's behavior, he can find some trend of bidder's strategy and make use of it in analogous auction. Nevertheless, achieving universal verifiability of the winning bid, i.e., all bidders can be convinced that the winning bid is dealt with according to the rule, demands opening all bids including loser's bid.

Recent development of the researches regarding such privacy issues of the sealed-bid auction protocol are listed in Table 1. The first attempt to deal with such problem was done by Kikuchi, Harkavy and Tyger[7]. (Recently, Sako[8] pointed out that in their work, several problem remains, e.g. their scheme cannot deal with a tie case.) Several works present efficient solutions to cope with both hiding loser's bids and offering a universal verifiability of a winning bid. Roughly speaking, the schemes in [3][9][4] work as follows. A bidder sends commitment to his bid to the auctioneer, and once the bidding period closes, all bidders open the commitment from the highest bid one by one. Opening the commitment ends up when the winning bid is determined, so losing bids are never opened. Therefore, an auctioneer does not get any useful information except the winning bid since all these procedures cannot be performed without the bidder's help. As the commitment scheme, [3][9] uses a convertible undeniable signature, and [4] uses a hash chaining technique. However, the drawback of this approach is that all bidders have to take part in the protocol during opening bids. Simultaneously, Sako[8][10] shows another approach, in which a set of distributed auctioneers prepares a pair of encryption/decryption-key corresponding each biddable value in a distributed fashion (threshold cryptosystem[11] is employed), and bidder encrypts his bid with encryption-key corresponding to his bid. Once the bidding period closes, auctioneers decrypt the ciphertext with (distributed) decryption-key corresponding each bid from the highest biddable value one by one. Subsequent decryption proceeds unless the winning bid can be determined. After the auction is decided, a set of auctioneers cannot decrypt losing bids, even when up to a threshold of auctioneers are malicious. This protocol is quite efficient, but unfortunately, it has no fairness among bidders and auctioneers in the fol-

*This work was performed in part of Research for the Future Program (RFTF) supported by Japan Society for the Promotion of Science (JSPS) under contract no. JSPS-RFTF 96P00604 and also supported by Association of Radio Industries and Businesses (ARIB) under the Public Participation Program for Frequency Resources Development.

CCS '00, Athens, Greece.

lowing sense: a bidder has to rely on an uncertain evidence that more than a threshold of auctioneers are honest.

Recently, Cachin[12] proposed a different sealed-bid auction protocol which is constructed from a "millionaire's protocol," in which two parties want to determine who is richer without disclosing anything else about their wealth. His protocol employs two semi-trusted parties which are employed as auction servers, T and V. The server V chooses the random values for n instances of the private bidding protocol between every two parties. The bidders encrypt their bids, send them to the server V, but are not involved further. The server V determines the highest bid through n successive queries to the server T who obliviously compares two bids, but who does not learn anything about the bids. At the end, the server V learns a partial order of the bids, but not more. Another task by Naor et al.[13] introduced a simple architecture for preserving the pivacy of the bids of losers while maintaining communication and computational efficiency. They employed additional third party *auction issuer* that generates the programs (circuit) for computing the auctions but does not take an active part in the protocol. Their protocol ensures that, barring collusion between the auctioneer and the auction issuer, neither party gains any information about the bids, even after the auction is over. Moreover, bidders can verify that the auction was performed correctly.

Both [12] and [13], however, still have the same problem as [8][10], i.e., a bidder has to believe the absence of a collusion among the parties who open and sort the bids. We take a totally different trust model from all these schemes. For efficiently achieving the universal verifiability, the privacy of bids and the fairness among bidders and auctioneers, we adopt an *optimistic* approach, which was originally introduced by Asokan et al.[1][2]. It relies on the existence of a third trusted party but only invoked in the case of an exception. The protocol is *optimistic* since an auctioneer takes the risk of sharing a key for decrypting bids among bidders, optimistically hoping that all bidders will respond by sending the share in order to repudiate that his bid is the value corresponding decryption key. If a bidder wants to bid, he will respond by sending the proof of knowledge of his share without giving any information of the share itself. Therefore, After the winning bid is determined, auctioneer cannot get any information on the decryption-keys for subsequent opening. If a bidder does not reply as expected, the auctioneer asks the third party to resolve the dispute (this implies that sufficient evidence must be accumulated during the protocol to support the resolution of the dispute.) In order to guarantee that the dispute can be resolved, we use the technique of *verifiable encryption* (i.e., a way to encrypt the message under a designated public key and subsequently prove that the resulting ciphertext indeed contains such messages). Recently, Ateniese[14] shows efficient protocol for verifiable encryption of various types of cryptographic functions.

Consequently, our protocol results in a practical sealed-bid auction protocol that allows an auctioneer to determine the winning bid in a universally verifiable way and simultaneously prevents even an auctioneer from getting any useful information of bids of losers. Previous schemes[3][4] require the bidder's help during opening procedures. On the other hand, our protocol is quite efficient since a bidder takes a part only at the beginning. More importantly, our scheme is robust against cheating bidders; i.e., any deviation of bidders cannot prevent the auctioneer from determining the auction. To the best of our knowledge, this is the first construction of a universally verifiable sealed-bid auction protocol in an optimistic approach.

2. DEFINITION

2.1 Model and Definition

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 auction. At some 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 any publicly known, deterministic rule. When convenient, however, we assume that this rule dictates that the highest bidder be chosen as the winner.

The notations used in this paper are briefly described in Table 2. Let $\mathcal{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_N\}$ be a set of N bidders who take part in an auction and offer a price, and $\mathcal{A}$ be auctioneer who holds an auction and manages a bulletin board. We assume all bidders and auctioneer can produce their signature (denoted as $sig_{\mathcal{B}_i}$ and $sig_{\mathcal{A}}$, respectively.) Let $\mathcal{T}$ be an (off-line) third trusted party who resolves the dispute and $VE(x)$ be the verifiable encryption of x with $\mathcal{T}$'s public key (see section 2.2).

$\mathcal{W} = \{w_0, \ldots, w_l\}$, where $w_0 < \cdots < w_l$, be a set of $l+1$ biddable values, from which each bidder must choose his bid and submit it during the bidding period. Let us denote $\mathcal{B}_i$'s bid as θ_i. In the opening phase, the highest bidder, i.e., the bidder whose bid has the highest index, is determined as the winner.

The following parameters are used in the protocol. Let p and q be large primes such that $q|p-1$ and let g be an element of order q in Z_p^*. Let $H(.)$ denote an ideal collision resistant cryptographic hash function for Fiat-Shamir heuristic. We assume this function maps from the integer space to Z_q. Suppose $E(x, ek)$ is the discrete logarithm based encryption function of x with the public key $ek \in Z_q$, where $dk = \log_g ek$ is the decryption key to invert E. (p, q, g, H, E, ek) are public for all participants.

We assume that the encryption function E is semantically secure in order not to reveal any information of bids. Intuitively, a cryptosystem is semantically secure if, a passive attacker, who knows that one of just two possible messages has been encrypted, cannot yield any information about which of the two was actually encrypted by simply analyzing the ciphertext. This property can be achieved by padding the random number in a suitable way, as well as by using semantically secure public-key cryptosystem such as Cramer-Shoup cryptosystem[15].

We also assume the use of a bulletin board(BB) setting where participants read and write in authenticated manner. No one can cancel any information once written to the BB.

2.2 Verifiable Encryption

Given g^x, where g is the generator of a prime-order subgroup of Z_q^*, it is hard to compute x. Suppose, now, that $\mathcal{T}$ selects an appropriate group G of order n in which computing the discrete logarithm is an easy task, i.e., given an

Table 1: Comparison

	using technique	auctioneer(s)	hiding bids of losers	opener of bids
[5]	verifiable signature sharing	not trusted	No	auctioneer(s)
[7]	secret sharing	trusted	Yes/No	auctioneer(s)
[8][10]	(distributed) public-key crypto	trusted	Yes	auctioneer(s)
[3][9]	convertible undeniable signature	not trusted	Yes	bidder
[4]	hash chaining	not trusted	Yes	bidder
proposal	verifiable encryption	not trusted	Yes	auctioneer

Table 2: Notation

$\mathcal{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_N\}$	:	bidder ($\lvert\mathcal{B}\rvert = N$)
$\mathcal{A}$	:	auctioneer
$\mathcal{T}$	:	third trusted party (TTP)
$VE(s)$	:	verifiable encryption of s with $\mathcal{T}$'s public key [14]
p, q	:	primes s.t. $q \mid p-1$
$g \in G_q$	:	publicly known element of order q in Z_p^*
$E(x, y)$	:	DLP-based encryption of y with public key x (e.g. [15])
$H(\cdot)$	:	an ideal cryptographic hash function (for the Fiat-Shamir heuristic[16])
$Yes, No \in \{0,1\}^\xi$	:	predetermined description for indicating bidder's intention,
$\mathcal{W} = \{w_0, \ldots, w_l\}$	:	a set of $l+1$ prices which can be chosen as a bidding price ($w_0 < \cdots < w_l$)
θ_i	:	$\mathcal{B}_i$'s bidding price

element $h \in G$ and $h^x \bmod n$, getting x is trivial. Therefore, a verifiable encryption of x could be made just by sending g^x and $h^x \bmod n$ and then proving that $\log_g g^x = \log_h h^x$. Obviously, only $\mathcal{T}$ should be able to compute discrete logarithms to the base h, i.e., h and a description of the group G have to be public and constitute a trapdoor function of some sort. As for such a mechanism to find the discrete logarithm with trap-door, Naccache-Stern cryptosystem [17] is one of the suitable function.

Naccache-Stern cryptosystem can shortly be described as follows: let $n = pq$ be an RSA modulus and B a small integer. Compute σ as a square-free odd B-smooth integer such that it divides $\phi(n)$ and is prime to $\phi(n)/\sigma$ (suggested size $\sigma > 2^{160}$). Let h be an element whose multiplicative order modulo n is a large multiple of σ. A message $m < \sigma$ is encrypted by computing $h^m \bmod n$. Decryption is performed using the prime factors of σ, getting m by Chinese remaindering (see [17] for details). The resulting scheme is quite efficient. The semantic security of the scheme is equivalent to the higher-residuosity assumption in the case where n is of the special form described above, such that $\phi(n)$ contains a B-smooth divisor r. This problem is widely believed to be intractable.

The verifiable encryption of x given g^x, denoted as $VE(x)$, is performed by computing $h^x \bmod n$ and showing that $\log_g g^x$ is equal to $\log_h h^x$ by making use of the technique of *proof of knowledge*. Chaum and Pedersen[18] show how to prove the knowledge of the equality of discrete logarithm for groups with known order. Camenisch and Michels[19][20] present a concrete protocol for proving the equality of discrete logarithms for groups with unknown order. Their protocol is mostly based on a technique developed by Fujisaki and Okamoto[21].

Let $\epsilon > 1$ be a security parameter. Let $x \in \{0,1\}^{l_g}$ be the secret information of the prover such that $y_1 = g^x$ and $y_2 = h^x$ holds. Then, a pair $(c, s) \in \{0,1\}^k \times \{-2^{l_g+k}, \ldots, 2^{\epsilon(l_g+k)}\}$ is a proof of knowledge of $\log_g g^x = \log_h h^x$ and can be computed as follows.

1. Choose $r \in_R \{0,1\}^{\epsilon(l_g+k)}$ and compute $t_1 \leftarrow g^r$ and $t_2 \leftarrow h^r$.
2. $c \leftarrow H(g \| h \| y_1 \| y_2 \| t_1 \| t_2)$
3. $s \leftarrow r - cx$ (in Z)

THEOREM 2.1. *If the strong RSA assumption holds, then the underlying interactive protocol corresponding above proof is an honest-verifier statistical zero-knowledge proof* [21] [19] [20].

3. PROTOCOL

Our sealed-bid auction protocol consists of four parts, i.e., *registration*, *bidding*, *opening*, and *dispute*.

3.1 Registration Phase

The auctioneer resisters bidders as the participants of the auction and issues the certificate. Table 3 shows the protocol flow of the registration phase. Informally, a registration protocol works as follows. At the beginning of the protocol, the bidder $\mathcal{B}_i$ randomly chooses $l+1$ integers $(s_{i0}, \ldots, s_{il})$ and computes $(\alpha_{i0}, \ldots, \alpha_{il})$, where $\alpha_{ij} = g^{s_{ij}} \bmod p$. Then, $\mathcal{B}_i$ generates $(\beta_{i0}, \ldots, \beta_{il})$, where β_{ij} is a verifiable encryption $VE(s_{ij})$, i.e., anyone can be convinced that β_{ij} is exactly the encryption of s_{ij} with $\mathcal{T}$'s public-key, but only $\mathcal{T}$ can decrypt s_{ij}. Let us denote $2(l+1)$-tuple $((\alpha_{i0}, \beta_{i0}), \ldots, (\alpha_{il}, \beta_{il}))$ as m_i. Then, $\mathcal{B}_i$ produces his signature $\sigma_i = sig_{\mathcal{B}_i}(m_i)$ and sends a pair (m_i, σ_i) to the auctioneer $\mathcal{A}$.

$\mathcal{A}$ verifies that (m_i, σ_i) is correct with $\mathcal{B}_i$'s public key. If this test is true, then $\mathcal{A}$ makes a certificate $cert_i = (z_{i0}, \ldots, z_{il})$, where z_{ij} is $\mathcal{A}$'s signature on $(\mathcal{B}_i \| \alpha_{ij})$, and sends $cert_i$ to $\mathcal{B}_i$, who verifies it with $\mathcal{A}$'s public key and stores them in his storage securely.

Table 3: Registration phase

$\mathcal{B}_i$		$\mathcal{A}$
For $j = 0, \ldots, l$ $s_{ij} \in_R Z_q$ $\alpha_{ij} \leftarrow g^{s_{ij}} \bmod p$ $\beta_{ij} \leftarrow VE(s_{ij})$ Set $m_i = ((\alpha_{i0}, \beta_{i0}), \ldots, (\alpha_{il}, \beta_{il}))$ $\sigma_i = sig_{\mathcal{B}_i}(m_i)$	$\xrightarrow{m_i, \sigma_i}$	
		For $j = 0, \ldots, l$ check α_{ij}, β_{ij} $z_{ij} \leftarrow sig_{\mathcal{A}}(\mathcal{B}_i \| \alpha_{ij})$ $cert_i = (z_{i0}, \ldots, z_{il})$
	$\xleftarrow{cert_i}$	
Check $cert_i$		
		For $j = 0, \ldots, l$ $s_{Aj} \in_R Z_q$ $\alpha_{Aj} \leftarrow g^{s_{Aj}} \bmod p$ $ek_j \leftarrow \alpha_{Aj} \times \prod_{\mathcal{B}_i \in \mathcal{B}} \alpha_{ij} \bmod p$ publish $((m_1, \sigma_1), \ldots, (m_N, \sigma_N)), (ek_0, \ldots, ek_l)$

At the end of the registration phase, $\mathcal{A}$ randomly chooses $l+1$ integers $(s_{\mathcal{A}_0}, \ldots, s_{\mathcal{A}_l})$ and compute $(ek_0, \ldots, ek_l)$, where ek_j is the encryption-key corresponding the bidding price w_j, and can be computed by

$$ek_j = g^{s_{\mathcal{A}_j}} \times \prod_{\mathcal{B}_i \in \mathcal{B}} \alpha_{ij} \bmod p$$

where corresponding decryption-key dk_j is denoted as,

$$dk_j = s_{\mathcal{A}_j} + \sum_{\mathcal{B}_i \in \mathcal{B}} s_{ij} \bmod q.$$

Note that $s_{\mathcal{A}_j}$ and $s_{1j}, \ldots, s_{nj}$ are shares of dk_j using $(N+1, N+1)$ secret sharing scheme[22]. Finally, $\mathcal{A}$ publishes $((m_1, \sigma_1), \ldots, (m_N, \ldots, \sigma_N))$ and $(ek_0, \ldots, ek_l)$ in the BB.

3.2 Bidding Phase

Each bidder B_i chooses a bidding price w_k from the set $\mathcal{W}$, then he makes his bidding information $com_i = (com_{i0}, \ldots, com_{il})$ using the public encryption-key $\{ek_0, \ldots, ek_l\}$, and finally he sends com_i with his signature to $\mathcal{A}$. Table 4 shows the protocol flow of the registration phase. At first, a bidder $\mathcal{B}_i$ generate the bidding information $(com_{i0}, \ldots, com_{il})$, where com_{ij} is $\mathcal{B}_i$'s commitment to w_j. This commitment is produced by encrypting the bidding information with the encryption-key ek_j according to publicly known rule. For the simplicity of description, suppose $s_{ij} = s_{il}$, $\alpha_{ij} = \alpha_{il}$, and $\beta_{ij} = \beta_{il}$ when $j < 0$. Then, the form of the message encrypted here can be described as

$$com_{ij} = E(ek_j, I_{ij} \| \alpha_{ij-1} \| z_{ij-1})$$

where α_{ij-1}, z_{ij-1} are generated in the registration phase, and I_{ij} indicates the $\mathcal{B}_i$'s choice whether he wants to bid the price w_j.

Let θ_i be $\mathcal{B}_i$'s bidding price. If $w_j \neq \theta_i$, I_{ij}, called "*no-form*," can be described as

$$I_{ij} = (No \| s_{ij-1})$$

where No is ξ-bit string which is publicly defined by the auctioneer before the bidding phase, and s_{ij-1} is B_i's shares of dk_{j-1}. Obviously, if the auctioneer can decrypt com_i and there are no bidder whose bidding price is equal to w_j, the auctioneer can reconstruct the decryption-key dk_{j-1} since he can collect $N+1$ shares of dk_{j-1}. If $w_j = \theta_i$, I_{ij}, called "*yes-form*," can be presented by

$$I_{ij} = (Yes \| proof(s_{ij-1}))$$

where Yes is ξ-bit string and $proof(x)$ $(x \in Z_q)$ is a proof of knowledge of x, which allows a prover to prove the possession of x to anyone without revealing itself. This can be done by the technique of Schnorr-like signature schemes[23]. Consequently, given $y = g^x \bmod p$, $proof(x)$ can be generated as follows.

1. randomly chooses $r \in Z_q$.
2. compute $c = H(g^r \bmod p || y)$ and $e = r - cx \bmod q$

where (c, e) is $proof(x)$ and can be publicly checked by $c \stackrel{?}{=} H(g^e y^c \bmod p || y)$.

Note that, in this case, $\mathcal{B}_i$ does not reveal the information of s_{ij-1} but only prove the possession of it. If $\mathcal{A}$ finds that for some γ, $com_{i\gamma}$ contains this type of message, $\mathcal{B}_i$'s bidding value is $w_{i\gamma}$ and he is a successful bidder. If the winner is decided, $\mathcal{A}$ cannot reconstruct the next decryption-key $dk_{\gamma-1}$ since he does not get $s_{i\gamma-1}$, i.e., one of the shares of $dk_{\gamma-1}$. Therefore, $\mathcal{A}$ cannot decrypt $com_{i\gamma-1}, \ldots, com_{i0}$ for all i subsequently, because $\mathcal{A}$ cannot decrypt com_{ij} without knowing dk_j which is recovered by the shared information in com_{ij+1}. This property achieves the universal verifiability of the winning bid, as well as hiding bids of losers.

In our scheme, all bidders who have been registered at the registration phase must bid *before* the bidding period closes. If $\mathcal{B}_i$ wants to give up the bidding, he should open his all shares $(s_{i0}, \ldots, s_{iN})$ and $\mathcal{T}$'s certificate $cert_i$ to the bulletin board. If $\mathcal{B}_i$ does neither give com_i to $\mathcal{A}$ nor open his shares,

Table 4: Bidding phase

For $j = l, \ldots, 0$
  if $w_j = w_{i\gamma}$
    $r \in_R Z_q$
    $c \leftarrow H(g^r || \alpha_{ij-1})$
    $e \leftarrow r - cs_{ij-1}$
    $com_{ij} \leftarrow E(ek_j, Yes \| c \| e \| \alpha_{ij-1} \| z_{ij-1})$
  else
    $com_{ij} \leftarrow E(ek_j, No \| s_{ij-1} \| \alpha_{ij-1} \| z_{ij-1})$
$com_i \leftarrow (com_{i0}, \ \ldots, \ com_{il})$
Send $com_i, sig_{\mathcal{B}_i}(com_i)$ to $\mathcal{A}$

$\mathcal{A}$ excludes $\mathcal{B}_i$ from the list of participants, and then requests $\mathcal{T}$ to recover $(s_{i0}, \ldots, s_{iN})$ by decrypting $(\beta_{i0}, \ldots, \beta_{iN})$ and to send them to $\mathcal{A}$. Using these values, $\mathcal{A}$ can continue this auction without bidding again from scratch (see section 3.4 for the detail).

3.3 Opening Phase

Once the bidding period closes, $\mathcal{B}_i$ confirms that the content of BB is correct according to the rule, and then publishes the values $(s_{il}, \alpha_{il}, z_{il})$ and $\mathcal{A}$ checks if $g^{s_{il}} = \alpha_{il}$ and $z_{il} = sig_{\mathcal{A}}(\mathcal{B}_i \| \alpha_{il})$ in the BB. If $\mathcal{B}_i$ opens no messages or this check is failed, $\mathcal{A}$ runs the dispute protocol $Dispute(\mathcal{B}_i)$, after which $\mathcal{B}_i$ is removed from the bidder's list. Opening procedures can be described as follows.

1. set $j = l$.
2. $\mathcal{A}$ computes dk_j by
$$dk_j \leftarrow s_{Aj} + \sum_{\mathcal{B}_i \in \mathcal{B}} s_{ij} \bmod q$$
and publishes dk_j in the BB.
3. for all $\mathcal{B}_i \in \mathcal{B}$, $\mathcal{A}$ performs the following.
   (a) compute I_{ij}, α_{ij-1} and z_{ij-1} by decrypting com_{ij} with the key dk_j.
   (b) If I_{ij} is *no-form*, $\mathcal{A}$ evaluates
   $$g^{s_{ij-1}} \stackrel{?}{=} \alpha_{ij-1} \bmod p \quad (1)$$
   $$z_{ij-1} \stackrel{?}{=} sig_{\mathcal{A}}(B_i \| \alpha_{ij-1}) \quad (2)$$
   where s_{ij-1} is contained in the description of I_{ij} in principle. Passing these tests indicates that w_j is not B_i's bidding price. If s_{ij-1} is not contained or these tests are failed, $\mathcal{A}$ performs $Dispute(\mathcal{B}_i)$ in order to remove $\mathcal{B}_i$ from the system safely (see section 3.4).
   (c) If I_{ij} is *yes-form*, $\mathcal{A}$ verifies
   $$c \stackrel{?}{=} H(g^e \alpha_{ij-1}{}^c \bmod p || \alpha_{ij-1}) \quad (3)$$
   $$z_{ij-1} \stackrel{?}{=} sig_{\mathcal{A}}(B_i \| \alpha_{ij-1}) \quad (4)$$
   where $proof(s_{ij-1}) = (c, e)$ is contained as a part of I_{ij} in principle. If these tests are true, $\mathcal{B}_i$ is a winner. In this case, $\mathcal{A}$ cannot compute dk_{ij-1} since $\mathcal{A}$ does not get the value of s_{ij-1}. Therefore, $\mathcal{A}$ cannot get any useful information of loser's bids at all. If $proof(s_{ij-1})$ is not contained or these tests are failed, $\mathcal{A}$ performs $Dispute(\mathcal{B}_i)$ in order to remove $\mathcal{B}_i$ (see section 3.4).
4. If there are at least one winner, $\mathcal{A}$ declares the identity of the winner(s) and finishes the opening, otherwise, if $j > 0$, return to 2 by putting $j := j - 1$. If $j = 0$, $\mathcal{A}$ finishes the opening by declaring no winners.

DEFINITION 3.1 (WINNER). *A bidder $\mathcal{B}_i$ with his bid w_γ can be considered as the winner of the auction if and only if all of the following conditions are satisfied.*

1. *$\mathcal{B}_i$ has not been eliminated from the bidder's list by $Dispute(\mathcal{B}_i)$.*
2. *The decryption of $com_{i\gamma}$ includes $proof(s_{i\gamma-1})$, as well as (3) and (4) are satisfied for $j = \gamma$.*
3. *If $\gamma < l$, for $\forall j \in \{l, \ldots, \gamma + 1\}$, the decryption of com_{ij} contains s_{ij-1}, as well as (1) and (2) are satisfied.*
4. *(m_i, σ_i) is a correct pair of a message and $\mathcal{B}_i$'s signature on it.*
5. *For $\forall j \in \{\gamma, \ldots, l\}$, α_{ij} in the decryption of com_{ij} is equal to α_{ij} appeared in m_i.*

3.4 Dispute

If $\mathcal{B}_i$ cheats or simply crashes, $\mathcal{A}$ invokes the protocol called $Dispute(\mathcal{B}_i)$, which are two-party protocol between $\mathcal{A}$ and $\mathcal{T}$ for resolving the dispute. At the beginning of this protocol, $\mathcal{A}$ sends (m_i, σ_i) and, if necessary, com_i to $\mathcal{T}$, who checks $\sigma_i = sig_{\mathcal{B}_i}(m_i)$ and confirms $\mathcal{B}_i$'s deviation from the rule. For instance, the loss of his registration information and sending irregular messages can be considered as the deviation. If the confirmation is true, $\mathcal{T}$ obtains $(s_{i0}, \ldots, s_{il})$ by decrypting $(\beta_{i0}, \ldots, \beta_{il}) = (VE(s_{i0}), \ldots, VE(s_{il}))$ with his private key. The decrypted message is sent to $\mathcal{A}$, who verifies them after receiving and performs the following procedures.

$$\forall j \in \{0, \ldots, l\} \quad s_{Aj} \leftarrow s_{Aj} + s_{ij} \bmod q$$

$$\mathcal{B} \leftarrow \mathcal{B} - \{\mathcal{B}_i\}$$

As a result of the execution of this protocol, $\mathcal{A}$ can exclude $\mathcal{B}_i$ from the bidder's list and can continue opening bids.

4. ANALYSIS

A brief description of several properties of our protocol is as follows.

4.1 Security

We claimed that the following properties described in [8][10] are achieved in our protocol.

Fairness *No one can disclose the content of any of the bids until the bidding period closes.*

Opening bids requires the first decryption key dk_l that is shared among all bidders and auctioneer. Therefore, no one can disclose any information of bids unless all bidders open their shares $(s_{1l}, \ldots, s_{Nl})$ after confirming that the bidding period closes.

Privacy of losing bid *All bidding prices except the contract price is not revealed to anyone including the auctioneer.*

If the bidder $\mathcal{B}_i$ with his bid w_γ is the winner, he does not disclose $s_{i\gamma-1}$ but $proof(s_{i\gamma-1})$. Therefore, the auctioneer cannot get any information of $dk_{\gamma-1}$ and decrypt the subsequent commitments to bids.

Universal verifiability *It is universally verifiable that the price of the successful bid is highest among all bids.*

In our protocol, when the winning bid w_γ, given dk_l, $\ldots, dl_\gamma$ anyone can simulate the procedure to open bids using the information on the BB. These decryption keys are available after the execution of the opening procedure (They are published by the auctioneer during the opening phase.)

Correctness *The winning bid is indeed the highest bid.*

Let $\mathcal{B}_{win}$ be the winner and his bid be w_γ. After the execution of the opening procedure, the auctioneer and all bidders can get convince that $\mathcal{B}_{win}$ satisfies that all conditions described in the definition 3.1 (due to the property of a *universal verifiability*). Here, we suppose there exists a bidder whose bid is higher than w_γ. Let us denote him and his bid as $\mathcal{B}_X(\neq \mathcal{B}_{win})$ and $w_\xi(> w_\gamma)$, respectively. In this case, $\mathcal{B}_X$ does not disclose $s_{X\xi-1}$ in the decryption of $com_{X\xi}$ but open $proof(s_{X\xi-1})$. Consequently, auctioneer (and bidders) cannot get any information of bids lower than w_ξ and they does not check $\mathcal{B}_{win}$'s bid. This is contradiction.

In addition, auctioneer cannot alter any bids, due to the unforgeability of bidder's signature and the property of the BB.

Non-repudiation *The winners cannot deny they submitted the winning bid.*

During the bidding phase, all bidders produce their signature on the commitment to their bids and publishes them on the BB. Therefore, the submission of their bids is undeniable due to the unforgeability of their signature and the property of the BB.

Robustness *No bidder can make the protocol impossible by his malicious act. Namely, even after detecting the cheater, the auctioneer can continue the protocol without bidding again from scratch.*

The auctioneer can continue the protocol by eliminating cheating bidders through the execution of the dispute protocol. Once the cheaters have been eliminated, they cannot make any corruption at all.

Soundness *Nobody can impersonate any other bidder to make a bid.*

During the registration phase, the auctioneer publishes the signatures of all bidders $(m_1, \sigma_1), \ldots, (m_N, \sigma_N)$ during the registration phase. These signatures are checked by all bidders at the beginning of the opening phase. Therefore, no one can pretend to be another bidder due to the unforgeability of bidder's signatures and the property of the BB.

4.2 Efficiency

In our protocol, the round complexity between a bidder and the auctioneer is only three. (registration phase, bidding phase, and the beginning of opening phase). This is superior to [3][9][4]. On the other hand, unfortunately, our communication complexity is inferior than them due to the generation of the commitment to all biddable values. In some practical application of sealed-bid auction, however, bidders should be considered to be off-line, in the sense that all bidders cannot communicate with the auctioneer simultaneously, but only can communicate individually. During the opening phase, [3][9][4] require that all bidders are on-line, while our scheme allows all bidders to take part only at the beginning.

Typically, there are two classes of privacy of bids. Our protocol, as well as [3][9][8][10], does not reveal only the value of bids, but also the order of them, while [12][13] does not conceal the order of bids. (i.e., one auction server learns some information about the partial order of the bids.) Up to now, all protocols (including ours) which enjoy the former privacy, requires that the auctioneers exponentially large amount of computation/communication with respect to the length of bids. These requirements impose bandwidth and latency problems on all the servers(or bidders). Furthermore, the messages sent are longer due to the generation of commitments to all biddable values, which may be problematic in some settings. (e.g. if this number is large.) More efficient protocol with respect to the length of bids will be expected.

4.3 Anonymity of Bidder's Identity

Our protocol itself does not give the anonymity for bidders. (i.e. who attends the auction.) Our protocol reveals the bidder's identity in the registration phase that causes privacy issues in some kind of the auction. Though there exist a lot of known techniques[24][25] providing the restricted anonymity with a sort of off-line TTP, a simple use of these techniques means that there still exists TTP they must trust in terms of the security from the bidder's viewpoint. Achieving the anonymity of the bidders without an on-line TTP is a future work to be solved.

5. CONCLUSIONS

In this paper, we proposed a new sealed-bid auction protocol that allows an auctioneer to determine the winning bid in a universally verifiable way, and simultaneously that prevents even an auctioneer from getting any useful information

of bids of losers. We adopt an optimistic approach, i.e., the TTP takes part in the protocol only if one bidder cheats or simply crashes. Our protocol is quite efficient since a bidder takes part only at the beginning. More importantly, our scheme is robust against cheating bidders; i.e. any deviation of bidders cannot prevent the auctioneer from determining the auction. To the best of our knowledge, this work is the first construction of a universally verifiable sealed-bid auction protocol in an optimistic approach.

However, plenty of works remains. Especially, a drawback of our protocol is that all bidders have to make preregistration before starting the bidding phase and communication complexity is relatively high. Furthermore, the collusion between bidders and auctioneers should be considered. These will be our future works.

Acknowledgements

Special thanks to Kazue Sako, Tatsuyuki Matsushita and Akira Otsuka for helpful discussion and comments during the preparation of this paper. Finally, the authors also thank the anonymous refrees for comments which improved presentation of the paper.

6. REFERENCES

[1] N. Asokan, M. Schunter, and M. Waidner. Optimistic protocol for fair exchange. In *Proc. of ACM-CCS'97*, pages 8–17, 1997.

[2] N. Asokan, V. Shoup, and M. Waidner. Optimistic fair exchange of digital signatures. In *Proc. of EUROCRYPT'98*, pages 591–606, 1998.

[3] S. Miyazaki and K. Sakurai. A bulletin board-based auction system with protecting the bidder's strategy. In *Proc. of SCIS'99 (in Japanese)*, pages 41–46, 1999.

[4] K. Kobayashi and H. Morita. Efficient sealed-bid auction with quantitative competition using one-way functions. In *Technical Report of IEICE, ISEC95-30*, pages 31–37, 1999.

[5] M. Franklin and M. Reiter. The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 22(5):302–312, 1996.

[6] M. Franklin and M. Reiter. Verifiable signature sharing. In *Proc. of EUROCRYPT'95*, pages 50–63, 1995.

[7] H. Kikuchi, M. Harkavy, and J. D. Tygar. Multi-round anonymous auction schemes. In *IEEE Workshop on Dependable and Real-Time E-Commerce System*, pages 62–69, 1998.

[8] K. Sako. Universary verifiable auction protocol which hides losing bids. In *Proc. of SCIS'99 (in Japanese)*, pages 35–39, 1999.

[9] K. Sakurai and S. Miyazaki. A bulletin-board based digital auction scheme with bidding down strategy - towards anonymous electronic bidding without anonymous channels nor trusted centers. In *Proc. of CRYPTEC'99*, pages 180–187, 1999.

[10] K. Sako. An auction protocol which hides bids of losers. In *Proc. of PKC'2000*, pages 422–432, 2000.

[11] Y. Desmedt and Y. Frankel. Threshold cryptosystem. In *Proc. of CRYPTO'89*, pages 307–315, 1990.

[12] C. Cachin. Efficient private bidding and auctions with an oblivious third party. In *Proc. of ACM-CCS'99*, 1999.

[13] M. Naor, B. Pinkas, and R. Sumner. Privacy preserving auctions and mechanism design. In *Proc. of The 1st ACM Conference on Electronic Commerce*, 1999.

[14] G. Ateniese. Efficient verifiable encryption (and fair exchange) of digital signatures. In *Proc. of ACM-CCS'99*, pages 138–146, 1999.

[15] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proc. of CRYPTO'98*, pages 13–25, 1998.

[16] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Proc. of Crypto'86*, pages 186–194, 1986.

[17] D. Naccache and J. Stern. A new public key cryptosystem based on higher residues. In *Proc. of ACM-CCS'98*, pages 59–66, 1998.

[18] D. Chaum and T. P. Pedersen. Wallet databases with observers. In *Proc. of Crypto'92*, pages 89–105, 1992.

[19] J. Camenisch and M. Michels. A group signature scheme with improved efficiency. In *Proc. of ASIACRYPT'98*, pages 160–174, 1998.

[20] J. Camenisch and M. Michels. Separability and efficiency for generic group signature schemes. In *Proc. of CRYPTO'99*, 1999.

[21] E. Fujisaki and T. Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *Proc. of CRYPTO'97*, pages 16–30, 1997.

[22] A. Shamir. How to share a secret. *Communication of the ACM*, 22:612–613, 1979.

[23] C. P. Schnorr. Efficient identification and signatures for smart cards. In *Proc. of Eurocrypt'89*, pages 688–689, 1989.

[24] J. Kilian and E. Petrank. Identity escrow. In *Proc. of CRYPTO'98*, pages 169–185, 1998.

[25] K. Sako. Restricted anonymous participation. In *Proc. of SCIS'2000 (in Japanese)*, pages SCIS2000–B12, 2000.

[26] J. Cohen and M. Fischer. A robust and verifiable cryptographically secure election scheme. In *Proc. of FOCS'85*, pages 372–382, 1985.

[27] M. Kudo. Secure electronic sealed-bid auction protocol with public key cryptography. *IEICE Trans. Fundamentals*, E81-A(1):20–26, 1998.