INFORMATION
SCIENCE
TECHNICAL
REPORT

NAIST-IS-TR99002
ISSN 0919-9527

Anonymous Bidding Protocols Using an Anonymous Undeniable Signature

Toru Nakanishi, Toru Fujiwara
and Hajime Watanabe

January 1999

NAIST

〒 630-0101
奈良県生駒市高山町 8916-5
奈良先端科学技術大学院大学
情報科学研究科

Graduate School of Information Science
Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, Nara 630-0101, Japan

Anonymous Bidding Protocols Using an Anonymous Undeniable Signature Scheme

Toru NAKANISHI,[†]

Toru FUJIWARA[††] and

Hajime WATANABE[†††]

[†] Department of Information Technology,
Faculty of Engineering, Okayama University,
Okayama 700-0082, Japan

[††] Department of Informatics and Mathematical Science,
Graduate School of Engineering Science, Osaka University,
Toyonaka, Osaka 560-8531 Japan

[†††] Graduate School of Information Science,
Nara Institute of Science and Technology,
Ikoma, Nara 630-0101 Japan

SUMMARY Anonymous bidding protocols using an anonymous undeniable signature scheme without assuming the existence of any reliable center are proposed. The anonymity of a bidding protocol means that the participation of anyone to the bidding except for a successful bidder is kept secret. For simplicity, assume that the bidder who bids the lowest price is chosen as the successful bidder. Then we point out that fairness of an anonymous bidding would be violated if it is possible for the bidder who bids the lowest price not to reveal his name and to withdraw the bid. Thus the key to construct the anonymous bidding protocol is to give a method for identifying the bidder who bids the lowest price but does not reveal his name. An anonymous bidding protocol proposed so far solves this problem by assuming the existence of reliable centers. Instead of assuming the existence of any reliable center, an anonymous undeniable signature scheme is used in this paper. The anonymity of a signature scheme means that anyone cannot distinguish a signature of a signer from that of another. The validity of a signature in the anonymous undeniable signature scheme is verified by an interactive manner. The true signer cannot repudiate his signature and the others can repudiate it. Thus by communicating with all candidates of the signer, it is possible to identify the true signer. In this paper, it is proved that the anonymous undeniable signature scheme can be constructed. A basic bidding protocol using the anonymous undeniable signature scheme is presented first, where the manager of the bidding has to communicate with every user in the network to identify illegal bidders, only when the existence of them is detected. By grouping users, we construct a modified protocol where the manager has only to communicate with every user in some specified groups to identify illegal bidders.
key words: bidding, cryptographic protocol, anonymity, undeniable signature scheme

1. Introduction

Many cryptographic protocols for bidding, voting, and so on have been proposed, say [1] – [5]. This paper deals with bidding protocols. All the users in a network do not necessary to participate in a bidding. A user who offers a price for the bidding is called a bidder. Hereafter, for simplicity, we assume that the bidder who bids the lowest price is chosen as the successful bidder.

A bidding protocol is desirable to be anonymous in the sense that the participation of a user to the bidding who obeys the protocol but is not a successful bidder is kept secret from anyone. This is because the price can be used to estimate bidder's ability which is useful for the conspiracy on the future bidding [2].

The anonymous bidding protocol proposed in [1] assumes that reliable centers exist. In the protocol, the reliable centers know the correspondence between bidders and bids, and they choose the bidder who bids the lowest price as the successful bidder. But it is assumed that they do not disclose the correspondence. In [3], an anonymous auction protocol, where the anonymity is not violated even if reliable centers conspire, is proposed. In the protocol, each bidder divides the digital cash of his bid price into pieces by a secret sharing scheme and sends them to multiple centers, one for each center. This means that any bidder has to deposit his bid price to the centers. This protocol is appropriate for the type of bidding where a bidder offers an amount which the bidder will spend in purchasing the bidden target. An example of bidding in this type is a bidding of real estate held by a court. But this protocol is not appropriate for the type of bidding where a bidder offers an amount which the bidder will get in selling the bidden target. An example of bidding in this type is a bidding of a public undertaking held by a public organization.

In [2], a protocol without any reliable center is proposed. In the protocol, all bid prices become public after all bidders bid, and the bidder who bids the lowest price reveals his name by himself. If the bidder does not reveal his name, it is impossible to identify him. Hence the bid with lowest price must be ignored and the bid with the second lowest price is chosen as the successful bid. Then, fairness of the bidding would be violated as shown in the following example. 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 $price_{min}$, which seems to be minimum in the bidding, and Bob bids $price_{real}$ with $price_{real} > price_{min}$.

2. After all bid prices became public, suppose that $price_{min}$ is the lowest. They check whether anyone bids $price$ with $price_{real} > price > price_{min}$ or not. If one bids, Alice reveals her name and becomes a successful bidder. Otherwise, Alice does not reveal her name and later Bob is chosen as the successful bidder.

This violates fairness since Alice and Bob may choose the price for the successful bid after they know others' bid prices. The key to construct the anonymous bidding protocol is to give a method for identifying the bidder who bids the lowest price even when he does not want to reveal his name.

In this paper, in order to resolve the above problem without assuming the existence of any reliable center, an anonymous undeniable signature scheme, a variant of the undeniable signature scheme [6]–[8], is used. The anonymity of a signature scheme means that anyone cannot distinguish a signature of a signer from that of another. The validity of a signature in the anonymous undeniable signature scheme is verified by an interactive proof scheme with a candidate of the signer. The true signer cannot repudiate his signature while the others can. By communicating with all candidates of the signer, it is possible to identify the true signer. When each bidder is forced to attach the signature to his bid, it becomes possible to identify the bidder who bids the lowest price even if he does not reveal his name by himself.

In Section 2, conditions which anonymous bidding protocols should satisfy are observed. In Section 3, it is shown that the anonymous undeniable signature scheme used in the proposed anonymous bidding protocols can be constructed. In Section 4, a basic protocol is constructed, where the manager of the bidding has to communicate with every user in the network to identify illegal bidders, only when the existence of them is detected. By grouping users, we construct a modified protocol where the manager has only to communicate with every user in some specified groups to identify illegal bidders.

2. Conditions for anonymous bidding protocols

This section observes conditions which anonymous bidding protocols should satisfy. We call a protocol satisfying the following conditions an *anonymous bidding protocol*.

1. **Validity of public notices:** Information of the bidding from the manager 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 of the bid, valid bid prices cannot be leaked to the others.

3. **Impossibility of pretense:** No one can act for another user as a valid bidder.

4. **Validity of bid prices:** Valid bid prices cannot be modified by the others. After the deadline of the bid, any bidder cannot modify his bid price.

5. **Validity of successful bid:** The price of the successful bid is the lowest in all bid prices.

6. **Anonymity:** The participation to the bidding of a user in the network who obeys the protocol but is not the successful bidder is kept secret from anyone.

We do not prohibit for a bidder to offer multiple bids. Even if a bidder offers multiple bids, the effective bid can be defined as the bid with the lowest price among them because these bids are well-ordered. Since the bid prices of other valid bidders cannot be leaked from Condition 2, offering multiple bids is meaningless. The problem described in Section 1 that the bidder who bids the lowest price does not reveal his name is against Condition 5, validity of successful bid.

Two specific anonymous bidding protocols are presented in Section 4. Before describing them, it is shown that the anonymous undeniable signature scheme used in the protocols can be constructed.

3. Anonymous undeniable signature scheme

In [7], a practical undeniable signature scheme is proposed, whose security is based on the following assumption: It is infeasible to compute the discrete logarithm modulo a large prime number. In [9], a group signature scheme is proposed, where the group signature scheme satisfies the followings: (1) Only members of the group can sign messages, and anyone can determine whether or not a given signature is a valid signature of a member of the group.

(2) From a signature only, anyone except for the signer and any authority cannot identify the member of the group who signed. (3) In case of dispute later on, the signer of a signature can be identified. The group signature scheme [9] is derived from the undeniable signature scheme [7]. The anonymity of the group signature scheme holds under the assumption that the undeniable signature scheme is anonymous. Under the assumption, the practical anonymous undeniable signature scheme is adopted to construct the proposed anonymous bidding protocols. In the remainder of this section, the computational anonymity of the signature scheme is formally defined, and, under the general assumption that a one-to-one one-way function exists, it is proved that an anonymous undeniable signature scheme can be constructed.

For a message m and a signer's identifier (ID) i, consider a probabilistic polynomial time algorithm which outputs i's signature for m. Here we assume that only polynomially bounded resources are available for adversaries.

We define the computational anonymity of a probabilistic signature scheme as the analogue of the security of probabilistic encryptions. There are three definitions of the security of probabilistic encryptions, and these three definitions have been proved to be equivalent [10]. Among them, the definition based on the computational indistinguishability can be stated intuitively as follows: For any pair of messages, m_0 and m_1, any probabilistic polynomial time algorithm (called distinguisher) cannot distinguish a ciphertext of m_0 from that of m_1.

Intuitively, a probabilistic signature scheme is computationally anonymous if, for any pair of the signers, i_0 and i_1, any distinguisher cannot distinguish a signature of i_0 from that of i_1. A sequence of signers is called a *signer sequence* and a sequence of signatures is called a *signature sequence*. For a signer sequence $\bar{i} = (i_1, i_2, \ldots, i_k)$, a sequence $(s_1, s_2, \ldots, s_k)$ is called a signature sequence of $\bar{i}$ if s_j is a signature of signer i_j with $1 \leq j \leq k$. Even if a distinguisher cannot distinguish a signature from another one, it may distinguish signature sequences. For example, consider two signer sequences (Alice, Alice) and (Alice, Bob), and a signature scheme, where, given any signature sequence (s_1, s_2), a receiver of the sequence can verify whether the signer of s_1 is the same as that of s_2 or not. Then, the distinguisher can distinguish a signature sequence of (Alice, Alice) from that of (Alice, Bob), even if he cannot distinguish a signature of Alice from that of Bob. For this reason, the computational anonymity of a probabilistic signature scheme will be defined on a signature sequence.

Let n be a security parameter. We use the following definition:

Definition 1: $f(n)$ is *negligible* in n if, for any positive constant c, there exists a constant, n_0, such that $f(n) < 1/n^c$ for any $n > n_0$.

Let $A(x_1, x_2, \ldots, x_k)$ be a probabilistic algorithm A with k inputs $x_1, x_2, \ldots, x_k$, and let $\mathcal{R}(A)$ be the range of A, that is, the set of outputs of A. For fixed values $t_1, t_2, \ldots, t_k$, $A(t_1, t_2, \ldots, t_k)$ can be regarded as a source which takes a value with the probability that $A(t_1, t_2, \ldots, t_k)$ outputs the value. If $A(\cdots)$ and $B(\cdots)$ are probabilistic algorithms, $A(\cdots B(\cdots)\cdots)$ is the probabilistic algorithm obtained by composing A and B (i.e. running A on B's output). For a source A and an output of A, a, let $Pr(A = a)$ be the probability that A outputs a. Let $t(n)$ (or simply t) be an integer bounded by a polynomial of n. Given t and a probabilistic signature scheme $\mathcal{S}$, we use the following probabilistic polynomial time algorithms to define the computational anonymity of a probabilistic signature scheme:

Signer sequence generator I**:** I outputs t signer IDs.

Message sequence generator M**:** M outputs t messages.

Signature sequence generator $SIGN$**:** Given a probabilistic signature scheme $\mathcal{S}$, let $sign(i, m)$ be a signing algorithm for signer i and message m on $\mathcal{S}$. $SIGN(\overline{i}, \overline{m})$ for $\mathcal{S}$ outputs t signatures $\overline{s} = (sign(i_1, m_1),\ sign(i_2, m_2),\ \ldots,\ sign(i_t, m_t))$ on inputs $\overline{i} = (i_1, i_2, \ldots, i_t) \in \mathcal{R}(I)$ and $\overline{m} = (m_1,\ m_2,\ \ldots,\ m_t) \in \mathcal{R}(M)$.

Distinguisher D**:** D outputs a bit on inputs $\overline{i_0}, \overline{i_1} \in \mathcal{R}(I)$ and $\overline{s} \in \mathcal{R}(SIGN(I, M))$.

Then, the computational anonymity of a probabilistic signature scheme is defined as follows:

Definition 2: A probabilistic signature scheme $\mathcal{S}$ is *computationally anonymous* if, for any I, M, and D, $|Pr(D(\overline{i_0}, \overline{i_1}, SIGN(\overline{i_0}, \overline{m_0})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN(\overline{i_1}, \overline{m_1})) = 1)|$ is negligible for any $\overline{i_0}, \overline{i_1} \in \mathcal{R}(I)$ and $\overline{m_0}, \overline{m_1} \in \mathcal{R}(M)$, where $SIGN$ is a signature sequence generator for $\mathcal{S}$.

Definition 2 means that a probabilistic signature scheme $\mathcal{S}$ is anonymous if, for any pair of signer sequences, $\overline{i_0}$ and $\overline{i_1}$, any probabilistic polynomial time algorithm cannot distinguish a signature sequence of $\overline{i_0}$ from that of $\overline{i_1}$.

Next we construct a secure anonymous undeniable signature scheme. The convertible undeniable signature scheme is a variant of the undeniable signature scheme, where an undeniable signature becomes a normal digital signature if the signer reveals a secret key. Chaum et al. proved constructively that a secure convertible undeniable signature scheme exists if and only if a secure digital signature scheme exists [8]. In the following, we briefly review the scheme. Since we do not need convertibility for the applications of the scheme in Section 4, we consider a simplified scheme without convertibility. Afterward, we show that the simplified scheme is computationally anonymous.

First we follow the definition of the pseudo-random generator in [11]. It can be constructed from the hard-core bits of any one-way function [11],[12].

Definition 3: [Pseudo-random generator PRG] Let $l(n)$ (or simply l) be an integer bounded by a polynomial of n such that $l(n) > n$. Let D^R be a probabilistic polynomial time algorithm which outputs a bit on inputs t bit-strings of length l. A function $PRG : \{0,1\}^n \mapsto \{0,1\}^l$ is said to be a *pseudo-random generator* if, for any D^R, $|Pr(D^R(\overline{x}) = 1) - Pr(D^R(\overline{p}) = 1)|$ is negligible for $\overline{x} = (x_1, x_2, \ldots, x_t)$ and $\overline{p} = (PRG(y_1), PRG(y_2), \ldots, PRG(y_t))$ with truly random sequences $x_i \in \{0,1\}^l$ and $y_i \in \{0,1\}^n$ for $1 \leq i \leq t$.

Note that, for any $l(n)$, a pseudo-random generator PRG can be constructed [11],[12]. Let $PRG_i(r)$ be the i-th bit of $PRG(r)$. We use the following well-known encryption scheme using the pseudo-random generator for enough large l.

Encryption Scheme $E(m, r)$**:** Let $u(n)$ (or simply u) be an integer with $u(n) \leq l(n)$. For a message $m = (b_1, b_2, \ldots, b_u)$ where $b_i \in \{0,1\}$ with $1 \leq i \leq u$ and a truly random sequence $r \in \{0,1\}^n$, the encryption algorithm $E(m, r)$ outputs $(PRG_{a \cdot u+1}(r) \oplus b_1, PRG_{a \cdot u+2}(r) \oplus b_2, \ldots, PRG_{(a+1) \cdot u}(r) \oplus b_u, a)$, where a is an integer with $0 \leq a < \lfloor l/u \rfloor$ which indicates the part used in $PRG(r)$. If E is used multiple times for the same random sequence r, the different parts in $PRG(r)$ must be used. For simplicity, a is initially set as 0, and is incremented by 1 after the sequence $(PRG_{a \cdot u+1}(r), PRG_{a \cdot u+2}(r), \ldots, PRG_{(a+1) \cdot u}(r))$ is used for the encryption.

Now we present a simplified version of the signature scheme in [8]. We call the simplified version AUS, where AUS stands for the anonymous undeniable signature. The difference between them is explained later. In the signature scheme in [8] and AUS, the digital signature

scheme which is not existentially forgeable against adaptive chosen message attacks is used. Hereafter we call this signature scheme simply the secure digital signature scheme.

Signature scheme AUS [8]**:** Let sk and pk be signer i's secret key and public key on a secure digital signature scheme and let $BC(m, r)$ be a bit commitment for a message m and a random sequence r. On AUS, the signer i's secret keys are sk, K, and R, where K and R are chosen randomly by him, and his public keys are pk and $PK = BC(K, R)$. Note that the length of K is n since K is used as the random input of E, and the length of R depends on the bit commitment scheme.

Let $s(m)$ be i's secure digital signature for m. Then i's signature for m on AUS, $sign(i, m)$, is given by

$$sign(i, m) = E(s(m), K),$$

where E is the above encryption algorithm. Note that i can make $\lfloor l/u \rfloor$ signatures for a fixed K.

The verifying protocol of AUS is as follows: Let $V^i(m, s)$ be the function verifying the validity of i's secure digital signature s, i.e.

$$V^i(m, s) = \begin{cases} 1, & \text{for } s \in \sigma^i(m), \\ 0, & \text{otherwise,} \end{cases}$$

where $\sigma^i(m)$ is the set of signer i's secure digital signatures for message m. When i proves that a string Str is i's valid signature, he proves that he knows K, R, and s which satisfy $P1 \wedge P2 \wedge P3 = 1$ with the general zero-knowledge interactive proof (ZKIP) protocol of [13] for NP languages, where $P1$, $P2$, and $P3$ are the following predicates:

$(P1)$ $PK = BC(K, R)$.

$(P2)$ $Str = E(s, K)$, for some a with $0 \leq a < \lfloor l/u \rfloor$.

$(P3)$ $V^i(m, s) = 1$.

When i proves that a string Str is not i's valid signature, he proves that he knows K, R, and s which satisfy $P1 \wedge P2 \wedge \overline{P3} = 1$ with the general ZKIP protocol.

Remark 1: If one proves that $P1$ is true, K becomes a fixed value which satisfies $PK = BC(K, R)$. When i proves that Str is not i's valid signature, i only has to prove $Str = E(s, K)$ with his K and $V^i(m, s) \neq 1$. Also, without proving $P1$, the signer can prove that $Str = E(s, K)$ and $V^i(m, s) \neq 1$ since he can choose another K. This is why the predicate $P1$ is required as well as the predicates $P2$ and $P3$.

Remark 2: There are two types of bit commitment scheme, interactive one and non-interactive one. An interactive scheme can be constructed from any one-way function [14]. The non-interactive probabilistic encryption scheme in [15], which is secure in the sense of the definition based on the computational indistinguishability in [10], can be constructed from any one-to-one one-way function [13]. Note that our anonymity of a probabilistic signature scheme is also defined based on the computational indistinguishability. Let $\overline{E}(m, r)$ be the probabilistic encryption algorithm in the scheme [15] for a message m and a random sequence, key, r. Then, it holds that, if $\overline{E}(m, r) = \overline{E}(m', r')$, $m = m'$. This means that the encryption scheme can be used as a non-interactive bit commitment scheme. Thus, the non-interactive scheme can be constructed from any one-to-one one-way function. The construction of a non-interactive scheme from any one-way function is unknown. We adopt a non-interactive bit commitment scheme for efficiency. Theorem 1 stated below also holds when an interactive scheme is used.

The difference between AUS and the original scheme in [8] is as follows: A signature in the original scheme is $BC(s(m), f_K(m))$ where $f_K(m)$ is pseudo-random function for m using key K [16], while that in AUS is $E(s(m), K)$. Since $f_K(m)$ is used to convert an undeniable signature into a digital signature, $f_K(m)$ is not required in an unconvertible undeniable signature. As shown in [8], the bit commitment in the original scheme can be replaced by an encryption scheme. We use the encryption scheme E in AUS for simplicity. We can prove Lemma 1 in a similar way that the original scheme in [8] is proved to be secure undeniable since the difference between AUS and the original scheme does not influence the proof. However, whether or not Lemma 2 holds for the case where $E(s(m), K)$ is replaced by $E(s(m), f_K(m))$ is open. This is because, in the above encryption scheme E, the second argument is given to the input of PRG but $f_K(m)$ is not a truly random sequence. It is only proved in [11], [12]

that the output of PRG is computationally indistinguishable from a truly random sequence if the input is a truly random sequence.

Lemma 1: AUS is a secure undeniable signature scheme.

Next, we prove the computational anonymity.

Lemma 2: AUS is computationally anonymous if pseudo-random generator PRG exists.

Proof: Consider the following variant of AUS, denoted $\mathrm{AUS_{TR}}$: A signature on $\mathrm{AUS_{TR}}$ is constructed by using a truly random sequence instead of $PRG(r)$ in encryption E. Let $SIGN^{\mathrm{AUS}}$ be a signature sequence generator for AUS, and let $SIGN^{\mathrm{AUS_{TR}}}$ be a signature sequence generator for $\mathrm{AUS_{TR}}$. Let $SIGN^{\mathrm{DS}}$ be a signature sequence generator for the secure digital signature $s(m)$ used in AUS.

First, we prove that

$$\forall I, \forall M, \forall D, \forall \overline{i_0}, \overline{i_1} \in \mathcal{R}(I), \forall \overline{m_0} \in \mathcal{R}(M), \forall c, \exists n_0, \forall n > n_0 :$$

$$|Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_0}, \overline{m_0})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})) = 1)| < 1/n^c, \quad (1)$$

if pseudo-random generator PRG exists.

Assume that there are I, M, D, $\overline{i_0}, \overline{i_1} \in \mathcal{R}(I)$ and $\overline{m_0} \in \mathcal{R}(M)$ such that $|Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_0}, \overline{m_0})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})) = 1)|$ is not negligible. Define $\overline{s_0} = (s_1, s_2, \ldots, s_t) \stackrel{\triangle}{=} SIGN^{DS}(\overline{i_0}, \overline{m_0})$. Let $\overline{i_0} = (i_1, i_2, \ldots, i_t)$. We prove the statement (1) by contradiction, that is, under this assumption, we show that there exists a probabilistic polynomial time algorithm D^R which contradicts the existence of PRG. Note that our subgoal is to show the **existence** of D^R, and hence we need not to give a procedure to find $\overline{i_0}, \overline{i_1}$ and $\overline{s_0}$. The signer sequence $\overline{i_0}$ may contain a signer twice or more. For $1 \leq j \leq t$, let $\mathrm{first}(i_j)$ denote the smallest integer j_0 such that $i_j = i_{j_0}$ with $1 \leq j_0 \leq j$, and let $\mathrm{turn}(i_j)$ denote the number of i_k such that $i_k = i_j$ with $1 \leq k < j$. For a sequence $z \in \{0,1\}^l$ and $0 \leq j < t$, let $\mathrm{part}(z, j)$ denote the subsequence from the $(ju+1)$-th bit to the $(j+1)u$-th bit of z.

Now, we present the algorithm D^R for D, $\overline{i_0} = (i_1, i_2, \ldots, i_t), \overline{m_0}$ and $\overline{s_0} = (s_1, s_2, \ldots, s_t)$.

1. The input of D^R is a t-tuple of $\{0,1\}^l$, denoted $(z_1, z_2, \ldots, z_t)$.

2. The output of D^R is $D(\overline{i_0}, \overline{i_1}, (v_1, v_2, \ldots, v_t))$, where v_j is the bit-wise XOR of s_j and $\mathrm{part}(z_{\mathrm{first}(i_j)}, \mathrm{turn}(i_j))$ for $1 \leq j \leq t$.

We will show that $|Pr(D^R(\overline{x}) = 1) - Pr(D^R(\overline{p}) = 1)|$ is not negligible for $\overline{x} = (x_1, x_2, \ldots, x_t)$ and $\overline{p} = (PRG(y_1), PRG(y_2), \ldots, PRG(y_t))$ with truly random sequences $x_i \in \{0,1\}^l$ and $y_i \in \{0,1\}^n$ for $1 \leq i \leq t$ (refer to Definition 3). If the input of D^R, $(z_1, z_2, \ldots, z_t)$, is $(x_1, x_2, \ldots, x_t)$, the probability distribution of $(v_1, v_2, \ldots, v_t)$ is the same as that of $SIGN^{\mathrm{AUS_{TR}}}(\overline{i_0}, \overline{m_0})$. This is because the signature on $\mathrm{AUS_{TR}}$ is the bit-wise XOR between the digital signature for a message and a truly random sequence. If the input $(z_1, \ldots, z_t)$ is $(PRG(y_1), PRG(y_2), \ldots, PRG(y_t))$, the probability distribution of $(v_1, v_2, \ldots, v_t)$ is the same as that of $SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})$. This holds owing to the followings: The signature on AUS is the bit-wise XOR between the digital signature for a message and a part of $PRG(y)$ for a truly random sequence y, where y is fixed for each signer and the part of $PRG(y)$ used for the signature on AUS is the subsequence from the $(au+1)$-th bit to the $(a+1)u$-th bit of $PRG(y)$ when one signer computes the $(a+1)$-th signature with $0 \leq a < t$. v_j is also the bit-wise XOR between digital signature s_j and a part of $PRG(y_j)$ for $1 \leq j \leq t$, where y_j is fixed for each signer and the part of $PRG(y_j)$ used for v_j is the subsequence from the $(au+1)$-th bit to the $(a+1)u$-th bit of $PRG(y_j)$ when one signer computes the $(a+1)$-th signature with $0 \leq a < t$. From the sameness of the probability distributions, we have that

$$Pr(D^R(\overline{x}) = 1) = Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_0}, \overline{m_0})) = 1), \text{ and}$$

$$Pr(D^R(\overline{p}) = 1) = Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})) = 1),$$

for $\overline{x} = (x_1, x_2, \ldots, x_t)$ and $\overline{p} = (PRG(y_1), PRG(y_2), \ldots, PRG(y_t))$ with truly random sequences $x_i \in \{0,1\}^l$ and $y_i \in \{0,1\}^n$ for $1 \leq i \leq t$. Therefore, from the assumption, $|Pr(D^R(\overline{x}) = 1) - Pr(D^R(\overline{p}) = 1)|$ is not negligible. This contradicts the existence of PRG.

Similarly,

$$\forall I, \forall M, \forall D, \forall \overline{i_0}, \overline{i_1} \in \mathcal{R}(I), \forall \overline{m_1} \in \mathcal{R}(M), \forall c, \exists n_0, \forall n > n_0 :$$

$$|Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_1}, \overline{m_1})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_1}, \overline{m_1})) = 1)| < 1/n^c. \quad (2)$$

Let

$$\alpha = Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_0}, \overline{m_0})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})) = 1), \quad (3)$$

$$\beta = Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_1}, \overline{m_1})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_1}, \overline{m_1})) = 1). \quad (4)$$

Inequalities (1) and (2) can be rewritten as

$$\forall I, \forall M, \forall D, \forall \overline{i_0}, \overline{i_1} \in \mathcal{R}(I), \forall \overline{m_0}, \overline{m_1} \in \mathcal{R}(M), \forall c, \exists n_0, \forall n > n_0 : |\alpha| < 1/n^c \text{ and } |\beta| < 1/n^c. \quad (5)$$

Encryption E is the bit-wise XOR of a message and a part of $PRG(r)$. Therefore when truly random sequence is used instead of $PRG(r)$, all values in $\mathcal{R}(SIGN^{\mathrm{AUS_{TR}}}(I, M))$ are equally likely. Thus,

$$\forall I, \forall M, \forall D, \forall \overline{i_0}, \overline{i_1} \in \mathcal{R}(I), \forall \overline{m_0}, \overline{m_1} \in \mathcal{R}(M), \forall c, \exists n_0, \forall n > n_0 :$$

$$|Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_0}, \overline{m_0})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS_{TR}}}(\overline{i_1}, \overline{m_1})) = 1)| < 1/n^c. \quad (6)$$

By applying (3) and (4) to (6), we have that

$$\forall I, \forall M, \forall D, \forall \overline{i_0}, \overline{i_1} \in \mathcal{R}(I), \forall \overline{m_0}, \overline{m_1} \in \mathcal{R}(M), \forall c, \exists n_0, \forall n > n_0 :$$

$$|Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})) = 1) + \alpha - (Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_1}, \overline{m_1})) = 1) + \beta)| < 1/n^c.$$

Therefore, from (5),

$$\forall I, \forall M, \forall D, \forall \overline{i_0}, \overline{i_1} \in \mathcal{R}(I), \forall \overline{m_0}, \overline{m_1} \in \mathcal{R}(M), \forall c, \exists n_0, \forall n > n_0 :$$

$$|Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_0}, \overline{m_0})) = 1) - Pr(D(\overline{i_0}, \overline{i_1}, SIGN^{\mathrm{AUS}}(\overline{i_1}, \overline{m_1})) = 1)| < 1/n^c.$$

Thus AUS is computationally anonymous. □

From Lemmas 1 and 2, AUS is a secure anonymous undeniable signature scheme. Next theorem shows that AUS can be constructed from a one-to-one one-way function.

Theorem 1: The secure anonymous undeniable signature scheme AUS can be constructed if a one-to-one one-way function exists.

Proof: Assume that a one-to-one one-way function exists. Then, as shown in [11] and [12], we can construct the pseudo-random generator from the hard-core bits of the one-way function, and so the above encryption scheme. As shown in [17], we can construct a secure digital signature scheme, and as shown in [13], we can construct a bit commitment scheme. Thus we can construct AUS by the same way as the original scheme in [8]. □

4. Anonymous bidding protocol

4.1 Basic protocol

This subsection proposes a basic bidding protocol satisfying the six conditions in Section 2.

4.1.1 Environment

In [2], the existence of *anonymous broadcast network* is assumed. 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 [18]. We construct the protocol in the anonymous broadcast network.

This protocol has the following entities.

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

Note that the manager is not needed to be a reliable authority.

Users: Persons or organizations in a network. Some of them will participate in the bidding. They publish their public keys and keep their secret keys on an anonymous undeniable signature. The registration of users are not included in this protocol.

4.1.2 Operations

The following operations are used in this protocol.

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

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

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

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

As we show in Section 3, secure digital signature scheme, secure anonymous undeniable signature scheme, and bit commitment scheme can be constructed if a one-to-one one-way function exists.

4.1.3 Protocol

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

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

1. Let M_BID be the message which specifies the contents of the bidding and the period of the bid, and BID_ID be the identifier of the bidding which is different from those of the other bidding. 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 $price_i$ and a random sequence r_i. He computes his anonymous undeniable signature for the concatenation of BID_ID and the bit commitment. Within 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 anonymous undeniable signature scheme prevents the repudiation of the bid and the pretense by the other bidders. The bit commitment scheme assures the validity of the bid price and the secrecy of it.

[Revealing stage] After the period of the bid, 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 in anonymity.

1. Let $PERIOD\_REV$ be the message which specifies the period when the bidders must reveal the contents of their bit commitments. The manager publishes $PERIOD\_REV$

with his digital signature for $PERIOD\_REV$,

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

2. Within the period, the bidder U_i publishes the concatenation of $price_i$, r_i, and his bid,

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

3. The manager checks whether each bid satisfies the following condition or not: The bit commitment in the bid can be opened by r_i, and the price in the bit commitment is the same as $price_i$. If there is a bid which does not satisfy the condition or is not revealed, the discovering stage is executed to identify the bidder. Otherwise, the successful bid stage is executed.

   Since anyone in the network can check the above condition as well, the illegal operations by the manager can be detected.

[**Successful bid stage**] In this stage, the bidder who makes a successful bid is decided and his validity is checked.

1. The manager decides the lowest bid price $price_{min}$ in all bid prices, and publishes it with his signature for it,

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

2. The bidder who bids the price publishes his user identifier,

$$UID_{min}.$$

3. If the bidder who bids the lowest price does not reveal his identifier, the discovering stage is executed to identify the bidder. Otherwise, the manager verifies the bidder revealing his identifier by using the verifying protocol of the anonymous undeniable signature scheme. If he is not valid, his bid is removed and we return to Step 1 in this stage. Otherwise, the bidder becomes the successful bidder.

[**Discovering stage**] This stage is executed, if there are bids which satisfy one of the following conditions:

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

(b) The bid has the lowest price but the owner of the bid does not reveal his identifier in the successful stage.

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

1. The manager communicates with every user in the network by using the verifying protocol of the anonymous undeniable signature scheme. If the signature in the illegal bid is valid, then the signer of it cannot repudiate it and the others can repudiate it. Thus the manager can identify the illegal bidder for each illegal bid. If the signature is not valid, every user can repudiate it. The illegal bid is ignored and removed.

Remark 3: If someone offers a bid with very low price whose undeniable signature is replaced by 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 become the successful bid since the bidder of it cannot prove that he is the bidder of it. The bid with the lowest price among the bids except for such bids is chosen as the successful bid.

In this protocol, the manager has to communicate with every user in the network to identify illegal bidders. In the next subsection, by grouping users, we construct a modified protocol where the manager has only to communicate with every user in some specified groups to identify illegal bidders. As mentioned later, the modified protocol is better in the communication cost but the basic protocol is better in the anonymity.

We confirm that the basic 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 digital signatures of the manager, the unforgeability of the digital signature scheme prevents anyone from pretending him.

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

Impossibility of pretense: There are two ways for a user U_i to try to pretend a valid user U_j. One is that U_i makes the anonymous undeniable signature for the message which U_j have not made so far. But this is hard because of the unforgeability of the anonymous undeniable signature scheme. The other is that U_i uses the signature which U_j made so far. Since U_j's signatures used in the past bidding have different bidding identifiers from the current identifier BID_ID, U_i cannot pretend U_j by using the signatures. In case of the signatures used in the current bidding, since the signature is for the price which U_j offers in the bidding, it is meaningless to use the signature.

Validity of bid price: The anonymous broadcast network prevents anyone from modifying the prices committed. 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 of the bid.

Validity of successful bid: It is possible to identify the bidder who does not properly reveal his bid price at the revealing stage, or who bids the lowest price but does not reveal his identifier at the successful bid stage. Thus the bidder who bids the lowest price is always chosen as a successful bidder.

Anonymity: Because of the anonymous undeniable signature scheme and the anonymous broadcast network, it is difficult to identify the bidder only from a bid and public information for users. Thus the anonymity holds.

4.2 Modified protocol

By grouping users, we construct a modified protocol where the manager has only to communicate with every user in some specified groups to identity illegal bidders.

4.2.1 Environment

We add the following to the participants for the basic protocol.

Group center: Center which computes each group's identifier GID_j, its secret key and its public key on the digital signature scheme.

Group administrators: Each administrator registers users for his group and controls the information of the users. He has the group's secret key on the digital signature scheme and distributes it to the users in the group. He computes the users' identifiers and publishes them.

Note that it is not necessary that the group center and the group administrators are reliable. If they are dishonest, a bidder may conspire with them and can make a signature of other group. But this is not a serious problem, which is discussed below. User U_i in the group G_j has user identifier UID_i, group identifier GID_j and the group's secret key on the digital signature scheme, and thus every user in G_j can compute G_j's digital signature without disclosing his identity.

4.2.2 Operations

In addition to the operations in the basic protocol, $DS_j(m)$ denotes the group G_j's digital signature for message m.

4.2.3 Protocol

This protocol consists of the bid stage, the revealing stage, the successful bid stage and the discovering stage as well as the basic protocol. And the modified protocol also has the same flow of the stages as the basic protocol. Only the differences from the basic protocol are described in the following.

[Bid stage] In Step 2, a bidder U_i in the group G_j publishes the bid in the basic protocol with G_j's digital signature for it, and in addition to them he also publishes the group identifiers GID_j,

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

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

And Step 3 follows.

3. The manager checks whether the group signature in the bid is valid or not. If it is not valid, the bid is ignored and removed.

[**Revealing stage**] This stage is the same as in the basic protocol.

[**Successful bid stage**] In Step 3, the manager verifies not only the validity of the anonymous undeniable signature but also the validity of the group signature.

[**Discovering stage**] The manager specifies the group from the group signature in the bid, and communicates with every user in the group by using the verifying protocol of the anonymous undeniable signature scheme. If the illegal bidder is not found, the manager communicates with every user in the network.

The discussion in the basic protocol is also effective in the modified one except for the anonymity. The anonymity is weaker than that in basic protocol because the group to which the bidder belongs can be specified from his bid. But the bidder's identity can not be specified.

The basic protocol may be used if the discovering stage is not frequently executed or the number of candidates for illegal bidders is not much larger than that of the bidder. Otherwise, the communication cost of the entire protocol is dominated by that of the discovering stage, which is proportional to the number of candidates for illegal bidders. In the basic protocol, the manager has to communicate with every user in the network in the discovering stage. But in the modified protocol, the manager has only to communicate with every user in a group for each illegal bidder in the discovering stage (refer to Figure 2). Thus the number of candidates for an illegal bidder in the modified protocol is about 1/(the number of groups) of the number in the basic protocol if the number of members in a group is equal to that in another.

To simplify matters, the digital signature scheme is used to authenticate the membership of group in this protocol. But if a user conspires with the group center, the group administrators or users in other group, he is authenticated as the member in the other group. Even if a bidder can make a signature of the other group, he cannot become a successful bidder since the signature is verified in the successful bid stage. Thus, this problem does not violate the conditions in Section 2 but only the communication cost is the same as that in basic protocol.

In [9], group signature schemes are proposed, where each signer computes a signature of a group on the secret key of the signer and the signer can be identified in case of dispute later on. Thus it discourages the signer from giving the key other ones. Furthermore, one among the schemes does not require any reliable center if the correspondence between public key and its owner is assured. If this group signature scheme is used to authenticate the membership of group in this protocol, the problem that a dishonest user is authenticated as the member in the other group is resolved. But this group signature scheme is inefficient if the number of members in a group is large.

5. Conclusion

Anonymous bidding protocols using an anonymous undeniable signature scheme have been proposed. Under the assumption that a practical undeniable signature scheme [7] is anonymous, the scheme is used. In this paper, under the general assumption that a one-to-one one-way function exists, it has been proved that an anonymous undeniable signature scheme can be constructed. In the proposed anonymous bidding protocols, a manager is not needed to be reliable since the illegal operation by the manager can be detected. The group center and group administrators in the modified protocol in Section 4.2 also are not needed to be reliable since the illegal operations by them do not violate the conditions in Section 2. Thus, the protocols do not require any reliable center as well as those of [2]. Furthermore, the problem which may occur in those of [2], that is successful bid made by the bidder who does not offer the minimum price, is resolved. In the proposed basic protocol, the manager has to communicate with every user in the network to identify illegal bidders, only when the existence of them is detected. In the proposed modified protocol, by grouping users, the manager has only to communicate with every user in some specified groups to identify illegal bidders, although the anonymity of the modified protocol is slightly weaker than that of the basic protocol.

References

[1] M. Sumita, T. Takata, T. Fujiwara, and T. Kasami, "A protocol for bidding," Proc. of the 1991 Symposium on Cryptography and Information Security, 12C, 1991.

[2] Y. Imamura, T. Matsumoto, and H. Imai, "Electronic anonymous bidding schemes," Proc. of the 1994 Symposium on Cryptography and Information Security, 11B, 1994.

[3] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," Proc. of the 1995 IEEE Symposium on Security and Privacy, pp. 2–14, 1995.

[4] J. C. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," Proc. of the 26th Annual ACM Symposium on Theory of Computing, pp. 544–553, 1994.

[5] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme — a practical solution to the implementation of a voting booth —," Advances in Cryptology — EUROCRYPT '95, LNCS 921, Springer–Verlag, pp. 393–403, 1995.

[6] D. Chaum and H. van Antwerpen, "Undeniable signatures," Advances in Cryptology — CRYPTO '89, LNCS 435, Springer–Verlag, pp. 212–216, 1990.

[7] D. Chaum, "Zero-knowledge undeniable signatures," Advances in Cryptology — EUROCRYPT '90, LNCS 473, Springer–Verlag, pp. 458–464, 1991.

[8] J. Boyar, D. Chaum, I. Damgard, and T. Pederson, "Convertible undeniable signature," Advances in Cryptology — CRYPTO '90, LNCS 537, Springer–Verlag, pp. 189–205, 1991.

[9] D. Chaum and E. van Heijst, "Group signatures," Advances in Cryptology — EUROCRYPT '91, LNCS 547, Springer–Verlag, pp. 241–246, 1991.

[10] S. Micali, C. Rackoff, and B. Sloan, "The notion of security for probabilistic cryptosystems," SIAM Journal on Computing, vol. 17, no. 2, pp. 412–426, Apr. 1988.

[11] A. C. Yao, "Theory and applications of trapdoor functions," Proc. of the 23rd IEEE Annual Symposium on Foundations of Computer Science, pp. 80–91, 1982.

[12] O. Goldreich and L. A. Levin, "A hard-core predicate for all one-way functions," Proc. of the 21st Annual ACM Symposium on Theory of Computing, pp. 25–32, 1989.

[13] O. Goldreich, S. Micali, and A. Wigderson, "Proof that yield nothing but their validity and a methodology of cryptographic protocol design," Proc. of the 27th IEEE Annual Symposium on Foundations of Computer Science, pp. 174–187, 1986.

[14] M. Naor, "Bit commitment using pseudo-randomness," Advances in Cryptology — CRYPTO '89, LNCS 435, Springer–Verlag, pp. 128–136, 1990.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, Apr. 1984.

[16] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," Journal of the ACM, vol. 33, no. 4, pp. 792–807, Oct. 1986.

[17] J. Rompel, "One-way functions are necessary and sufficient for secure signature," Proc. of the 22nd Annual ACM Symposium on Theory of Computing, pp. 387–394, 1990.

[18] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84–88, Feb. 1981.

[19] T. Okamoto and K. Ohta, "Designated confirmer signatures using trapdoor function," Proc.of the 1994 Symposium on Cryptography and Information Security, 16B, 1994.

[20] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," Journal of Computer and System Sciences, vol. 37, no. 2, pp. 156–189, Oct. 1988.

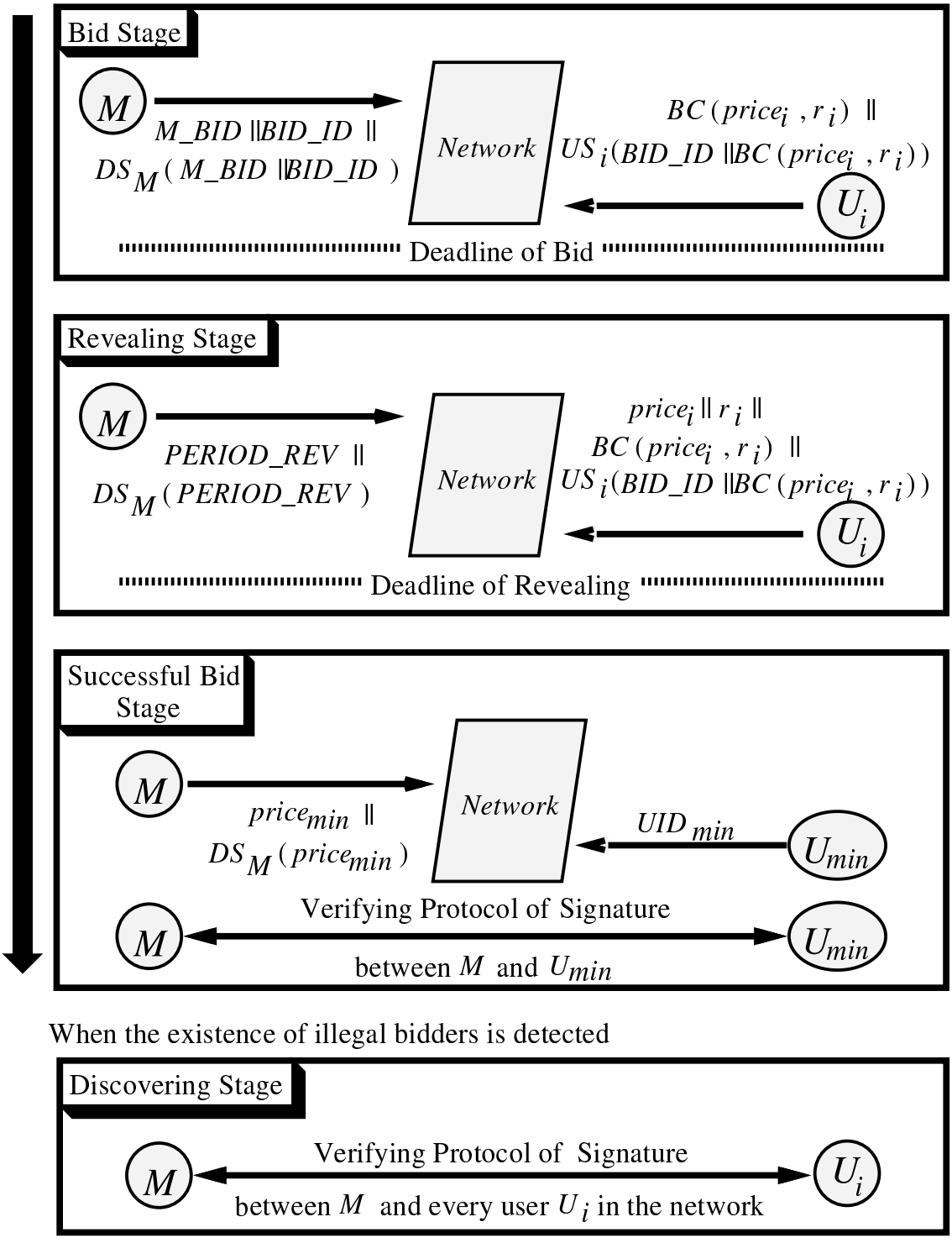
Biography

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. In 1998, he joined the Department of Information Technology, Okayama University, Okayama, Japan. His research interests are cryptography and information 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.

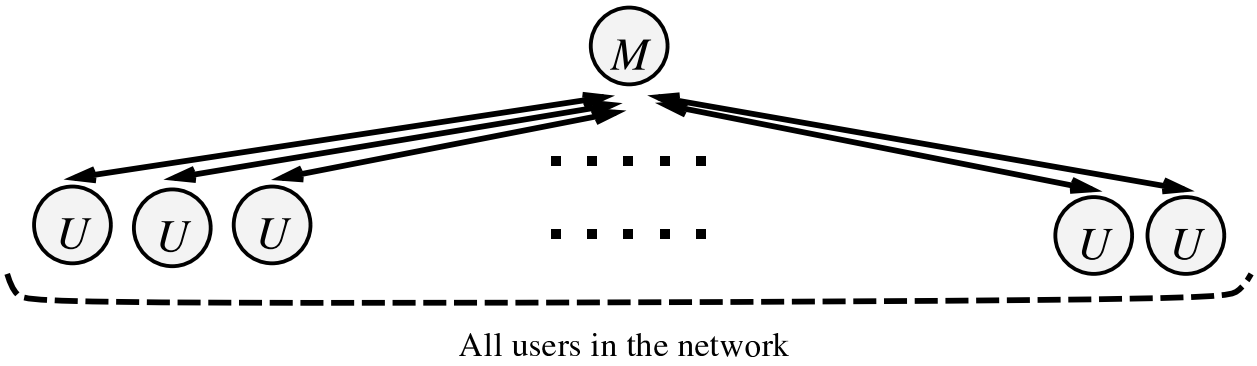
Hajime Watanabe was born in Nara, Japan, on November 3, 1968. He received the B.E., M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Toyonaka, Osaka, Japan, in 1991, 1993 and 1997, respectively. In 1994, he joined Graduate School of Information and Science, Nara Institute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

List of captions

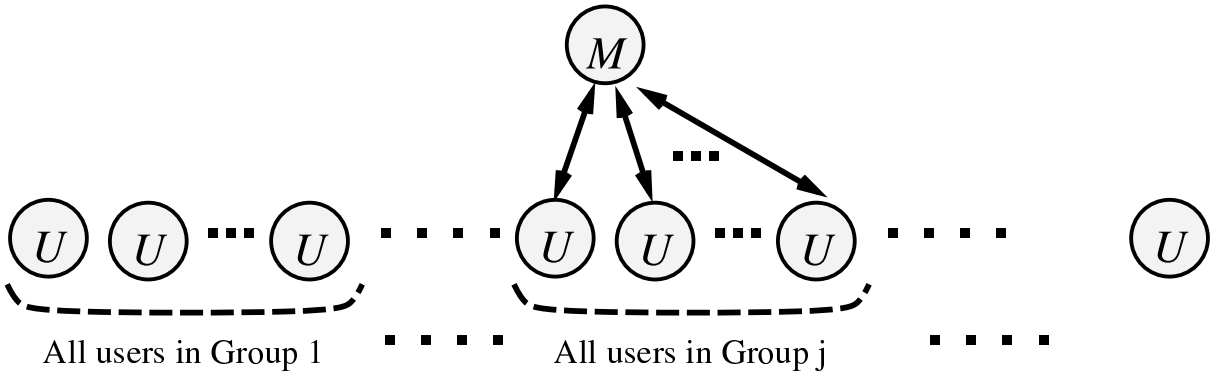


When the existence of illegal bidders is detected

Figure 1: Basic protocol.



(a) The discovering stage in the basic protocol



(b) The discovering stage in the modified protocol

Figure 2: Difference of the discovering stages in the protocols.