Provably Secure Multi-signature Scheme with Signers’ Intentions

Kei Kawauchi,† Hiroshi Minato,‡ Atsuko Miyaji and Mitsuru Tada

In this paper, we propose a multi-signature scheme, in which each signer can express her intention in the message to be signed. An intention is a piece of information which can be attached to a signature. However, no multi-signature scheme dealing with intentions without loss of efficiency has been introduced. First, we consider a multi-signature scheme realizing the concept of signers’ intentions by utilizing existing schemes, and name it primitive method. After that, we introduce the proposed multi-signature scheme which is more efficient than the primitive method in view of the computational cost for verification and in view of the signature size. The proposed multi-signature scheme is shown to be secure even against adaptive chosen message insider attacks.

1. Introduction

A multi-signature scheme, in which plural entities (signers) jointly sign an identical message, has the advantage that it is efficient in view of the signature size and in view of the computational cost for verification. Hence we can say that a multi-signature scheme is quite useful in the following case:

- We often see a notice on a bulletin board on campus, which informs club members of an event. A notice frequently requires members to write down their names on it. It is very convenient for members to check who wants to take part in the event.

Now, we suppose that a captain of the club wants to know whether or not each member (e.g., Alice, Bob and etc.) wants to attend the event. If the name is written by him/her on the notice, it is clear that he/she wants to take part in the event. But, if not, does that mean he/she does not want? The answer is No because he/she might not see the notice and also he/she does not positively express that he/she does not want to take part in the event. To make the matter sure, the captain should require members to write down their names, and also Yes or No on the notice to avoid such a problem. It is very good idea.

For example, Alice may sign the notice adding the word No. On the other hand, Bob may sign it adding the word Yes. Then, we call these Yes or No signers’ intentions. A captain may prepare a notice which has two spaces for signing. One is a space for signers who express Yes. The other is a space for signers who express No. The members put their name on one of two spaces. Unfortunately, there has been no proposal of any multi-signature schemes which efficiently handle the notice with Yes and No, namely signatures with signers’ intentions. Each signer provides two secret-keys, one for expressing Yes, and the other for expressing No.

It is, however, far from a good way since each entity has to manage more keys. As another countermeasure, the captain can provide two messages to be signed, one for Yes, and the other for No. Accordingly, verification is required twice for those two multi-signatures. But unlike in the first countermeasure, each entity has only to manage one key. In the example given above, signers’ possible intentions are only Yes and No, and we consider that signers, in general, have choices among \(I := \{I_1, \ldots, I_N\} \quad (N \geq 2)\). Each possible intention is denoted by some \(I_\ell \quad (\ell \in [1, N])\). (We can say that in the example given above, Yes and No are denoted by \(I_1\) and \(I_2\), respectively.) Hereafter such a multi-signature scheme in which plural messages are provided and plural multi-signatures are generated like in the second countermeasure, is called a primitive method. The details of this method are discussed in Section 3.

In this paper, we introduce a multi-signature
scheme with signers' intentions in which each signer has only to manage one key, in which one message to be signed is provided, hence in which only one multi-signature is generated, and furthermore in which only each signer can add her intention with respect to the given message. In a multi-signature scheme along the first countermeasure, each signer has to manage \( N \) keys, and in a multi-signature by the primitive method, the more the number \( N \) of signers' possible intentions gets, the more the signature size is and the more verification cost is required. On the other hand, in a multi-signature scheme with signers' intentions, the signature size is independent of \( N \), and hence the verification cost is much smaller than that in the primitive method. Hence a multi-signature scheme with signers' intentions can be more efficient than ones constructed along the countermeasures given above. The efficiency of the proposed scheme is outstanding. Take for example distributing vacation time among office workers. Now refer to the calendar Fig. 1. Each signer establishes his/her intention by signing his name on a single day. In the proposed scheme, verification for the calendar is needed just once. Namely, the calendar can be verified by just one equation.

The security is shown with the strategy that we reduce the security of multi-signature scheme to that of multi-round identification scheme in the random oracle model \(^1\)). To prove the security of multi-signature scheme with signers' intentions, we, for convenience' sake, consider two multi-round identification schemes with (prover's) intentions. We call those identification schemes ID-A and ID-B, respectively. The proof for the security of a multi-signature scheme with signers' intentions can be reduced to that for ID-A and ID-B. Concretely, if ID-A is secure against any polynomial-time passive adversaries, and if ID-B has zero-knowledge property, then multi-signature scheme with signers' intentions can be shown to be secure even against any polynomial-time active adversaries by using ID-reduction technique introduced by Ref. 9).

We can see related work as follows: In Refs. 9), 13), we can see several kinds of multi-signature schemes. In Refs. 2)∼5), we can see a multi-signature scheme which also guarantees the signing order. The scheme given by Ref. 8) provides signing order verifiability and message flexibility.

This paper is organized as follows: In Section 2, we give the notations we use in this paper. In Sections 3, we propose the primitive method, a combined scheme of conventional multi-signatures, in which signatures with signers' intentions can be dealt with. In Section 4, we propose a new multi-signature scheme which we call a multi-signature scheme with signers' intentions. In Section 5, we give provable security for the proposed scheme. In Section 6, we evaluate the performance of the primitive method and the proposed scheme. The conclusion is given in Section 7.
2. Preliminaries

To denotes an \( n \)-tuple \((a_1, \ldots, a_n)\), we often use the bold letter \( \mathbf{a} \). For an \( n \)-tuple \( \mathbf{a} \) \((= (a_1, \ldots, a_n))\) and for integer \( i, j \in [1, n] \) with \((1 \leq i < j \leq n)\), \( a_{i,j} \) denotes the \((j - i)\)-tuple \((a_i, \ldots, a_j)\).

2.1 Multi-signature Scheme

In a multi-signature scheme, plural signers (say, \( n \) signers) generate a signature for an identical message. However, we can realize such a situation by applying an ordinary (single) signature scheme \( n \) times. Then we shall extend a single signature scheme to be a multi-signature scheme so that the obtained multi-signature scheme satisfies the property that the signature size in the multi-signature scheme should be less than \( nL \) where \( L \) is the signature size in the single signature scheme.

In this paper, we use the multi-signature scheme, which is one-cycle type and is so-called a generic multi-signature scheme obtained by translating a multi-round identification scheme.

In a multi-signature scheme, \( n \) signers \( P_1, \ldots, P_n \) participate and each signer \( P_i \) publishes a public-key \( v_i \) and keeps a secret-key \( s_i \). In the following, we describe the scheme, each \( P_i \) can query to the public random oracle function \( f_i : \{0, 1\}^* \rightarrow \mathbb{Z}_q \). Let \( \mathcal{P} \) denotes the set \( \{P_1, \ldots, P_n\} \).

System parameter: Let \( p \) and \( q \) be primes such that \( q \) divides \((p - 1)\), and let \( g \) be an order-\( q \)-element in \( \mathbb{Z}_p^* \). The system parameter \( \text{sep} \) is the set \((p, q, g)\). The security parameter \( \text{SEP} \) is \(|q|\).

System parameters are common for all schemes. Then, we omit these in latter schemes.

Key-generation step: Each signer \( P_i \in \mathcal{P} \) provides a pair of a secret-key and the corresponding public-key. Her secret-key is a random element \( s_i \in \mathbb{Z}_q^* \), and the corresponding public-key \( v_i \) is defined \( g^{s_i} \) (mod \( p \)). When \( P_i \) registers the public-key \( v_i \), she must show that she indeed has \( s_i \) in a zero-knowledge manner to prevent the key-generation phase attacks given by 10).

Signature generation step: Suppose that a set of signers \( \mathcal{P} \) generates a multi-signature for a message \( m \). The initial value \( y_0 \) is 0. For each \( i \in [1, n] \), the following is executed.

- \( P_i \) receives \((x_{1,i-1}, y_{1,i-1})\), \( m \) from \( P_{i-1} \). \( P_i \) picks up a random \( r_i \in \mathbb{Z}_q \) and computes \((x_i, e_i, y_i)\) as follows:
  \[ x_i := g^{r_i} \pmod{p}; \]
  \[ e_i := f_i(x_{1,i}, m); \]
  \[ y_i := y_{i-1} + s_i + r_i \cdot e_i \pmod{q}. \]

- \( P_i \) sends \((x_{1,i}, y_i)\), \( m \) to \( P_{i+1} \). Also let \( P_{n+1} := V \).

Verification step: Suppose that the verifier \( V \) receives a multi-signature \((x, y_n)\) for a message \( m \). Then \( V \) computes \( e_i := f_i(x_{1,i}, m) \) for each \( i \in [1, n] \). Also the verifier \( V \) checks the following equations:

\[ g^{y_n} = \prod_{i=1}^{n} (x_i^{e_i} \cdot v_i) \pmod{p}. \]

3. Primitive Method

In Section 1, we have intuitively mentioned how we can realize a multi-signature scheme with signers' intentions. Here we present a concrete scheme of the primitive method. Suppose that each \( P_i \) is required her intention \( \alpha_i \) for a message \( m \), and that her possible intention is in a set \( \mathcal{I} := \{I_1, \ldots, I_N\} \). For \( \ell \in [1, N] \), let \( m_\ell \) be the message corresponding to the intention \( I_\ell \) for \( m \).

Both system parameter and key-generation step are done in the same way as that of the multi-signature scheme in Section 2.

Signature generation step: Suppose that a set of signers \( \mathcal{P} \) generates a multi-signature for a set of message \( \{m_\ell\} \) with signers' intentions. Assume that \( y_{01}, \ldots, y_{0N} \) are set up to be zero. For each \( i \in [1, n] \), the following is executed.

- \( P_i \) chooses her intention \( \alpha_i \in \mathcal{I} \). Let \( \alpha_i = I_\ell \). \( P_i \) picks up a random \( r_i \in \mathbb{Z}_q \) and computes \((x_i, e_i, y_i)\) as follows:
  \[ x_i := g^{r_i} \pmod{p}; \]
  \[ e_i := f_i(x_{1,i}, m_\ell); \]
  \[ y_i := y_{i-1} + s_i + r_i \cdot e_i \pmod{q}. \]

- \( P_i \) sends \((x_{1,i}, y_i)\), \( m_\ell \) to \( P_{i+1} \). Also let \( P_{n+1} := V \).

Verification step: Suppose that the verifier

Vol. 43 No. 8  Provably Secure Multi-signature Scheme with Signers’ Intentions 2427
The set of public-keys $v^{(t)}$ is defined to be $\bigcup_{\alpha_i=1}^{q} \{v_i\}$, which is the set of the public keys of signers with intentions $\alpha_i$, and where $x^{(t)}$ and $e^{(t)}$ are defined as well as $v^{(t)}$. As we can guess from the primitive method given above, the total signature size in the primitive method turns out to be $n|p| + \#(\bigcup_{\alpha_i=1}^{q})/q|$. In evaluating the computational cost, more important is $\#(\bigcup_{\alpha_i=1}^{q})$, which is the most variety of the intentions actually chosen by $P$, rather than $\#I(=N)$, which is the number of the intentions provided for the message.

4. Proposed Scheme

In this section, we present a multi-signature scheme with signers’ intentions secure against active attacks. 

4.1 A Multi-signature Scheme with Signers’ Intentions

The primitive method discussed in the previous section, needs much verification cost in proportion to the number of the varieties of signers’ intentions. As seen in the primitive method, as $N$ increases, the scheme may get inefficient. Then we here propose a new multi-signature scheme with signers’ intentions. In this scheme, the total signature size is independent of $N$, and is the same with that in the scheme\(^9\). The process of generating $y_i$, a part of signature, is very unique. And the proposed scheme is secure even against adaptive chosen message insider attacks.

In the following, we describe the proposed scheme, in which each $P_i$ can query to the public random oracle function $f_i: \{0, 1\}^* \rightarrow Z_q$.

Both system parameter and key-generation step are done in the same way as that of the multi-signature scheme in Section 2.

Signature generation step: Suppose that a set of signers $P$ generates a multi-signature for a message $m$. The initial value $y_0$ is 0. For each $i \in [1, n]$, the following is executed.

- $P_i$ receives $(x_{[1,i-1]}, y_{i-1})$, $m$ and $\alpha_{[1,i-1]}$ from $P_{i-1}$. $P_i$ chooses her intention $\alpha_i \in I$, and picks up a random $r_i \in Z_q$ and computes $(x_i, e_i, y_i)$ as follows:
  
  $x_i := g^{\alpha_i}$ (mod $p$);
  $e_i := f_i(x_{[1,i]}, m, \alpha_{[1,i]})$;
  $y_i := y_{i-1} + \alpha_i + r_i \cdot e_i$ (mod $q$).

- $P_i$ sends $(x_{[1,i]}, y_i)$, $m$ and $\alpha_{[1,i]}$ to $P_{i+1}$. Also let $P_{n+1} := V$.

Verification step: Suppose that the verifier $V$ receives a multi-signature $(x, y_n)$ for a message $m$ with signers’ intentions $\alpha$. Then $V$ computes $e_i := f_i(x_{[1,i]}, m, \alpha_{[1,i]})$ for each $i \in [1, n]$. Also the verifier $V$ checks the following equations:

$$g^{y_n} \equiv \prod_{i=1}^{n} (x_i^{e_i} \cdot v_i^\alpha_i) \pmod{p}.$$

4.2 Model of the Proposed Scheme

In the previous subsection, we have presented the proposed scheme, which is based on Schnorr’s one\(^{12}\). The proposed scheme can be adopt other generic signature schemes such as ElGamal scheme\(^8\) and its variants like Ref. 7). In the following, we have the model of the proposed scheme. In the model, the symbols $\text{Cat}$, $\text{Sig}$ mean the function which computes the commitment ($x$ component) and the function which computes the signature ($y$ component). The function $\text{Sig}$ is actually identical to the function $\text{Ans}$ which computes the answer in the corresponding (multi-round) identification scheme. The range of the used random oracle functions which is the challenge in the identification scheme, is denoted by $E$.

System parameter: First of all, the system parameter $syp$ is chosen.

Key-generation step: Each signer $P_i \in P$ provides a pair of a secret-key and the corresponding public-key using a key-generation algorithm $G$ on input $k^i$. Her secret-key is denoted by $s_i$, and the corresponding public-key is denoted by $v_i$. It should be assumed that probability for any polynomial-time machine to find $s_i$ for given $v_i$ and $syp$ is negligible with respect to the security parameter $sep$. If the scheme has only the insensitive reduction\(^{10}\), then when $P_i$ registers the public-key $v_i$, she has to show that she indeed has $s_i$ in a zero-knowledge manner. If the scheme has the sensitive reduction\(^{10}\), then
this proof is not mandatory.

Signature generation step: Suppose that a set of signers \( P \) generates a multi-signature for a message \( m \) with signers’ intentions. The initial value \( y_0 = 0 \). For each \( i \in [1, n] \), the following is executed:
- \( P_i \) receives \((x_{[1,i-1]}, y_{i-1})\), \( m \) and \( \alpha_{[1,i-1]} \) from \( P_{i-1} \). \( P_i \) chooses her intention \( \alpha_i \in \mathcal{I} \), and picks up a random number \( r_i \) and computes \((x_i, e_i, y_i)\) as follows:
  \[ x_i := \text{Cmt}(r_i, s_i, \alpha_i); \]
  \[ e_i := f_i(x_{[1,i]}, m, \alpha_{[1,i]}); \]
  \[ y_i := \text{Sig}(s_i, r_i, e_i, \alpha_i, y_{i-1}). \]
\( P_i \) sends \((x_{[1,i]}, y_i)\), \( m \) and \( \alpha_{[1,i]} \) to \( P_{i+1} \). Also let \( P_{n+1} := V \).

Verification step: Suppose that the verifier \( V \) receives a multi-signature \((x, y_n)\) for a message \( m \) with signers’ intentions \( \alpha \). Then \( V \) computes \( e_i := f_i(x_{[1,i]}, m, \alpha_{[1,i]}); \) for each \( i \in [1, n] \). Also the verifier \( V \) computes the following equations:
\[ v := \text{Ver}(v, m, x, e, y_n, \alpha). \]
\( V \) accepts the multi-signature with signers’ intentions if \( v = 1 \), and rejects otherwise.

5. Security Consideration

In this section, we prove that the proposed scheme is secure against active adversaries. The attack model given below covers the most general attacks, adaptive chosen message insider attacks.

5.1 Adversary Model

For discussion of the security of multi-signature scheme with signers’ intentions, we here present the adversary model for the scheme.

MS-\( \alpha \) adversary

Given the system parameter \( \text{sys} \) and the public-keys \( v \), an MS-\( \alpha \) adversary \( M \) which can query to the random oracle functions \( f_i \) (\( i \in [1, n] \)), executes the following for each \( j \in [1, Q] \) with given \( Q \):
\begin{itemize}
  \item [(S1)] An MS-\( \alpha \) adversary \( M \) determine a message \( m_j \), a signer \( P_{i_j} \), and the signer’s intention \( \alpha_j \in \mathcal{I}^n \).
  \item [(S2)] Generate a valid partial multi-signature \((x_{[1,i-1]}, e_{[1,i-1]}, y_{i-1})\) by colluding with \( P \setminus \{P_{i_j}\} \).
  \item [(S3)] Send \((x_{[1,i-1]}, e_{[1,i-1]}, y_{i-1}, \alpha_{[1,i-1]})\) and \( \alpha_{i,i_j} \) to \( P_{i_j} \). To make the adversary stronger, we assume \( M \) can ask \( P_{i_j} \)’s signature for \( P_{i_j} \’s \) intention \( M \) chooses.
\end{itemize}

(S4) And get a valid partial multi-signature \((x_{[1,i]}, e_{[1,i]}, y_i)\) and the signers’ intentions \( \alpha_{[1,i]} \) from \( P_{i_j} \).

After \( Q \) iterations of these steps (S1), (S2), (S3) and (S4), the adversary \( M \) computes a multi-signature for a message \( m \) with signers’ intentions \( \alpha \), where for every \( j \in [1, Q] \), it must hold at least one of \( m \neq m_j \) and \( \alpha_{j,[i,j]} \neq \alpha_{[i,j]} \).

Here note that in the key-generation step, each signer is required to show that she indeed has the corresponding secret-key, if Type II\(^9\) is adopted. Hence we don’t have to consider the key generation phase attacks.

5.2 Definition of the Security for Multi-signature Scheme with Signers’ Intentions

Here we define the security of the proposed multi-signature scheme with signers’ intentions.

Definition 5.1 Suppose an MS-\( \alpha \)-adversary (probabilistic Turing machine) \( M \) can ask \( R_i \)-queries to \( f_i \) for each \( i \in [1, n] \), and is allowed \( Q \)-time execution of the steps from (S1) to (S4). If such an MS-\( \alpha \) adversary \( M \) can forge a multi-signature \((x, e, y_n)\) for a message \( m \) with signers’ intentions \( \alpha \) in time at most \( t \) with probability at least \( \epsilon \), then we say that \( M \) can \((t, Q, R, \epsilon)\)-break the multi-signature scheme with signers’ intentions. Here, the probability is taken over the coin flips of \( M \), \( f_1, \ldots, f_n \) and signing oracles \( P \).

Definition 5.2 A multi-signature scheme with signers’ intentions is said to be \((t, Q, R, \epsilon)\)-secure, if there is no MS-\( \alpha \) adversary which can \((t, Q, R, \epsilon)\)-break the multi-signature scheme with signers’ intentions. This security of the multi-signature scheme given by Ref.\(^9\) can be reduced to the security of multi-round identification scheme, from which the multi-signature scheme is derived. That means if the multi-round identification scheme is shown to be secure against polynomial-time adversaries, then it shall be shown that by ID-reduction lemma, in the multi-signature scheme, any adaptive chosen message insider polynomial-time adversary cannot existentially forge a signature. Also for the proposed scheme, the security of the multi-signature scheme with signers’ intentions can be reduced to the security of some kinds of multi-round identification schemes. Before showing
it, we first introduce two kinds of multi-round identification schemes. Those are slightly different from each other, and are necessary to prove the security of multi-signature scheme with signers’ intentions.

**Scheme ID-A:**

The participating entities are the prover $P$ and the verifier $V$.

System parameter is done in the same way as that of the multi-signature scheme in Section 2.

**Key-generation step:** $P$ provides $n$ pair of a secret-keys $s_i \in \mathbb{Z}_q$ and the corresponding public-keys $v_i$, where $v_i := g^{s_i} \pmod{p}$ ($i \in [1, n]$).

**Identification step:** $P$ chooses her intentions $\alpha \in I$ with $\#\alpha = n$. First $P$ picks up $n$ random $r_i \in \mathbb{Z}_q$, and computes $x_i := g^{r_i}$ ($\pmod{p}$) ($i \in [1, n]$). Then the prover $P$ and the verifier $V$ execute the following step for $i \in [1, n]$.

- $P$ sends the commitment $(x_i, \alpha_i)$ to $V$, and $V$ randomly picks up the challenge $e_i \in \mathbb{Z}_q$, and sends it to $P$.

After this iteration, $P$ computes the answer

$$y := \sum_{i=1}^{n} (s_i \cdot \alpha_i + r_i \cdot e_i) \pmod{q}.$$ 

Then $P$ sends $y$ to $V$. Receiving $(x, y)$ and $\alpha$, $V$ checks $(x, y)$ and $\alpha$ by following verification:

$$g^y \equiv \prod_{i=1}^{n} (x_i^{e_i} \cdot v_i^{\alpha_i}) \pmod{p}.$$ 

If this equality holds, then $V$ accepts the identification, and rejects, otherwise.

**Scheme ID-B:**

ID-B is different from ID-A in terms of the timing when $P$ declares. Namely in ID-B $P$ does before interaction between $P$ and $V$.

Both system parameter and key-generation step follows that of Scheme ID-A.

**Intention declaration step:** The prover $P$ publishes $\alpha \in I$ with $\#\alpha = n$. (This distribution does not have to be uniform.)

**Identification step:** $P$ picks up $n$ random $r_i \in \mathbb{Z}_q$, and computes $x_i := g^{r_i}$ ($\pmod{p}$) ($i \in [1, n]$). For the rest, the step is the same as the previous one.

As well as in the previous section, we can have the models of Schemes ID-A and ID-B, by using the functions $\text{Cmt}$, $\text{Ans}$ ($= \text{Sig}$) and $\text{Ver}$.

### 5.4 Definitions of the Security for Identification Schemes

Here we define the security for multi-round identification schemes.

**Definition 5.3** Suppose that an ID-adversary $M$ which does not have $s$, can pass the verification for some $\alpha$ in time at most $t$ with probability at least $\epsilon$. Then we say that ID-adversary $M$ can $(t, \epsilon)$-break the multi-round identification scheme.

**Definition 5.4** We say that a multi-round identification scheme is $(t, \epsilon)$-secure, if there is no ID-adversary which can $(t, \epsilon)$-break the scheme, and if $(x, e, y)$ with $\text{Ver}(v, m, x, e, y, \alpha) = 1$ for intentions $\alpha \in I$, satisfies $\text{Ver}(v, m, x, e, y, \alpha') = 0$ with overwhelming probability, for another (distinct) intentions $\alpha'$. Here, $\text{Ver}(v, m, x, e, y, \alpha)$ is the predicate to judge whether for intentions $\alpha$, the tuple $(x, e, y)$ passes the verification by using $v$. Its value is 1, if the predicate is true, and is 0, otherwise.

We define the zero-knowledge property for Scheme ID-B as follows:

**Definition 5.5** Suppose that a polynomial-time machine $S$ is given public-key $v$ and intentions $\alpha \in I$. Here we define the function $\eta(\text{sep})$ as follows:

$$\eta(\text{sep}) := \sum_{\gamma \in \mathbb{Z}_q^\times} \frac{\Pr[(x, e, y) \leftarrow \{P(s, \alpha), V(v, \alpha)\}; (x, e, y) = (\gamma, \lambda, \mu)\}}{\Pr[(x', e', y') \leftarrow \{S(v, \alpha)\}; (x', e', y') = (\gamma, \lambda, \mu)\]},$$

where $(x, e, y) \leftarrow \{P(s, \alpha), V(v, \alpha)\}$ denotes the event that $(2n + 1)$-tuple $(x, e, y)$ is obtained by the communication between $P$ on input $(s, \alpha)$ and $V$ on input $(v, \alpha)$. Then we say that the scheme has the statistical zero-knowledge property, if $\eta(\text{sep})$ is negligible. As a special case, if $\eta(\text{sep})$ is identically zero, then we say that the scheme has the perfect zero-knowledge property.

Then Scheme ID-B is shown to provide the perfect zero-knowledge property by constructing a simulator $S$, as follows:

- Given $v$ and $\alpha \in I$, $S$ picks up $y \in \mathbb{Z}_q$ and $e \in \mathbb{Z}_q^n$ to compute $\beta$, such that $y = \sum_{i=1}^{n} (e_i \cdot \beta_i)$ ($\pmod{q}$), and $\gamma_i$ such that $\alpha_i + e_i \cdot \gamma_i = 0$ ($\pmod{q}$) ($i \in [1, n]$). Then $S$ computes $x_i := g^{\beta_i} v^{\gamma_i}$ ($\pmod{p}$) ($i \in [1, n]$).

Such an $(x, e, y)$ indeed passes the verification.
Lemma 5.6 Scheme ID-B has the perfect zero-knowledge property.

Proof. We compute the following to probability of appearance of the \((2n + 1)\)-tuple \((x, e, y)\):

- The probability of appearance of the \((2n + 1)\)-tuple \((x, e, y)\) which can pass the verification for some \(\alpha\).

\[
\Pr \left[ (\kappa, \lambda, \mu) \leftarrow \left( P(s, \alpha), V(v, \alpha) \right) \right] = \frac{1}{q^{2n}};
\]

\[
\Pr \left[ (\kappa, \lambda, \mu) \leftarrow S(v, \alpha) \right] = \frac{1}{q^{2n}}.
\]

- The probability of appearance of the \((2n + 1)\)-tuple \((x, e, y)\) which can’t pass the verification for some \(\alpha\).

\[
\Pr \left[ (\kappa, \lambda, \mu) \leftarrow \left( P(s, \alpha), V(v, \alpha) \right) \right] = 0;
\]

\[
\Pr \left[ (\kappa, \lambda, \mu) \leftarrow S(v, \alpha) \right] = 0.
\]

Thus we get that each distributions of probabilities are the same. So Scheme ID-B has the perfect zero-knowledge property. ■

As mentioned in Lemma 5.6, ID-B has the perfect zero-knowledge property, whereas ID-A does not. Because the simulator does not know the distributions of probabilities for each of signers’ intentions. But we can prove that the proposed scheme is secure against an active adversaries. Because it is possible to simulate the signature which an active adversary queries to signing oracle as long as ID-B has the zero-knowledge property. Consequently, if there exists an active adversary which has the signing oracle, then we can construct a passive adversary which needs no signing oracle, using an active adversary. Hence if there exists a passive adversary which can break the proposed scheme, then we can construct an attacker which can break ID-A. But the attacker cannot break ID-B. Because the prover cannot execute the intention declaration step in ID-B, by reason of the prover doesn’t know in advance what all signers’ intentions as the commitment the passive adversary chosen are. In this way, we can understand to need two identification schemes, Scheme ID-A and Scheme ID-B to show the security of the proposed scheme.

An adversary model for Scheme ID-A is given as follows.

**ID-adversary**

An ID-adversary \(M\) is a machine, which, on input \(v\), executes Scheme ID-A with \(V\), and tries to pass the verification for some signers’ intentions \(\alpha\). The ID-adversary \(M\) is so-called a passive attacker, which cannot accomplish the attack in the middle.

5.5 ID-reduction Lemma and Heavy Row Lemma

Since Scheme ID-B provides the zero-knowledge property, we can obtain the following ID-reduction lemma.

Lemma 5.7 (i) If there exists an MS-\(\alpha\) adversary \(A_\alpha\) which can \((t, Q, R, \epsilon)\)-break the scheme, then there also exists an MS-\(\alpha\) adversary \(A_1\) which can \((t, Q, 1, \epsilon_1)\)-break the scheme, where \(1\) is the \(n\)-tuple \((1, \ldots, 1)\), and \(\epsilon_1 := a_n\) with \(a_0 := \epsilon\) and \(a_i := \left( a_{i-1} - \frac{1}{q} \right) / R_i\).

(ii) If there exists an MS-\(\alpha\) adversary \(A_1\) which can \((t, Q, 1, \epsilon_1)\)-break the scheme, then there also exists an MS-\(\alpha\) adversary \(A_p\) which can \((t^+, 0, 1, \epsilon_p)\)-break the scheme, where \(t^+ := t + \Phi_2\). \(\Phi_2\) is the time for simulation of \(Q\) multi-signatures and \(\epsilon_p := \epsilon_1 - Q / q\).

(iii) If there exists an MS-\(\alpha\) adversary \(A_p\) which can \((t^+, 0, 1, \epsilon_p)\)-break the scheme, then there also exists an ID-adversary \(A_{id}\) which can \((t^+, \epsilon_p)\)-break the scheme.

Proof.(Sketch) The proof is also the same with that of Lemma 9 in Ref.9.

Lemma 5.8 Let \(\epsilon_p \geq \frac{2^{n+1}}{q}\). If there exists an ID-adversary which can \((t^+, \epsilon_p)\)-break the scheme, then there exists a machine \(M\) which can compute \(s(= s_1 + \cdots + s_n \mod q)\) on input \(v\) in time \(t^*\) with success probability \(\epsilon^*\). Here \(t^*\) and \(\epsilon^*\) are defined as follows:

\[
t^* := \frac{t^++}{3\epsilon_p} \left( 2^{2n+1} + 1 \right) + \Phi_L;
\]

\[
\epsilon^* := \frac{F_1(\epsilon_p)}{3} \prod_{i=1}^{n} \left( \frac{1}{2} F_i(\epsilon_p) \right)^{2^{i-1}},
\]

where \(t^++ := t^* + \Phi_V\), \(\Phi_V\) is the time for verification, \(\Phi_L\) is the time for finding \(s\) in the final stage of reduction, and the function \(F_i(\epsilon_p)\) is defined to be \(1 - \left( 1 - \frac{\epsilon_p}{2} \right)^{2^n}\).

Proof. Also for Scheme ID-A, we can obtain the Heavy row lemma like Ref.9. Hence we can obtain \(2^n\) simultaneous equations with \((2^n + n - 1)\) unknowns. Among those unknowns, the \(n\) ones are the secret-keys, and the rest are \(r\) components. From these equations, we can get \(s\). The required time and the probability can be obtained as well as in Ref.9.

Next we show one more property for security
of multi-signature schemes with signers’ intentions.

**Lemma 5.9** Suppose that the tuple \((x, e, y)\) passes the verification for signers’ intentions \(\alpha \in I\). Then the very tuple \((x, e, y)\) is rejected for another signers’ intentions \(\alpha'\) with overwhelming probability.

**Proof.** It comes from the fact that for \(\alpha, \alpha' \in I\) with \(\alpha \neq \alpha'\), it holds the following:

\[
\Pr \left[ (x, e, y, \alpha) \rightarrow [P(s), V(v)] : \text{Ver}(v, x, e, y, \alpha') = 1 \right] \leq 1/q,
\]

where \(\text{Ver}\) is the verification equation. ■

Combining Lemmas 5.7, 5.8 and 5.9, we can obtain the following theorem.

**Theorem 5.10** Let \(\epsilon_p \geq \frac{2^{n+1}}{q^n}\). Suppose that the computation of \(s\) from \(v\) (the key searching problems) satisfying \(v_1 \times \cdots \times v_n = g^s \pmod{p}\) is \((t', \epsilon')\)-secure. Then the proposed multi-signature scheme with signers’ intentions is \((t, Q, R, \epsilon)\)-secure.

Suppose that \(t\) and \(t'\) are bounded by a polynomial on the security parameter \(|q|\). Then \(\epsilon\) is non-negligible with respect to \(|q|\) if and only if so is \(\epsilon'\).

### 6. Efficiency Consideration

We evaluate the computational amount for verification in the proposed scheme on the basis of the required number of modular-\(p\) multiplications, and also the total size of signatures.

The required number of modular-\(p\) multiplications is calculated by a simple binary method. For \((g_1^{a_1} \cdot g_2^{a_2} \cdots g_n^{a_n})\) where \(|a_1| = |a_2| = \cdots = |a_n| = |q|\) and \(|g_1| = |g_2| = \cdots = |g_n| = |p|\), the required number of modular-\(p\) multiplications is \((\frac{n+1}{2})|q| - 1\). In the computational amount for signing, there is no difference between the proposed scheme and the primitive method. It will not be discussed here. **Table 1** summarizes the total size of signatures and the computational amount for verification in the primitive method and the proposed scheme.

In the primitive method, the required number of modular-\(p\) multiplications is related to \(#(\bigcup_i \{\alpha_i\})\). In other words, the primitive method loses its merit in proportion to the increase of \(#(\bigcup_i \{\alpha_i\})\), because \(#(\bigcup_i \{\alpha_i\})\) multi-signatures are verified in the primitive method. On the other hand, the proposed scheme is very unique. The proposed scheme has two properties simultaneously.

- One is the property as a multi-signature scheme, which is suited to plural signers.
- The other is the property, which is suited to plural signers’ intentions.

Roughly speaking, the former property makes the gap of the required number of modular-\(p\) multiplications between the single-signature scheme and the proposed (multi-signature) scheme. Second property, in the primitive method, the number of equations for verification (or the number of signatures) depends on the number of varieties of signers’ intentions. Finally, in the proposed scheme, the number of equations for verification (or the number of signatures) do not depend on the number of signers or the number of varieties of signers’ intentions.

### 7. Conclusion

We have proposed an idea of signers’ intentions for multi-signature scheme, and have given the multi-signature scheme with signers’ intentions. Then, we have shown that the proposed scheme has a computational advantage for verification, compared to the primitive method. The proposed scheme is proved to be secure against adaptive chosen message insider adversaries, by reducing it to that of two kind of multi-round identification schemes. This approach is also applicable to various multi-signature schemes such as two-cycle multi-signature schemes.

**Acknowledgments** The authors would like to express our thanks to Dr. Takeshi Okamoto at Tokyo Denki University for his invaluable advice and useful comments.
References


(Received December 4, 2001)
(Accepted June 4, 2002)

Kei Kawauchi received the B.E. degree from the Department of Aerospace Engineering, National Defense Academy, Kanagawa, Japan in 1997, and received the M. Info. Sc. degree from JAIST (Japan Advanced Institute of Science and Technology) in 2002. He is currently pursuing a doctorate degree in the same field at Chiba University, Chiba, Japan. His research interest includes the theory of computation. He has joined Japan Grand Self Defense Force since 1997 up to the present.

Hiroshi Minato received the B.A. degree in Economics from Shinshu University, Japan in 1991, and the M.S. degree in Information Science from Japan Advanced Institute of Science and Technology (JAIST), Japan in 2001. He is currently a M.S. student in the Department of Electrical Engineering and Computer Science at Tufts University, located in Medford, Massachusetts, U.S.A. His interest is in E-commerce and E-government. He worked for 8 years in foreign exchange trading and its software development for an investment bank.
Atsuko Miyaji received the B. Sc., the M. Sc., and Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Matsushita Electric Industrial Co., Ltd from 1990 to 1998 and engaged in research and development for secure communication. She has been an associate professor at JAIST (Japan Advanced Institute of Science and Technology) since 1998. She has joined the computer science department of University of California, Davis since 2002. Her research interests include the application of projective varieties theory into cryptography and information security. She received IPSJ Sakai Special Researcher Award in 2002. She is a member of the Institute of Electronics, Information and Communication Engineers and the Information Processing Society of Japan.

Mitsuru Tada was born in Kyoto, Japan, in September 1969. He received the B.S., M.I.S. and Dr. I.S. degrees from Tohoku University, Japan, in 1992, 1995 and 1998, respectively. He was an associate at School of Information Science, Japan Advanced Institute of Science and Technology from 1998 to 2001. He has been an associate professor at Institute of Media and Information Technology, Chiba University, Japan, since December 2001. He received the SCIS paper award of IEICE in 2000. His interests are on mathematical logic, cryptology and computational complexity theory. Dr. Tada is a member of IEICE.