A multi-signature scheme with signers' intentions secure against active attacks

Kei Kawauchi[1], Hiroshi Minato[2], Atsuko Miyaji[1], and Mitsuru Tada[1]

[1] School of Information Science,
Japan Advanced Institute of Science and Technology (JAIST),
Asahidai 1-1, Tatsunokuchi, Nomi, Ishikawa, 923-1292, Japan.
{kei-k, miyaji, mt}@jaist.ac.jp
[2] Department of Electrical Engineering and Computer Science,
Tufts University,
Halligan Hall, 161 College Avenue, Medford, Massachusetts 02155-5528, USA.
hminato@eecs.tufts.edu

Abstract. In this paper, we propose a multi-signature scheme, in which each signer can express her *intention* associating with the message to be signed. Signers' intentions mean a kind of information which can be newly attached to a signature in signers' generating it. However, we have never been introduced any multi-signature scheme dealing with intentions without loss of its efficiency.
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 are more efficient in view of the computational cost for verification and in view of the signature size than primitive method. 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 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 the captain must fix that members who have never written their names do not want, because it may happen that they have overlooked the

message. 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 for the 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.

To be sure that the captain can take countermeasure to meet such a situation by making each signer provide two secret-keys, one for expressing `Yes`, and the other for expressing `No`, but it is 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, twice verification is required 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 $\mathcal{I} := \{I_1 \ldots, I_N\}(N \geq 2)$. Each possible intention is denoted by some $I_\ell(\ell \in [1, N])$. (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 message are provide and plural multi-signature are generated like in the second countermeasure, is called *primitive method*. The details of this method are discussed in Section3. 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 massage. 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. Hence a multi-signature scheme with signers' intentions can be more efficient than ones constructed along the countermeasures given above. In that situation, the efficiency of the proposed scheme is outstanding. We can take for example, distributing vacation time among office workers. Now refer to the calendar (Figure 1). The calendar includes multi-signatures with many varieties of signers' intentions, as people put their name on one of days. 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

Mon	Tue	Wed	Thu	Fri	Sat	Sun
			1 Maria Amy	2 Sydney	3	4
5 Matthew Michael	6 Jacob Joshua Joseph Hannah	7 Ashley Emily	8	9 Olivia Hunter Adam Morgan	10	11
12 Austin Alexis	13 Taylor Jessica	14	15 Cody Sarah Kevin	16 Erin Mary Sara	17	18
19 Amanda Amber John	20 Madison Allison Megan	21 Kayla William	22 Eric Samuel	23 Luke Paul Alex	24	25
26 Peter David James	27 Justin Ryan Jordan	28 Robert	29 Dakota Thomas Julia	30 Miguel Destiny	31	

Fig. 1. Calendar

(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`. Concrete to say, 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 [7].

We can see related work as follows: In [7, 10], we can see several kinds of multi-signature schemes. In [2–5], we can see a multi-signature scheme which guarantee also the signing order. The scheme given by [6] 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 combination 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 $\boldsymbol{a}$. For an n-tuple $\boldsymbol{a}(= (a_1, \ldots, a_n))$ and for integer $i, j \in [1, n]$ with $(1 \leq i < j \leq n)$, $\boldsymbol{a}_{[i,j]}$ denotes the $(j - i)$-tuple $(a_i, \ldots, a_j)$.

2.1 Multi-signature scheme [7]

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 shall satisfy 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 [9] 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 [1] $f_i : \{0, 1\}^* \to \mathbf{Z}_q$. Let $\mathcal{P}$ denotes the set $\{P_1, \ldots, P_n\}$.

System parameter: System parameters p, q, g are published, and satisfy the following properties:

- A trusted center publishes two large primes p and q such that $q|(p - 1)$.
- Element $g \in \mathbf{Z}_p^*$ of order 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 $s_i \in \mathbf{Z}_q$ and the corresponding public-key v_i, where $v_i := g^{s_i} \pmod p (i \in [1, n])$ and n is the number of signers. In the registration, P_i is required to show that she indeed has s_i.

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 $(\boldsymbol{x}_{[1,i-1]}, y_{i-1})$, m from P_{i-1}. P_i picks up a random $r_i \in \mathbf{Z}_q$ and computes (x_i, e_i, y_i) as follows:

$$\begin{aligned} x_i &:= g^{r_i} \pmod p, \\ e_i &:= f_i(\boldsymbol{x}_{[1,i]}, m), \\ y_i &:= y_{i-1} + s_i + r_i \cdot e_i \pmod q. \end{aligned}$$

  P_i sends $(\boldsymbol{x}_{[1,i]}, y_i)$, m to P_{i+1}. Also let $P_{n+1} := V$.

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

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

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 α_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_ℓ be the message corresponding to the intention I_ℓ 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 $y_0^{(I_1)}, \ldots, y_0^{(I_N)}$ are set up to be zero. For each $i \in [1, n]$, the following is executed.

- P_i receives $(\boldsymbol{x}_{[1,i-1]}, y_{i-1}^{(I_1)}, \ldots, y_{i-1}^{(I_N)})$, $\{m_\ell\}$ and $\boldsymbol{\alpha}_{[1,i-1]}$ from P_{i-1}. P_i chooses her intention $\alpha_i \in \mathcal{I}$. Let $\alpha_i = I_\ell$. P_i picks up a random $r_i \in \mathbf{Z}_q$ and computes (x_i, e_i, y_i) as follows:

$$\begin{aligned} x_i &:= g^{r_i} \pmod{p}, \\ e_i &:= f_i(\boldsymbol{x}_{[1,i]}^{(I_\ell)}, m), \\ y_i^{(I_\ell)} &:= y_{i-1}^{(I_\ell)} + s_i + r_i \cdot e_i \pmod{q}. \end{aligned}$$

  where $\boldsymbol{x}_{[1,i]}^{(I_\ell)}$ is defined to be $\bigcup_{j \le i, \alpha_j = I_\ell} \{x_j\}$. For every $I_{\ell'} \in \mathcal{I} \backslash \{I_\ell\}$, let $y_i^{(I_{\ell'})} := y_{i-1}^{(I_{\ell'})}$.
  P_i sends $(\boldsymbol{x}_{[1,i]}, y_i^{(I_1)}, \ldots, y_i^{(I_N)})$, $\{m_\ell\}$ and $\boldsymbol{\alpha}_{[1,i]}$ to P_{i+1}. Also let $P_{n+1} := V$.

Verification step: Suppose that the verifier V receives a multi-signature $(\boldsymbol{x}, y_n^{(I_1)}, \ldots, y_n^{(I_N)})$ for a set of message $\{m_\ell\}$ with signers' intentions $\boldsymbol{\alpha}$. Then V computes $e_i := f_i(\boldsymbol{x}_{[1,i]}^{(I_\ell)}, m_\ell)$ for each $i \in [1, n]$. Also the verifier V checks the following equations by the received $(\boldsymbol{x}, y_n^{(I_1)}, \ldots, y_n^{(I_N)})$.

$$g^{y_n{}^{(I_\ell)}} \stackrel{?}{\equiv} \prod_{\substack{1 \le i \le n \\ \alpha_i = I_\ell}}^{n} \left(x_i^{(I_\ell)^{e_i}} \cdot v_i^{(I_\ell)} \right) \pmod{p} \quad (\forall I_\ell \in \mathcal{I})$$

The set of public-keys $\boldsymbol{v}^{(I_\ell)}$ is defined to be $\bigcup_{\alpha_i=I_\ell}\{v_i\}$, and where $\boldsymbol{x}^{(I_\ell)}$ and $\boldsymbol{e}^{(I_\ell)}$ are defined as well as $\boldsymbol{v}^{(I_\ell)}$. As we can guess from the primitive method given above, the total signature size in the primitive method turns out to be $n|p| + N|q|$, by $(N-1)|q|$ which is larger than the signature size in the scheme [7].

4 Proposed scheme

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 gets 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 [7]. 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 $f_i : \{0,1\}^* \to \mathbf{Z}_q$, and that anyone can access the public random oracle function $h : \{0,1\}^* \to \mathbf{Z}_q$.

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 $\mathcal{P}$ 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 $(\boldsymbol{x}_{[1,i-1]}, y_{i-1})$, m and $\boldsymbol{\alpha}_{[1,i-1]}$ from P_{i-1}. P_i chooses her intention $\alpha_i \in \mathcal{I}$, and picks up a random $r_i \in \mathbf{Z}_q$ and computes (x_i, e_i, y_i) as follows:

$$\begin{aligned} x_i &:= g^{r_i} \pmod p, \\ e_i &:= f_i(\boldsymbol{x}_{[1,i]}, m, \boldsymbol{\alpha}_{[1,i]}), \\ y_i &:= y_{i-1} + s_i \cdot \theta_i + r_i \cdot e_i \pmod q, \end{aligned}$$

  where $\theta_i := h(\alpha_i)$. P_i sends $(\boldsymbol{x}_{[1,i]}, y_i)$, m and $\boldsymbol{\alpha}_{[1,i]}$ to P_{i+1}. Also let $P_{n+1} := V$.

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

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

5 Security Consideration

In this section, we prove that the proposed scheme is secure against *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-$\boldsymbol{\alpha}$ adversary Given the system parameter (p, q, g) and the public-keys $\boldsymbol{v}$, an MS-$\boldsymbol{\alpha}$ adversary $\mathcal{M}$ 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:

(S1) An MS-$\boldsymbol{\alpha}$ adversary $\mathcal{M}$ determine a message m_j, a signer P_{i_j}, and the signer's intention $\boldsymbol{\alpha}_j \in \mathcal{I}^n$,
(S2) Generate a valid partial multi-signature $(\boldsymbol{x}_{[1,i_j-1]}, \boldsymbol{e}_{[1,i_j-1]}, y_{i_j-1})$ by colluding with $\mathcal{P}\backslash\{P_{i_j}\}$,
(S3) Send $(\boldsymbol{x}_{[1,i_j-1]}, \boldsymbol{e}_{[1,i_j-1]}, y_{i_j-1}, \boldsymbol{\alpha}_{j[1,i_j-1]})$ and α_{j,i_j} to P_{i_j}. To make tha adversary stronger, we assume $\mathcal{M}$ can ask P_{i_j}'s signature for P_{i_j}'s intention $\mathcal{M}$ chooses.
(S4) And get a valid partial multi-signature $(\boldsymbol{x}_{[1,i_j]}, \boldsymbol{e}_{[1,i_j]}, y_{i_j})$ and the singers' intentions $\boldsymbol{\alpha}_{[1,i_j]}$ from P_{i_j}.

After Q iterations of this step, the adversary $\mathcal{M}$ computes a multi-signature for a message m with signers' intentions $\boldsymbol{\alpha}$, where for every $j \in [1, Q]$, it must hold at least one of $m \neq m_j$ and $\boldsymbol{\alpha}_{j[i_j,i_j]} \neq \boldsymbol{\alpha}_{[i_j,i_j]}$.
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 [7] is adopted. Hence we don't have to consider *the key generation phase attacks* given by [8].

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 1. Suppose an MS-$\boldsymbol{\alpha}$ adversary (probabilistic Turing machine) $\mathcal{M}$ 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-$\boldsymbol{\alpha}$ adversary $\mathcal{M}$ can forge a multi-signature $(\boldsymbol{x}, \boldsymbol{e}, y_n)$ for a message m with signers' intentions $\boldsymbol{\alpha}$ in time at most t with probability at least ϵ, then we say that $\mathcal{M}$ can $(t, Q, \boldsymbol{R}, \epsilon) -$ *break the multi-signature scheme with signers' intentions.* Here, the probability is taken over the coin flips of $\mathcal{M}, f_1, \ldots, f_n$ and signing oracles $\mathcal{P}$.

Definition 2. A multi-signature scheme with signers' intentions is said to be $(t, Q, \boldsymbol{R}, \epsilon) -$ *secure*, if there is no MS-$\boldsymbol{\alpha}$ adversary which can $(t, Q, \boldsymbol{R}, \epsilon)$-break the scheme, and if for a message m, a multi-signature $(\boldsymbol{x}, \boldsymbol{e}, y_n)$ which is valid for signers' intentions $\boldsymbol{\alpha}$, is invalid for another signers' intentions $\boldsymbol{\alpha}'$ with overwhelming probability.

5.3 Identification schemes

As we can seen in [7], the security of the multi-signature scheme given by [7] 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, and both of them can access the public random oracle function $h : \{0,1\}^* \to \mathbf{Z}_q$.

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 $s_i \in \mathbf{Z}_q$ 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 $\boldsymbol{\alpha} \in \mathcal{I}$ with $\#\boldsymbol{\alpha} = n$. First P picks up n random $r_i \in \mathbf{Z}_q$, 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, α_i) to V, and V randomly picks up the challenge $e_i \in \mathbf{Z}_q$, and sends it to P.

After this iteration, P computes the answer

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

where $\theta_i := h(\alpha_i)$. Then P sends y to V.
Receiving $(\boldsymbol{x}, y)$ and $\boldsymbol{\alpha}$, the verifier V figures out θ_i for each $i \in [1,n]$. V checks $(\boldsymbol{x}, y)$ and $\boldsymbol{\alpha}$ by following verification:

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

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 $\boldsymbol{\alpha} \in \mathcal{I}$ with $\#\boldsymbol{\alpha} = n$. (This distribution does not have to be uniform.)

Identification step: P picks up n random $r_i \in \mathbf{Z}_q$, 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.

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

Definition 3. Suppose that an ID-adversary $\mathcal{M}$ which does not have $\boldsymbol{s}$, can pass the verification for some $\boldsymbol{\alpha}$ in time at most t with probability at least ϵ. Then we say that ID-adversary $\mathcal{M}$ can $(t, \epsilon)-$*break the multi-round identification schemes.*

Definition 4. We say that a multi-round identification scheme is $(t, \epsilon)-$*secure*, if there is no ID-adversary which can (t, ϵ)-break the scheme, $(\boldsymbol{x}, \boldsymbol{e}, y)$ which can pass the verification for intentions $\boldsymbol{\alpha} \in \mathcal{I}$, does not pass the verification for another (distinct) intentions $\boldsymbol{\alpha}'$ with overwhelming probability.

We define *the zero-knowledge property* for Scheme $\mathtt{ID}-\mathtt{B}$ as follows:

Definition 5. Suppose that a polynomial-time machine $\mathcal{S}$ is given public-key $\boldsymbol{v}$ and intentions $\boldsymbol{\alpha}$. Then we say the scheme has *the perfect zero-knowledge property*, if

$$\sum_{\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu} \left| \Pr[(\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu) \leftarrow [P(\boldsymbol{s}, \boldsymbol{\alpha}), V(\boldsymbol{v}, \boldsymbol{\alpha})]] - \Pr[(\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu) \leftarrow \mathcal{S}(\boldsymbol{v}, \boldsymbol{\alpha})] \right| = 0$$

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

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

Such an $(\boldsymbol{x}, \boldsymbol{e}, y)$ indeed passes the verification.

Lemma 1. Scheme ID-B has *the perfect zero-knowledge property*

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

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

- $\Pr\left[(\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu) \leftarrow [P(\boldsymbol{s}, \boldsymbol{\alpha}), V(\boldsymbol{v}, \boldsymbol{\alpha})]\right] = 1/q^{2n}$
- $\Pr\left[(\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu) \leftarrow \mathcal{S}(\boldsymbol{v}, \boldsymbol{\alpha})]\right] = 1/q^{2n}$

– The probability of appearance of the $(2n+1)$-tuple $(\boldsymbol{x}, \boldsymbol{e}, y)$ which can't pass the verification for some $\boldsymbol{\alpha}$.
- $\Pr\left[(\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu) \leftarrow [P(\boldsymbol{s}, \boldsymbol{\alpha}), V(\boldsymbol{v}, \boldsymbol{\alpha})]\right] = 0$
- $\Pr\left[(\boldsymbol{\kappa}, \boldsymbol{\lambda}, \mu) \leftarrow \mathcal{S}(\boldsymbol{v}, \boldsymbol{\alpha})]\right] = 0$

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

An adversary model for Scheme $\mathtt{ID}-\mathtt{A}$ is given as follows.

ID-adversary

An ID-adversary $\mathcal{M}$ is a machine, which, on input $\boldsymbol{v}$, executes Scheme $\mathtt{ID}-\mathtt{A}$ with V, and tries to pass the verification for some signers' intentions $\boldsymbol{\alpha}$. The ID-adversary $\mathcal{M}$ is so-called a *passive attacker*, which cannot accomplish *the attack in the middle.*

5.4 ID-reduction lemma

If Scheme $\mathtt{ID}-\mathtt{B}$ provides the zero-knowledge property, we can obtain the following ID-reduction lemma.

Lemma 2. (i) If there exists an MS-$\boldsymbol{\alpha}$ adversary which can $(t, Q, \boldsymbol{R}, \epsilon)-$break the scheme, then there also exists an MS-$\boldsymbol{\alpha}$ adversary which can $(t, Q, \mathbf{1}, \epsilon_1)-$break the scheme, where $\mathbf{1}$ 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-$\boldsymbol{\alpha}$ adversary which can $(t, Q, \mathbf{1}, \epsilon_1)-$break the scheme, then there also exists an MS-$\boldsymbol{\alpha}$ adversary which can $(t^+, 0, \mathbf{1}, \epsilon_{\mathtt{p}})-$ break the scheme, where $t^+ := t + \Phi_{\mathtt{S}}$, $\Phi_{\mathtt{S}}$ is the simulation time of Q multi-signatures and $\epsilon_{\mathtt{p}} := \epsilon_1 - \frac{Q}{q}$.

(iii) If there exists an MS-$\boldsymbol{\alpha}$ adversary which can $(t^+, 0, \mathbf{1}, \epsilon_{\mathtt{p}})-$break the scheme, then there also exists an ID-adversary which can $(t^+, \epsilon_{\mathtt{p}})-$ break the scheme.

Proof. (Sketch) The proof is also the same with that of Lemma 9 in [7]. □

Lemma 3. Let $\epsilon_{\mathtt{p}} \geq \frac{2^{n+1}}{q^n}$. If there exists an ID-adversary which can $(t^+, \epsilon_{\mathtt{p}})-$break the scheme, then there exists a machine $\mathcal{M}$ which can compute a linear combination of $\boldsymbol{s}$ on input $\boldsymbol{v}$ in time t' with success probability ϵ'. Here t' and ϵ' are defined as follows:

$$t' := \frac{t^{++}}{3\epsilon_{\mathtt{p}}}\left(2^{(2n+1)}+1\right) + \Phi_{\mathtt{C}}\ ; \quad \epsilon' := \prod_{i=1}^{n-1} p_i(\epsilon_{\mathtt{p}}).$$

Here $p_1(\epsilon_{\mathtt{p}}) := \left(1-\left(1-\epsilon_{\mathtt{p}}\right)^{\frac{1}{\epsilon}}\right)$; $p_i(\epsilon_{\mathtt{p}}) := \left(\frac{1}{2}\left(1-\left(1-\frac{\epsilon_{\mathtt{p}}}{2^i}\right)^{\frac{2^i}{\epsilon}}\right)\right)^{2^{(i-1)}}$ $(i \geq 1)$;

where $t^{++} := t^{+} + \Phi_{\mathtt{V}}$, $\Phi_{\mathtt{V}}$ is the verification time of identification protocol, $\Phi_{\mathtt{C}}$ is the calculation time of $\boldsymbol{s}$ in the final stage of reduction.

Proof. (Sketch) Also for Scheme `ID-A`, we can obtain the Heavy row lemma like [7]. Hence we can obtain 2^n simultaneous equations with $(2^n + n - 1)$ unknowns. Among those unknowns, the n ones the secret-keys, and the rest are r components. From these equations, we can get one linear combination on only $\boldsymbol{s}$. The required time and the probability can be obtained as well as in [7]. □

By providing n linear combinations on $\boldsymbol{s}$, we can find each s_i. Unfortunately, we cannot evaluate the probability that those equations are linear independent. In case $n = 2$, if the coefficients were uniform, then that probability would be at least $1 - \frac{2}{q}$.

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

Lemma 4. Suppose that the tuple $(\boldsymbol{x}, \boldsymbol{e}, y)$ passes the verification for signers' intentions $\boldsymbol{\alpha} \in \mathcal{I}$. Then the very tuple $(\boldsymbol{x}, \boldsymbol{e}, y)$ is rejected for another signers' intentions $\boldsymbol{\alpha}'$ with overwhelming probability.

Proof. (Sketch) It comes from the following:

$$\mathtt{Pr}\left[(\boldsymbol{x}, \boldsymbol{e}, y, \boldsymbol{\alpha}) \leftarrow [P(\boldsymbol{s}), V(\boldsymbol{v})] : \mathtt{Ver}(\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{e}, y, \boldsymbol{\alpha}') = 1 \,\middle|\, \mathtt{Ver}(\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{e}, y, \boldsymbol{\alpha}) = 1\right] \leq 1/q$$

holds for $\boldsymbol{\alpha}, \boldsymbol{\alpha}' \in \mathcal{I}$ with $\boldsymbol{\alpha} \neq \boldsymbol{\alpha}'$, where `Ver` is the verification equation. □

Combining Lemmas 2, 3 and 4, we can obtain the following theorem.

Theorem 1. Let $\epsilon_{\mathtt{p}} \geq \frac{2^{n+1}}{q^n}$. If there is no machine which can, on input $\boldsymbol{v}$, compute a linear combination on $\boldsymbol{s}$, in time t' with success probability ϵ', then the proposed multi-signature scheme with signers' intentions is $(t, Q, \boldsymbol{R}, \epsilon)-$*secure.*

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

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. In evaluating the computational cost, more important is $\#(\bigcup_i \{\alpha_i\})$, which is the most variety of the intentions actually chosen by $\mathcal{P}$, rather than $\#\mathcal{I}$, which is the number of the intentions provided for the message.

The required number of modular-p multiplication 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 $\left(\frac{n}{2} + 1\right)|q| - 1$. 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.

Table 1. Comparison of schemes

	total size of signatures	# of modular-p multiplications for verification
Primitive method	$n\|p\| + \#(\bigcup_i \{\alpha_i\})\|q\|$	$\left\{\frac{n+3\#\left(\bigcup_i \{\alpha_i\}\right)}{2}\right\}\|q\| - \#(\bigcup_i \{\alpha_i\}) + n$
Proposed scheme	$n\|p\| + \|q\|$	$\left(\frac{2n+3}{2}\right)\|q\| - 1$

In the primitive method, the required number of modular-p multiplications is related to $\#\left(\bigcup_i \{\alpha_i\}\right)$. In other words, the primitive method loses its merit in proportion to the increase of $\#\left(\bigcup_i \{\alpha_i\}\right)$, because $\#\left(\bigcup_i \{\alpha_i\}\right)$ 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.

Acknowledgement

The authors would like to thank Mr. Takeshi Okamoto of JAIST for his invaluable advice and useful comments.

References

[1] M. Bellare and P. Rogaway: *"Random oracles are practical: A paradigm for designing efficient protocols"*, Proceedings of the 1st Conference on Computer and Communications Security, ACM, 1993.

[2] M. Burmester, Y. Desmedt, H. Doi, M. Mambo, E. Okamoto, M. Tada and Y. Yoshifuji: *"A Structured ElGamal-Type Multisignature Scheme"*, Lecture Notes in Computer Science 1751, Third International Workshop on Practice and Theory in Public Key Cryptosystems - PKC2000, Springer-Verlag, pp.466-483, 2000.

[3] H. Doi, M. Mambo and E. Okamoto: *"On the Security of the RSA-Based Multisignature Scheme for Various Group Structures"*, Lecture Notes in Computer Science 1841, 5th Australasian Conference - ACISP2000, Springer-Verlag, pp.352-367, 2000.

[4] H. Doi, E. Okamoto and M. Mambo: *"Multisignature Schemes for Various Group Structures"*, The 36-th Annual Allerton Conference on Communication, Control and Computing, pp.713-722, 1999.

[5] H. Doi, E. Okamoto, M. Mambo and T. Uematsu: *"Multisignature Scheme with Specified Order"*, Proc. of the 1994 Symposium on Cryptography and Information security, SCIS94-2A, January 27-29, 1994.

[6] S. Mitomi and A. Miyaji: *"A multisignature Scheme with Message Flexibility, Order Flexibility and Order Verifiability"*, Lecture Notes in Computer Science 1841, 5th Australasian Conference - ACISP2000, Springer-Verlag, pp.298-312, 2000.

[7] K. Ohta and T. Okamoto: *"Multi-Signature Schemes Secure against Active Insider Attacks"*, IEICE transactions of fundamentals, vol. E-82-A. No.1, 1999.

[8] K. Ohta and T. Okamoto: *"Generic Construction Method of Multi-Signature Schemes"*, Proc. of The 2001 Symposium on Cryptography and Information Security, SCIS01-2B, January 23-26, 2001.

[9] D. Pointcheval and J. Stern: *"Security arguments for digital signatures and blind signatures"*, Journal of Cryptology, Volume 13, Number 3. pp.361-396, Springer-Verlag, 2000.

[10] A. Shimbo: *"Design of a modified ElGamal Signature Scheme"*, Proc. of The 1996 Workshop on Design and Evaluation of Cryptographic Algorithms, pp.37-44, November 27, 1996.