Regular Paper

An Anonymous Bidding Protocol without Any Reliable Center

Toru Nakanishi,[†] Toru Fujiwara[††] and Hajime Watanabe[†††]

An anonymous bidding protocol without any reliable center for a small community is proposed. The anonymity of a bidding protocol means that the participation of everyone involved in the bidding except for the successful bidder is kept secret. Since it is hard for a small community to establish a reliable center owing to the difficulty and cost of doing so, an anonymous bidding protocol without any reliable center is appropriate to its needs. In such a bidding protocol, a bidder can withdraw his bid after the deadline for bidding by ceasing to participate in the bidding. If this can be done anonymously, the price of the successful bid would be illegally manipulated by conspiratorial bidders. In the bidding protocol proposed in this paper, such a bidder can be identified. This discourages conspiratorial bidders from manipulating the price of the successful bid through withdrawing, by applying some sanctions against their acts.

1. Introduction

One step toward realizing fair electronic commerce has been the introduction into computer network of bidding procedures that were previously conducted in writing. A bidding is often conducted in a small community, that is, the participants are limited. In such a community, the establishment of any reliable center inside the community is not realistic, since it is rare for members of the community to have no interest in each other. Furthermore, the establishment of a center outside the community is also undesirable, because it involves considerable difficulties as regards reliability and cost. Some cryptographic protocols for bidding[1)~4)] depend on reliable centers, and thus are not appropriate for such small communities.

This paper deals with a bidding protocol without any reliable center. Hereafter, for simplicity, we assume that the person who makes the lowest bid is chosen as the successful bidder. It is desirable that a bidding protocol should be anonymous in the sense that the participation in the bidding of a person (or organization) who obeys the protocol but does not become a successful bidder is kept secret from everyone else. This is because the names of bidders and the correspondence between bidders and their bids constitute useful information for conspirators in future bidding procedures[5)].

In Imamura, et al.[5)], an anonymous bidding protocol without any reliable center is proposed. In the protocol, each bidder anonymously broadcasts a cryptogram of his bid price before the deadline for bidding. After the deadline, each bidder publishes his price by broadcasting the key to the cryptogram anonymously, and the bidder who offers the lowest of the published prices reveals his name. If a bidder who broadcasts a cryptogram does not broadcast his key, his bid is ignored. Similarly, if the bidder who offers the lowest price does not reveal his name, his bid is also ignored. As a result, the price of the successful bid can be illegally manipulated. The following example shows that conspiratorial bidders can benefit by using this fact[6)]. Suppose that Alice and Bob, who are conspiratorial bidders, want to prevent the other bidders from making a successful bid and to make a successful bid with a price as high as possible. They do the following:

(1) Alice bids $\mathit{price}_{\mathrm{min}}$, which seems to be the lowest price, and Bob bids $\mathit{price}_{\mathrm{desire}}$ with $\mathit{price}_{\mathrm{desire}} > \mathit{price}_{\mathrm{min}}$.

(2) Suppose that $\mathit{price}_{\mathrm{min}}$ is the lowest price. Then, after all other bid prices have become public, Alice and Bob check whether anyone has bid price with $\mathit{price}_{\mathrm{desire}} > \mathit{price} > \mathit{price}_{\mathrm{min}}$ or not. If so, Alice publishes her price, reveals her name and becomes the successful bidder. Otherwise, Alice does not publish her price, or does not reveal her name. In this case, Bob is chosen as the successful bidder.

This example shows that Alice and Bob may

[†] Department of Communication Network Engineering, Faculty of Engineering, Okayama University

[††] Department of Informatics and Mathematical Science, Graduate School of Engineering Science, Osaka University

[†††] Computer Science Division, Electrotechnical Laboratory

choose the price for the successful bid after they know others' bid prices. A solution for this coalition problem is to provide a method for identifying the anonymous bidder when he does not publish his price or does not reveal his name, and then to apply some sanction against him to discourage such a coalition.

This paper proposes an anonymous bidding protocol without any reliable center, where the above coalition problem is solved. The protocol is constructed on the assumptions that (1) an anonymous broadcast network exists and (2) a verification key for a signature generated by each individual who will participate in the bidding is published, and the correspondence between the individual and the verification key is known to everyone in the network. The anonymous broadcast network is a network in which a message is correctly sent to all participants, and furthermore the sender cannot be identified, as also assumed in Imamura, et al.[5]. The second assumption can be accomplished by using a certification authority (CA), for example. A CA is a part of an infrastructure for realizing electronic commerce, and need not participate in the proposed protocol directly. In this sense, our proposed protocol does not have any reliable center. Furthermore, even if a CA is used, the anonymity is not compromised by conspiring with the CA. To identify an anonymous bidder who does not obey the protocol, an undeniable signature scheme satisfying the requirement that signatures are anonymous is used. The anonymity of a signature means that it does not disclose the identity of the signer. The signer of a signature in the undeniable signature scheme can be identified by an interactive proof scheme with a candidate for the signer. The true signer cannot repudiate his signature while the others can. By communicating with all candidates for the signer, it is possible to identify the true signer. Since each bidder is forced to attach the signature to his bid, it becomes possible to identify an anonymous bidder disobeying the protocol. Thus, if Alice and Bob coalesce as above, Alice can be identified, and some sanction is applied to discourage such a coalition.

After we pointed out the above coalition problem in Nakanishi, el al.[6], a bidding protocol was proposed in Miyazaki, el al.[7]. The feature of this protocol is that the prices of all except the successful bid are kept secret even after the bidding. If someone obtains the bid prices, he can learn the strategies of the bidders and may use the information in future bidding procedures. The protocol has the merit of avoiding such learning by keeping the bid prices secret[7]. In this protocol, a list of prices that may be bid is agreed by the participants in advance. After the deadline for bidding, the following is executed for each price in ascending order from the lowest price in the list: If a bidder really offered the price, he proves that he did so, and becomes the successful bidder. Otherwise, every bidder proves that he did not bid that price. This prevents the withdrawal of a bid, and thus the above coalition problem is solved.

However, in this protocol, there is a registration center and it can trace the bidder from his bid. That is, the anonymity depends on the reliability of the center, although the reliability affects only the anonymity. As mentioned above, we consider the situation in which it is hard to have a reliable center. If it is difficult to construct a protocol with the same feature without any reliable center, anonymity is most important so as not to provide useful information to potential conspirators. That is why we propose an anonymous bidding protocol without any reliable center. Furthermore, in the protocol proposed by Miyazaki, et al.[7], the communication cost of determining the price of the successful bid is proportional to the number of possible bid prices, and thus is efficient only for limited cases. Our protocol is more efficient except for the communication to identify illegal bidders, which is executed only when someone performs an illegal action.

Section 2 outlines the conditions that anonymous bidding protocols should satisfy. In Section 3, an anonymous bidding protocol is constructed, and is investigated to determine whether it satisfies the conditions.

2. Conditions for Anonymous Bidding Protocols

This section outlines the conditions that anonymous bidding protocols should satisfy. We call a protocol satisfying the following conditions an *anonymous bidding protocol.* These conditions are derived from the requirements in Imamura, et al.[5], except the impossibility of pretense, which is important for bidding on a computer network.

(1) **Validity of public notices:** Information on the bidding session, namely, each specific bidding, provided by the man-

ager of the bidding cannot be modified, and can be seen by anyone in the network. This information is called a *public notice*.

(2) **Secrecy of bid prices:** Until the deadline for bidding, valid bid prices cannot be leaked to others.

(3) **Impossibility of pretense:** No one can act for person as a valid bidder.

(4) **Impossibility of multiple bids:** No bidder who bids more than once in a bidding session can become the successful bidder.

(5) **Validity of bid prices:** Valid bid prices cannot be modified by others, even by the bidder.

(6) **Validity of successful bid:** The successful bid is the lowest price offered by any of the bidders who obeyed the protocol, and any bidder who obeyed the protocol before the deadline for bidding but disobeyed it after the deadline is identified.

(7) **Anonymity:** The participation in the bidding session of a user who obeys the protocol but is not the successful bidder is kept secret from everyone else.

In bidding protocols satisfying the validity of successful bid, the manipulation of the price of the successful bid, as indicated in Section 1, is prevented as follows: Since the successful bidder is chosen from only bidders obeying the protocol, conspiratorial Alice and Bob who want to prevent the other bidders from making a successful bid must obey the protocol before the deadline for bidding. However, when Alice and Bob find out that no one offers a price between their prices and Alice disobeys the later protocol so as not to make the successful bid, she is identified. The later identification discourages them from manipulating the price of the successful bid.

3. Anonymous Bidding Protocol

This section proposes an anonymous bidding protocol satisfying the seven conditions listed in Section 2. As indicated in Section 1, we construct the protocol by using an undeniable signature scheme that satisfies the anonymity of signatures, which is called an anonymous undeniable signature scheme. Since such a scheme has not been proposed, before constructing the protocol, an undeniable signature scheme in Chaum[8] is reviewed to discuss the anonymity of signatures.

3.1 An Undeniable Signature Scheme in Chaum[8]

Let p and q be sufficiently large primes such that $p = 2q + 1$, let g be a generator of a subgroup G, whose order is q, of Z_p^*, and let $\mathcal{H}$ be a one-way hash function. The participants in the scheme agree on p, q, g, and $\mathcal{H}$. Then, the signing and verification key for a participant are x chosen randomly from Z_q and $y = g^x \bmod p$, respectively. Assume that the verification key is published, and that the correspondence between the verification key and the owner is known to all participants. The signature for a message m is $z = h^x \bmod p$, where $h = \mathcal{H}(m)$. When a singer convinces a verifier that a signature z is a valid signature corresponding to the signer's verification key y and a message m, the signer communicates with the verifier by a confirmation protocol where it is proved that the signer knows x such that $z = h^x \bmod p$ and $y = g^x \bmod p$ with zero-knowledge. When an alleged signer convinces a verifier that a string z is not a valid signature corresponding to the signer's verification key y and a message m, the signer communicates with the verifier by a disavowal protocol where it is proved that the signer knows x such that $z \neq h^x \bmod p$ and $y = g^x \bmod p$ with zero-knowledge. A concrete description of these zero-knowledge interactive protocols is given in Chaum[8]. These zero-knowledge interactive protocols can be converted into non-interactive ones by the same method as used in Fiat, et al.[9]. Thus, anyone with the non-interactive proof can verify its validity. In our anonymous bidding protocol, the signature scheme with the non-interactive proof is used. The communication costs of the confirmation and disavowal protocols in Chaum[8] are as follows: In the confirmation protocol, the length of sent messages is $6|p|$, and the computation requires about 10 exponentiations with modulus p. In the disavowal protocol, the length of sent messages is $8|p|$ in addition to the length of the two bit commitments, and the computation requires about 20 exponentiations with modulus p in addition to the computations of two bit commitments. If the bit commitment in Pedersen[10], which relies on the hardness of computing discrete logarithms as well as the undeniable signature scheme, is used for the same modulus, the length of the bit commitment is $|p|$, and the computation requires two exponentiations. Note that, in the undeniable signature scheme, the slightly modified confirmation protocol enables the signer to prove that two signatures are made by him without revealing his identity. This protocol is used in the situation where there are multiple bids at the lowest price, which is discussed at the end of the following subsection.

Next, we discuss the anonymity of the undeniable signature under the existence of a random hash function $\mathcal{H}(m)$ from any message m into G, and the following decision Diffie-Hellman (D-H) assumption[11]:

Decision Diffie-Hellman assumption: Let a and b be random elements from Z_q, and let v be a random element from G. Given a tuple, $(v_1 = g^a \bmod p, v_2 = g^b \bmod p, v)$, any probabilistic polynomial time algorithm determines whether $v \equiv g^{ab} \pmod p$ or not, that is, whether or not the discrete logarithm of v to the base v_2 is equal to that of v_1 to the base g, with negligible probability. □

Then, the following theorem holds:

Theorem 1 Assume the existence of a random hash function $\mathcal{H}$ and the decision D-H assumption. Then, given a value hashed from a message by $\mathcal{H}$, an undeniable signature of the value, and a verification key, it is infeasible to determine whether or not the undeniable signature is made with the message and a signing key corresponding to the verification key.

Proof: Assume that the theorem does not hold. Let x_1 and x_2 be random elements from Z_q, and let m be a string of finite length. Then, a probabilistic polynomial time algorithm A exists which, given a tuple, $(h = \mathcal{H}(m), z = h^{x_1} \bmod p, y = g^{x_2} \bmod p)$, determines whether or not the discrete logarithm of z to the base h is equal to that of y to the base g with non-negligible probability. Given a tuple, $(v_1 = g^a \bmod p, v_2 = g^b \bmod p, v)$, run A whose inputs are v_2 as h, v as z, and v_1 as y. Then, A determines whether or not the discrete logarithm of v to the base v_2 is equal to that of v_1 to the base g, with the probability, since the probability distributions (h, z, y) and (v_2, v, v_1) are the same. This contradicts the decision D-H assumption, and thus this theorem holds. □

This theorem does not directly imply the anonymity of signatures. For example, we have not proved that multiple signatures do not disclose information about the signer. However, no known attack can compromise the anonymity, to the best of our knowledge. Furthermore, in other anonymous signature schemes[12),13)] using the same assumption, such an attack is also unknown, though the relation between this undeniable signature scheme and the other anonymous signature schemes is also unknown. Therefore, this undeniable signature scheme is used as the anonymous undeniable signature scheme in the proposed anonymous bidding protocol. Note that any anonymous undeniable signature scheme can be used in the proposed anonymous bidding protocol.

3.2 Protocol

The proposed protocol as well as that in Imamura, el al.[5] is constructed on the assumption that an *anonymous broadcast network* exists. The broadcast network is a network where sent messages cannot be modified and the messages can be seen by anyone in the network. The anonymous network is a network where nobody except for a sender can identify the sender of any message, and is proposed in Chaum[14].

This protocol has the following entities:

Manager: Agent of a particular bidding. He broadcasts the public notice, checks the validity of bidders, discovers illegal bidders and so on. He publishes his verification key and keeps his signing key on a digital signature scheme.

Note that the manager is not required to be a reliable center.

Users: Persons or organizations in a group, called a participant group, whose members are ready to participate in a bidding session. User U_i publishes his verification key and keeps his signing key on an anonymous undeniable signature scheme.

The registration of users as members of the group is not included in this protocol. Assume that a verification key generated by each individual in the group is published, and that the correspondence between the verification key and the owner is known to everyone in the network, as mentioned in Section 1.

The following operations are used in this protocol:

Anonymous undeniable signature: $US_i(m)$ denotes the user U_i's anonymous undeniable signature for message m.

Digital signature: $DS_M(m)$ denotes the manager's secure digital signature for message m.

Bit commitment: $BC(m, r)$ denotes the bit commitment for message m and secret key r.

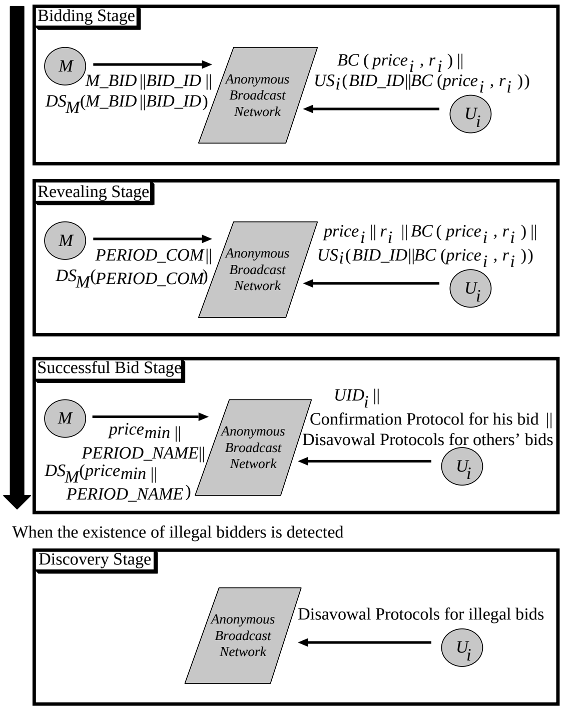
Bidding Stage
M
M_BID || BID_ID ||
DS_M(M_BID || BID_ID)
Anonymous Broadcast Network
BC (price_i , r_i) ||
US_i(BID_ID||BC (price_i , r_i))
U_i
Revealing Stage
M
PERIOD_COM||
DS_M(PERIOD_COM)
Anonymous Broadcast Network
price_i || r_i || BC (price_i , r_i) ||
US_i(BID_ID||BC (price_i , r_i))
U_i
Successful Bid Stage
M
price_min ||
PERIOD_NAME||
DS_M(price_min ||
PERIOD_NAME)
Anonymous Broadcast Network
UID_i ||
Confirmation Protocol for his bid ||
Disavowal Protocols for others' bids
U_i
When the existence of illegal bidders is detected
Discovery Stage
Anonymous Broadcast Network
Disavowal Protocols for illegal bids
U_i

Fig. 1 Proposed anonymous bidding protocol.

Concatenation: $m_1 \| m_2$ denotes the concatenation of two messages m_1 and m_2.

This protocol consists of four stages: the bidding stage, the revealing stage, the successful bid stage, and the discovery stage. If the bidders who do not obey the protocol in the revealing stage or the successful bid stage are not found, only the first three stages are executed. Otherwise, the discovery stage is executed, where the bidders are identified. Then the successful bid stage is executed. The protocol is depicted in **Fig. 1**.

[**Bidding stage**]

In this stage, the manager broadcasts a public notice and each bidder makes a bid.

(1) Let M_BID be a message that specifies the contents and period of the bidding, and let BID_ID be an identifier of the bidding session that is different from the identifiers of other bidding sessions. The manager publishes the concatenation of M_BID and BID_ID with his digital signature for it,

$$M\_BID \| BID\_ID \\ \| DS_M(M\_BID \| BID\_ID).$$

(2) A bidder U_i computes the bit commitment $BC(price_i, r_i)$ for his bid price $price_i$, using a secret random sequence r_i. He computes his undeniable signature for $BID\_ID \| BC(price_i, r_i)$. During the period of the bid, he publishes the concatenation of the bit commitment and the signature,

$$BC(price_i, r_i) \\ \| US_i(BID\_ID \| BC(price_i, r_i)).$$

The undeniable signature scheme prevents repudiation of a bid and pretense by other bidders. The bit commitment scheme ensures the validity and secrecy of the bidding price.

[**Revealing stage**]

After the bidding period, this stage is executed. In this stage, each bidder reveals the contents of his bit commitment and publishes his bid price. Note that this can be done anonymously.

(1) Let $PERIOD\_COM$ be a message that specifies the period in which the bidders must reveal the contents of their bit commitments. The manager publishes $PERIOD\_COM$ with his digital signature for $PERIOD\_COM$,

$$PERIOD\_COM \\ \| DS_M(PERIOD\_COM).$$

(2) During the period, the bidder U_i publishes the concatenation of $price_i$, r_i, and his bid,

$$price_i \| r_i \| BC(price_i, r_i) \\ \| US_i(BID\_ID \| BC(price_i, r_i)).$$

This published value is called the revealed bid.

(3) For every bid offered in the bidding stage, the manager checks whether the bid satisfies the following condition: The bit commitment in the bid can be opened by using the sequence r_i of some revealed bid, including the same bid, and the opened price is equal to $price_i$ of that revealed bid. If a bid does not satisfy this condition, the discovery stage is executed to identify the bidder. Otherwise, the successful bid stage is executed.
Since anyone in the network can check the above condition, any illegal behavior by the manager can be detected.

[**Successful bid stage**]

In this stage, all the bidders who have made successful bids are identified. Here, we assume that only one bid has the lowest bid price. At the end of this subsection, the case in which multiple bids have the lowest bid price is considered.

(1) The manager determines the lowest bid price $price_{\min}$ among all revealed bid prices. Let $PERIOD\_NAME$ be the message that specifies the period in which the bidder offering $price_{\min}$ must reveal his name. The manager publishes $price_{\min} \| PERIOD\_NAME$ with his digital signature for it,

$$price_{\min} \| PERIOD\_NAME \\ \| DS_M(price_{\min} \| PERIOD\_NAME).$$

(2) During the period, the bidder offering $price_{\min}$ publishes his identifier, $UID_{\min}$, the non-interactive proof with the confirmation protocol for his undeniable signature in his bid, and the non-interactive proofs with the disavowal protocols for the undeniable signatures in the other bids. The confirmation protocol ensures that he cast the bid with $price_{\min}$, and the disavowal protocols ensure that the bid is his only one in the bidding session.

(3) If the identifier with the valid non-interactive proofs is not published, the discovery stage is executed to identify the bidder. Otherwise, the user with the identifier becomes the successful bidder. Since anyone in the network can verify the proof, any illegal behavior by the manager can be detected.

[**Discovery stage**]

This stage is executed if there are any bids, called illegal bids, that satisfy one of the following conditions:

(a) The bids are not revealed correctly in the revealing stage, or

(b) the identifier with the valid non-interactive proofs is not published in the successful bid stage.

In this stage, the parties who made the illegal bids, called illegal bidders, are identified.

(1) The manager requests every user in the participant group to publish the non-interactive proof with the disavowal protocol for the undeniable signature in every illegal bid. If the signature in the illegal bid is valid, the illegal bidder cannot publish any valid non-interactive proof with the disavowal protocol by using the verification key corresponding to him, though the other users can publish it. Thus, the illegal bidder can be identified. If the signature in the illegal bid is not valid, every user can publish the valid non-interactive proof with the disavowal protocol. Such an illegal bid is ignored and removed.

If this stage is called from the revealing stage, the successful bid stage follows. If it is called from the successful bid stage, the successful bid stage is re-executed after the removal of the illegal bid.

Remark 1: If the illegal bidder, called Alice, and someone else, called Bob, disobey the discovery stage, it is hard to determine which offered the illegal bid. However, in this case, it does not matter that some sanctions can be applied to Alice and Bob for their illegal actions. This is because the other users obeying the bidding protocol are not identified, and Alice and Bob disobeyed the bidding protocol. □

Remark 2: If someone offers a bid with a low price whose undeniable signature part is no one's signature, say a random sequence, the bid may be chosen as the lowest bid in Step 1 of the successful bid stage. But such a bid never becomes the successful bid, since its bidder cannot prove that he made the bid. In this case, the bid with the lowest price except for such bids is chosen as the successful bid. □

The sanctions to be taken against illegal bidders are beyond the scope of this protocol. As stated in Section 1, the sanctions should discourage bidders from making illegal bids.

We confirm that this protocol satisfies the conditions in Section 2.

Validity of public notices: Because of the anonymous broadcast network, the messages from the manager cannot be modified and can be seen by anyone in the network. Since all the messages are sent together with the digital signatures of the manager, the unforgeability of the digital signature scheme prevents anyone from pretending to be him.

Secrecy of bid prices: The bit commitment scheme prevents the bid prices from being disclosed before the deadline for bidding.

Impossibility of pretense: For a user U_i to try to pretend to be a valid user U_j, U_i must use a signature previously made by U_j, because of the unforgeability of the undeniable signature scheme. Since U_j's signatures used in the past bidding session have different bidding identifiers from the current identifier BID_ID, U_i cannot pretend to be U_j by using the signatures. In case of the signatures used in the current bidding session, since the signature is for the price itself that U_j offers in the bidding session, it is meaningless to use the signature.

Impossibility of multiple bids: In the successful bid stage, the bidder who offers the lowest price is made to prove that the bid with the lowest price is his only one in one bidding session. Thus, a bidder who bid more than once in a bidding session cannot become the successful bidder.

Validity of bid price: The anonymous broadcast network prevents anyone from modifying his committed price. And since it is difficult to find m' and r' with $m' \neq m$ and $BC(m, r) = BC(m', r')$ for m and r, the sender cannot also modify his bid price after the deadline for bidding.

Validity of successful bid: As stated in the description of the bidding, revealing, and successful bid stage, the price of the successful bid is the lowest bid price offered by any of the bidders who obeyed the protocol. The bids offered by bidders who obeyed the bidding stage protocol include valid undeniable signatures. Thus, if a bidder disobeys the revealing stage or the successful bid stage protocol, he is identified from his signature in the discovery stage.

Anonymity: Because of the anonymous broadcast network, the secrecy of the bit commitment, the anonymity of the undeniable signatures, and the zero-knowledge of the confirmation and disavowal protocols, it is difficult to identify a bidder only from a bid and public information for users.

Consider the case in which a CA is used to determine the correspondence between the verification key and the owner. Since no one except for the signer can determine whether or not the anonymous undeniable signature was made with a signing key corresponding to a verification key, as shown in Theorem 1, the CA cannot determine it, either. Therefore, the above observations regarding anonymity also hold in this case.

Here, we discuss the communication and computation complexities of our protocol (without any reliable center) and the existing protocols (with centers)[1)~4)]. In the existing protocols, informally a bid consists of a commitment to a bidding price and the bidder's digital signature, and the centers reveal the bidding prices to determine the successful bidder. Then, when the undeniable signature in Chaum[8)] is used in our protocol, the computational complexity of obtaining a bid and its length in our protocol are comparable with those in the existing protocols, since the undeniable signature is as efficient as normal digital signatures (e.g., the RSA signature and Schnorr signature). On the other hand, in our protocol, when illegal bidders are found, the communication and computation costs of identifying the illegal bidders, which depend on the number of members in the participant group must be added, though this is not so in existing protocols. However, by applying some sanctions against illegal bids, their incidence can be minimized.

Finally, we will discuss a tie, that is, the case in which multiple bids have the lowest bid price. As selection methods for resolving the tie, a lottery, re-bidding, and so on may be used. A protocol for accomplishing the selection method is called a selection protocol, and the lottery protocol of Sako[15)] and the bidding protocol proposed in this paper can be used for a lottery and re-bidding, respectively. When a selection protocol is applied to the tie break, the applied protocol, called the tie break protocol, should not violate the conditions for the anonymous bidding protocol in Section 2. Since the tie break influences only the impossibility of pretense, the validity of the successful bid, and anonymity, only these conditions are discussed. To satisfy them, in the tie break protocol, (a) messages sent from the participants should be anonymous and (b) the winner of the tie break should be a tied bidder. In addition, (c) it should be possible to link every participant in the tie break to a tied bid. This is required in order to determine whether or not each tied bidder participates in the tie break protocol, so that a tied bidder who does not participate in it can be identified as an illegal bidder disobeying the protocol. Hereafter, a tie break protocol is constructed for the lottery protocol of Sako[15)], though similar methods can be applied to other selection protocols, including the proposed bidding protocol. In the construction, the proof that two signatures are made by the same signer is used without revealing his identity. In the undeniable signature scheme[8)], the discrete logarithms of signatures of the same signer to the base message are all the same. Thus, if the equality of the discrete logarithms is proved, the equality of the signers of the signatures is proved. The equality of the discrete logarithms can be proved by using slightly modified version of the confirmation protocol, which is called the linkage protocol. Then, the tie break protocol for the lottery protocol is as follows: All messages from the participants are sent through the anonymous broadcast network. The participant signs the sent messages on the undeniable signature scheme, and proves that the signature is made by a signer of an undeniable signature in a tied bid. In the tie break protocol, only messages attached by the undeniable signature whose signer is the same as that of the undeniable signature in a tied bid are effective. If a tied bid whose bidder does not participate in the tie break protocol exists, the bidder is identified as in the discovery stage. After the anonymous winner has been selected by the lottery protocol, the successful bid stage is executed, where the winner is the bidder offering the lowest price.

4. Conclusion

An anonymous bidding protocol using an undeniable signature scheme has been proposed, which, like that of Imamura, et al.[5], does not require any reliable center. Furthermore, the validity of the successful bid, which is not satisfied in that of Imamura, et al.[5], is satisfied. In the proposed protocol, the manager has to communicate with every user in the participant group to identify illegal bidders only when their existence is detected. In Nakanishi, el al.[16], a linkable group signature scheme without any reliable center is proposed. If the linkable group signature scheme is used instead of the undeniable signature, an anonymous bidding protocol can be constructed, where the participant group can be partitioned into multiple groups, and thus the manager has only to communicate with every user in a smaller group to identify illegal bidders. However, the bidding stage requires the more communication costs, since the verifying protocol of the group signature must be executed, whose communication costs are proportional to the group size. Thus, the protocol using the undeniable signature is more efficient than that using the linkable group signature from the viewpoint that the identification of illegal bidders reduces their occurrence.

References

1) Sumida, M., Takata, T., Fujiwara, T. and Kasami, T.: A Protocol for Bidding, *Proc. 1991 Symposium on Cryptography and Information Security*, 12C (1991).

2) Franklin, M.K. and Reiter, M.K.: The Design and Implementation of a Secure Auction Service, *Proc. 1995 IEEE Symposium on Security and Privacy*, pp.2–14 (1995).

3) Kikuchi, H., Harkavy, M. and Tyger, D.: Multi-round Anonymous Auction Protocols, *Proc. IEEE Workshop on Dependable and Real-Time E-Commerce System*, pp.62–69 (1998).

4) Sako, K.: Universally Verifiable Auction Protocol Which Hides Losing Bids, *Proc. 1999 Symposium on Cryptography and Information Security*, pp.35–39 (1999).

5) Imamura, Y., Matsumoto, T. and Imai, H.: Electronic Anonymous Bidding Schemes, *Proc. 1994 Symposium on Cryptography and Information Security*, 11B (1994).

6) Nakanishi, T., Watanabe, H., Fujiwara, T. and Kasami, T.: An Anonymous Bidding Protocol Using Undeniable Signature, *Proc. 1995 Symposium on Cryptography and Information Security*, B1.4 (1995).

7) Miyazaki, S. and Sakurai, K.: A Bulletin Board-based Auction System with Protecting the Bidder's Strategy, *Proc. 1999 Symposium on Cryptography and Information Security*, pp.41–46 (1999).

8) Chaum, D.: Zero-Knowledge Undeniable Signatures, *Advances in Cryptology – EUROCRYPT '90*, LNCS, Vol.473, pp.458–464, Springer-Verlag (1991).

9) Fiat, A. and Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems, *Advances in Cryptology – CRYPTO '86*, LNCS, Vol.263, pp.186–194, Springer-Verlag (1987).

10) Pedersen, T.P.: Non-interactive and Information-theoretic Secure Verifiable Secret Sharing, *Advances in Cryptology – CRYPTO '91*, LNCS, Vol.1361, pp.129–140, Springer-Verlag (1991).

11) Tsiounis, Y. and Yung, M.: On the Security of ElGamal Based Encryption, *Proc. 1998 International Workshop on Practice and Theory in Public Key Cryptography*, LNCS, Vol.1431, pp.117–134, Springer-Verlag (1998).

12) Chaum, D. and van Heijst, E.: Group Signatures, *Advances in Cryptology – EUROCRYPT '91*, LNCS, Vol.547, pp.241–246, Springer-Verlag (1991).

13) Camenisch, J. and Stadler, M.: Efficient Group Signature Schemes for Large Groups, *Advances in Cryptology – CRYPTO '97*, LNCS, Vol.1294, pp.410–424, Springer-Verlag (1997).

14) Chaum, D.: Untraceable Electronic Mail,

Return Addresses, and Digital Pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88 (1981).

15) Sako, K.: Drawing Lots Using E-mails, *Proc. 1997 Symposium on Cryptography and Information Security*, 27C (1997).

16) Nakanishi, T., Fujiwara, T. and Watanabe, H.: A Linkable Group Signature and its Application to Secret Voting, *Trans. IPS Japan*, Vol.40, No.7, pp.3085–3096 (1999).

(Received November 30, 1999)
(Accepted June 1, 2000)

Toru Nakanishi was born in Kagawa, Japan, on May 22, 1971. He received the M.E. degree in information and computer sciences from Osaka University, Toyonaka, Osaka, Japan, in 1995. He is currently a research associate of the Department of Communication Network Engineering, Okayama University, Okayama, Japan. His research interests are cryptography, information security, and network security.

Toru Fujiwara was born in Wakayama, Japan, on June 18, 1958. He received the B.E., M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Toyonaka, Osaka, Japan, in 1981, 1983 and 1986, respectively. In 1986 he joined the faculty of Osaka University. In 1989–1990 he was on leave as a Post Doctoral Fellow in the Department of Electrical Engineering, University of Hawaii, Honolulu. In 1992–1997, he was an Associate Professor at the Department of Information and Computer Sciences, Osaka University. Since 1997, he has been a professor at the Department of Informatics and Mathematical Science, Osaka University. His current research interests include coding theory and cryptography. Dr. Fujiwara is a member of the Institute of Electrical and Electronics Engineers, Inc. and the Information Processing Society of Japan.

Hajime Watanabe was born in Nara, Japan, on November 3, 1968. He received the B.E., M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Osaka, Japan, in 1991, 1993 and 1997, respectively. From 1994 to 1999, he was a research associate of Graduate School of Information and Science, Nara Institute of Science and Technology, Nara, Japan. In October 1999, He joined Electrotechnical Laboratory, Tsukuba, Japan. His research interests are cryptography and information security.