

A Structured Multisignature based on a Non-Commutative Ring Homomorphism

Naoto Yanai*, Eikoh Chida**, and Masahiro Mambo*

* Graduate School of System and Information Engineering
University of Tsukuba

E-mail: s0920776@coins.tsukuba.ac.jp, mambo@cs.tsukuba.ac.jp,

** Department of Electrical and Computer Engineering
Ichinoseki National College of Technology

E-mail: chida@ichinoseki.ac.jp

Abstract. Users' signing order is an important factor in multisignature schemes. In fact the signing order often reflects signer's rank in a signing group. So far, many multisignature schemes, called structured schemes, have been proposed that provide verifiability of the signing order associated with the structure of a group of signers. However, there are not many structured multisignature schemes utilizing an algebraic structure of underlying algebraic operation. In this paper, we adopt a non-commutative ring homomorphism for constructing a structured multisignature scheme and study the security of the constructed scheme under the discrete logarithm assumption.

Key words: Multisignature, Ring Homomorphism, Hierarchical Structure

1 Introduction

Electronic documents are prone to manipulation and digital signature is effective for proving legitimacy of the electronic documents. The electronic documents are often handled by multiple persons and authenticity of the documents should be guaranteed not only by a single person but by all associated persons. Multisignature allows multiple persons to sign a document and is suitable for such a situation.

In multisignature schemes, there are many cases where a signing order among signers is important. If the signing order is determined by signers' rank, such an order should be verifiable. A multisignature scheme is called structured scheme when a created multisignature represents the structure among signers. In the structured scheme, the signing order of signers with the same rank does not need to be considered, but that of signers with different rank needs to be.

Most of the structured schemes do not utilize the algebraic structure of underlying algebraic operation. We anticipate that algebraic structure is a rich

source for extending cryptographic schemes in various ways. In this paper, we construct a structured signature based on a non-commutative ring homomorphism and study the security of the proposed scheme.

2 Preliminaries

2.1 Non-Commutative Ring Homomorphism

In general, homomorphisms are defined as follows [2].

Let $\mathbb{G}_1, \mathbb{G}_2$ be groups with respect to the operations ' \circ ', ' \bullet ', respectively. We say that a function $f : \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a homomorphism from \mathbb{G}_1 to \mathbb{G}_2 if the following condition hold.

$$\text{For all } a, b \in \mathbb{G}_1, f(a \circ b) = f(a) \bullet f(b)$$

Let $\mathbb{R}_1, \mathbb{R}_2$ be rings with respect to the operations ' $+$ ', ' $*$ ', and ' \dagger ', ' \circ ', respectively. We say that a function $f : \mathbb{R}_1 \rightarrow \mathbb{R}_2$ is a ring homomorphism from \mathbb{R}_1 to \mathbb{R}_2 if the following condition hold.

$$\text{For all } a, b \in \mathbb{R}_1, \text{ and } f(a + b) = f(a) \dagger f(b), f(a * b) = f(a) \circ f(b)$$

We say that a function $f : \mathbb{R}_1 \rightarrow \mathbb{R}_2$ is a non-commutative ring homomorphism if multiplications $*$ and \circ are non-commutative operations, respectively.

We say that a function f is a one-way function if the following conditions hold.

- It is easy to calculate $f(x)$ from input x .
- It is difficult to calculate x from input $f(x)$.

The existense of a one-way function has not been proved yet. At the same, it is not proved that the function does not exist. Hereafter, we assume that a powering function is a one-way function. Computing the inverse of the powering function is called the discrete logarithm problem, DLP, and under the assumption described above DLP is difficult to solve.

A Example of Ring Homomorphism

We explain known results shown in [3]. The following non-commutative ring homomorphism is proposed.

- Definition of Operations

Addition ' \dagger ', multiplication ' \circ ' and addition ' $\dot{+}$ ', multiplication ' \odot ' are defined in rings \mathbb{R}, \mathbb{S} , respectively. We denote them by $(\mathbb{R}, \dagger, \circ)$, $(\mathbb{S}, \dot{+}, \odot)$. Those operations are defined as follows.

$$\begin{aligned} \dot{+} : \begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} \dot{+} \begin{pmatrix} b_1 & y \\ 0 & b_2 \end{pmatrix} &= \begin{pmatrix} a_1 + b_1 & x + y \\ 0 & a_2 + b_2 \end{pmatrix} \\ \odot : \begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} \odot \begin{pmatrix} b_1 & y \\ 0 & b_2 \end{pmatrix} &= \begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot y + b_2 \cdot x \\ 0 & a_2 \cdot b_2 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \dagger : \begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} \dagger \begin{pmatrix} b_1 & y \\ 0 & b_2 \end{pmatrix} &= \begin{pmatrix} a_1 + b_1 & x \cdot y \\ 0 & a_2 + b_2 \end{pmatrix} \\ \circ : \begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} \circ \begin{pmatrix} b_1 & y \\ 0 & b_2 \end{pmatrix} &= \begin{pmatrix} a_1 \cdot b_1 & y^{a_1} \cdot x^{b_2} \\ 0 & a_2 \cdot b_2 \end{pmatrix} \end{aligned}$$

– Definition of Function

A concrete one-way function $f : \mathbb{R} \rightarrow \mathbb{S}$ is defined as follows.

$$f \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) \equiv \begin{pmatrix} a \bmod p - 1 & g^b \bmod p \\ 0 & d \bmod p - 1 \end{pmatrix}$$

The one-way function $f : \mathbb{R} \rightarrow \mathbb{S}$ is proved to be a non-commutative ring homomorphism.

2.2 Related Work

A multisignature scheme using an extended RSA system is proposed in [5], and up until now many multisignature schemes have been proposed ([4,6,7,8,9,12,13]). Multisignature schemes that consider the signing order based on the structure among signers are proposed in [6, 7, 8, 9]. Most of such structured schemes do not utilize algebraic structure of underlying algebraic operation except the scheme in [9]. In [9], a structured multisignature scheme is proposed that utilizes non-commutative ring homomorphism for verifying the signing order among signers. However, the scheme in [9] does not accurately reflect the hierarchical structure of signers, because the scheme in [9] generates a different multisignature when the signing order is changed among signers with the same rank. Therefore, this paper proposes a multisignature scheme that fully reflects the hierarchical structure of signers by utilizing a non-commutative ring homomorphism. The proposed scheme generates the same multisignature even if the signing order is changed among signers with the same rank.

3 Construction of the Multisignature Scheme

3.1 Basic Idea

Fig.3-1 is a model of multisignature that consider both the signing order and hierarchical structure. In this figure, We assume that Charlie has higher commission than Alice and Bob. For signing a message m , Alice and Bob should to sign it ahead of Charlie. Signing from the lower rank often occurs in organizations.

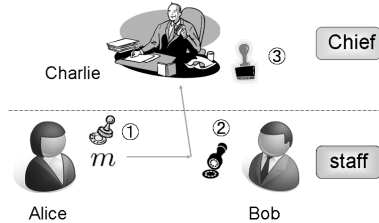


Fig.3-1. A model considering hierarchical structures

Signature schemes that have been in a practical use are constructed by a group homomorphism. The difference between a group and a ring is the number of operations. Various cryptographic functionalities would be realized by the increased number of operations.

When the signing order is important in a group homomorphism, non-commutative operation is appropriate. In this case, when the order between Alice and Bob is changed, we obtain a different result. That is,

$$\sigma_A * \sigma_B * \sigma_C \neq \sigma_B * \sigma_A * \sigma_C.$$

Here, σ_A denotes Alice's signature. Similarly, σ_B and σ_C denote Bob's signature and Charlie's signature, respectively. Next, we think about a case where a signature scheme is constructed by a commutative operation. In this case, the result does not change even if the order between Alice and Charlie is changed. That is,

$$\sigma_A \circ \sigma_B \circ \sigma_C = \sigma_A \circ \sigma_C \circ \sigma_B.$$

As a combination of these operations, a structured signature scheme can be constructed by a non-commutative ring homomorphism. Non-commutative operation is used between signers of different ranks, i.e. for a serial structure [7], and commutative operation is used between signers of the same rank, i.e. for a parallel structure [7].

We consider that signers with the same rank belong to a group, and all signers belong to somewhere in those groups. Whenever they send the generated multisignature to other group, they generate their signatures ahead.

3.2 Proposed Multisignature based on a Non-Commutative Ring Homomorphism

In this section, we propose a multisignature scheme based on a non-commutative ring homomorphism described in section 2.1. This scheme is a multisignature scheme that deals with hierarchical structure among signers.

Let the number of signers be N . In the scheme, signers are denoted by U_i ($1 \leq i \leq N$), and verifier denoted by V . We assume existence of a trusted center that generates signers' parameters.

Key Generation

1. A trusted center generates a big prime number p . Then, a trusted center chooses g from a finite field \mathbb{F}_p^* and, let the order of g be l .
2. All signers generate secret key $x_i \in \mathbb{Z}_l$ and public key y_i such that $y = g^{x_i} \text{ mod } p$.
3. All signers generate themselves ID information ID_i and rank information $rank_i$.
4. All signers exhibit $y_i, ID_i, rank_i$ to a public list.

All signer can find the information in the public list. All signer have each hash function $H_i : \{0, 1\}^* \rightarrow \{0, 1\}^k$.

Multisigning For simplicity, we assume that each multisignature is processed by U_i in the order from signer U_i to U_N . Each $U_i(1 \leq i \leq N)$ receives previous signer's multisignature $\tilde{\sigma}_i$ and public information $\mathbb{Y}_i, \mathbb{ID}_i, \mathbb{RANK}_i, \mathbb{U}_{i,j}$. The verification is performed by using the equation (1). If U_i is the first one, then the verification process is omitted.

U_i chooses random number $r_{i,1}, r_{i,2}, r_{i,3} \in \mathbb{Z}_l$, and calculates $u_{i,2} = g^{r_{i,2}} \bmod l$. Then, U_i calculates as follows.

$$\sigma_i \equiv \begin{pmatrix} r_{i,1} x_i + r_{i,2} H(M) \bmod p - 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} u_{i,1} & v_i \\ 0 & u_{i,3} \end{pmatrix},$$

if $rank_{i-1} = rank_i$, $\tilde{\sigma}_i \equiv \sigma_{i-1} \dot{+} \sigma_i$,
otherwise, $\tilde{\sigma}_i \equiv \sigma_{i-1} \odot \sigma_i$.

U_i sets $\mathbb{Y}_i = \mathbb{Y}_{i-1} || y_i$, $\mathbb{ID}_i = \mathbb{ID}_{i-1} || ID_i$, $\mathbb{RANK}_i = \mathbb{RANK}_{i-1} || rank_i$, $\mathbb{U}_{i,j} = \mathbb{U}_{i-1,j} || u_{i,j}$. If U_i is the first one, let the informations be $\mathbb{Y}_0 = \mathbb{ID}_0 = \mathbb{RANK}_0 = \mathbb{U}_{0,j} = \emptyset$, and $\tilde{\sigma}_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Then, $\tilde{\sigma}_1 \equiv \tilde{\sigma}_0 \dot{+} \sigma_1$. Finally, U_i gives $(\tilde{\sigma}_i, \mathbb{Y}_i, \mathbb{ID}_i, \mathbb{RANK}_i, \mathbb{U}_{i,j})$ to the next signer U_{i+1} . The last signer U_N sends $(\tilde{\sigma}_N, \mathbb{Y}_N, \mathbb{ID}_N, \mathbb{RANK}_N, \mathbb{U}_{N,j}, M)$ to a verifier V .

Verification If the following congruence holds for $i = N$, then a verifier outputs *accept*, otherwise outputs *reject*.

$$f(\tilde{\sigma}_i) \equiv \left(\dots \left(\begin{pmatrix} u_{1,1} y_1 \cdot u_{1,2}^{H(M)} \\ 0 \end{pmatrix} * \begin{pmatrix} u_{2,1} y_2 \cdot u_{2,2}^{H(M)} \\ 0 \end{pmatrix} \right) \dots \right) * \begin{pmatrix} u_{i,1} y_i \cdot u_{i,2}^{H(M)} \\ 0 \end{pmatrix} \quad (1)$$

Here, the operand $*$ is either $\dot{+}$ or \odot . The operand depends on \mathbb{ID}_i and \mathbb{RANK}_i . To be specific, if $rank_{i-1} = rank_i$, then $*$ is $\dot{+}$. Otherwise, $*$ is \odot . The calculating order depends on \mathbb{ID}_i .

4 The Security of the Proposed Scheme

We apply the security analysis given in [6] to our scheme. Since the multisignature scheme described in [6] deals with only serial structures and our scheme deals with both serial and parallel structures, the same result as in [6] may not be derived even if we do not consider the change of signer structure. Thus, we show the difficulty of signature forgery with a fixed signer structure in the proposed scheme at first. After that, we discuss the security of the signing order in subsection 4.6.

4.1 Definitions related to security

Definition 1 A probabilistic turing machine A breaks a key searching problem with (t, ϵ) if and only if A can find a secret key from a public key with success probability greater than ϵ within performing time t .

Definition 2 A key searching problem is (t, ϵ) -secure if and only if there is no probabilistic turing machine that can break it with (t, ϵ) .

Definition 3 A probabilistic turing machine A breaks an identification scheme with (t, ϵ) if and only if A as a prover can cheat honest verifier V with success probability greater than ϵ within performing time t .

Definition 4 An identification scheme is (t, ϵ) -secure if and only if there is no probabilistic turing machine that can break it with (t, ϵ) .

Definition 5 A probabilistic turing machine A breaks multisignature scheme with (t, ϵ) if and only if A can forge a multisignature of a message with success probability greater than ϵ within performing time t . Here, A doesn't conduct any attack that A acts as a verifier with a true prover.

Definition 6 A multisignature scheme is (t, ϵ) -secure if and only if there is no probabilistic turing machine that can break multisignature with (t, ϵ) .

Definition 7 A probabilistic turing machine A breaks a multisignature scheme with $(t, l_{sig}, l_{H_1}, \dots, l_{H_N}, \epsilon)$ if and only if A can forge a multisignature of a message with a success probability greater than ϵ within performing time t . Here, A can perform adaptive chosen message insider attack with l_{sig} pair of A 's intermediate partial signature and Prover's signature, and q_{H_i} query to H_i .

Definition 8 A multisignature scheme is $(t, l_{sig}, l_{H_1}, \dots, l_{H_N}, \epsilon)$ -secure against signature forgery with the same signer structure. if and only if there is no probabilistic turing machine that can break multisignature with $(t, l_{sig}, l_{H_1}, \dots, l_{H_N}, \epsilon)$.

Definition 9 A structured multisignature scheme resists against a signature forgery associated with the signing order if and only if there is no probabilistic turing machine that can forge a multisignature with the signing order.

4.2 Multi-Round Identification Scheme

To analyze the proposed scheme, we consider the following multi-round identification scheme.

Key Generation

1. A trusted center generates a big prime number p . Then, a trusted center chooses g from a finite field \mathbb{F}_p^* , and let the order of g be l .
2. Prover P generates N secret keys $x_i \in \mathbb{Z}_l$ and N public keys y_i such that $y_i = g^{x_i}$, where N is number of signers.
3. Prover P generates N signers' ID informations ID_i and rank informations $rank_i$.

Multi-Round Identification Iterate the following steps for $i = 1$ to N .

1. Prover P chooses three random number $r_{i,1}, r_{i,2}, r_{i,3} \in \mathbb{Z}_l$, and calculates $u_{i,2} = g^{r_{i,2}}$. Then, P sends $u_{i,j}$ ($1 \leq j \leq 3$) to verifier V . Here, $u_{i,1} = r_{i,1}, u_{i,3} = r_{i,3}$.
2. V generates random number d_i where d_i is answer of hash query $H_i(M)$. Then, V sends d_i to P .
3. P calculates as follows.

$$\sigma_i \equiv \begin{pmatrix} r_{i,1} x_i + r_{i,2} d_i \bmod p - 1 \\ 0 \quad r_{i,3} \end{pmatrix} \equiv \begin{pmatrix} u_{i,1} & v_i \\ 0 & u_{i,3} \end{pmatrix},$$

if $rank_{i-1} = rank_i$, $\tilde{\sigma}_i \equiv \sigma_{i-1} \dagger \sigma_i$,
otherwise, $\tilde{\sigma}_i \equiv \sigma_{i-1} \circ \sigma_i$.

4. P sends ID_i and $rank_i$ to V .

P sends $\tilde{\sigma}_N$ to V . Then, V check the following equation.

$$f(\tilde{\sigma}_i) \equiv \left(\dots \left(\begin{pmatrix} u_{1,1} & y_1 \cdot u_{1,2}^{d_1} \\ 0 & u_{1,3} \end{pmatrix} * \begin{pmatrix} u_{2,1} & y_2 \cdot u_{2,2}^{d_2} \\ 0 & u_{2,3} \end{pmatrix} \right) \dots \right) * \begin{pmatrix} u_{N,1} & y_N \cdot u_{N,2}^{d_N} \\ 0 & u_{N,3} \end{pmatrix}$$

Here, the operand is either \dagger or \circ . The operand depends on ID_i and $rank_i$. To be specific, if $rank_{i-1} = rank_i$, then $*$ is \dagger . Otherwise, $*$ is \circ .

Lemma 10 (Reduction Lemma of Multisignature) Let $\epsilon \geq \frac{1}{l}(l_{H_1}(l_{H_2}(\dots(l_{H_{N-1}}(l_{H_N}(\frac{2^{N+1}}{l^{N-1}} + l_{sig}) + 1) + 1) \dots) + 1) + 1)$.

1. If A_1 breaks a multisignature with $(t_1, l_{sig}, l_{H_i}, \dots, l_{H_N}, \epsilon_1)$, then there exists A_2 which breaks a multisignature with $(t_1, l_{sig}, 1, \dots, 1, \epsilon_2)$, where ϵ_2 is based on ϵ_{H_i} for $(1 \leq i \leq N)$. Here, let $\epsilon_{H_0} = \epsilon_1, \epsilon_{H_i} = \frac{\epsilon_{H_{i-1}} - \frac{1}{l}}{l_{H_i}}$.
2. If A_2 breaks a multisignature with $(t_1, l_{sig}, 1, \dots, 1, \epsilon_2)$, there exists A_3 which breaks a multisignature with $(t_3, 0, 1, \dots, 1, \epsilon_3)$, where $t_3 = t +$ (the simulation time of l_{sig} signatures) and $\epsilon_3 \geq \epsilon_2 - \frac{l_{sig}}{l}$.
3. If A_3 breaks a multisignature $(t_3, 0, 1, \dots, 1, \epsilon_3)$, there exists A_4 which breaks a multi-round identification scheme with (t_3, ϵ_3) .

Proof: The proof is almost the same with Lemma 9 in [6] and is omitted here.

4.3 Hierarchical Heavy Row Lemma

We use the hierarchical structures of a Boolean matrix and heavy row introduced in [6] to prove the security of our scheme. Assume that there is cheater A that can break multi-round identification scheme with (t, ϵ) .

Definition 11 We consider that the possible outcomes of the performing of a cheater A and an honest verifier V are denoted by a Boolean matrix $\mathcal{H}_i(r, d_1, \dots, d_{i-1}; d_i, \dots, d_N)$. The rows of the matrix correspond to all possible choices of r, d_1, \dots, d_{i-1} , where r is a random tape and d_1, \dots, d_{i-1} are all possible choices of hash function. The columns of the matrix correspond to all possible choices of d_i, \dots, d_N . Its entries are 0 if V rejects A 's proof, and 1 if V accepts A 's proof.

Definition 12 A row of matrix \mathcal{H}_i is i -heavy if the fraction of 1's along the row is at least $\epsilon/2^i$, where ϵ is the success probability of A .

Lemma 13 (Hierarchical Heavy Row Lemma) If the 1's in \mathcal{H} are located in 1-heavy rows of \mathcal{H}_1 , 2-heavy rows of $\mathcal{H}_2, \dots, (i-1)$ -heavy rows of \mathcal{H}_{i-1} simultaneously, then they are also located in i -heavy rows of \mathcal{H}_i with a probability of at least $\frac{1}{2}$.

Proof: The proof is almost the same with Lemma 12 in [6] and is omitted here.

4.4 Security of Multi-Round Identification Scheme

First, consider the case of two signers.

Lemma 14 If finding a secret key x_i from a public key y_i is $(t(2), \epsilon(2))$ -secure, then a multi-round identification scheme is (t, ϵ) -secure, where

$$t(2) = (t + \phi_1) \frac{11}{\epsilon} + \phi_2,$$

$$\epsilon(2) = \frac{1}{8} (1 - (1 - \epsilon)^{1/\epsilon}) (1 - (1 - \frac{\epsilon}{2})^{2/\epsilon}) (1 - (1 - \frac{\epsilon}{4})^{4/\epsilon})^2.$$

Here, ϕ_1 is the verification time of the identification protocol and ϕ_2 is the calculation time of s in the final step.

Sketch of Proof: The operation for the (1,2)-element in the addition '†' can be considered as the multiplication operation for the scheme in [6] and the proof for addition is almost same with Lemma 15 in [6]. On the other hand, the operation for the (1,2)-element in the multiplication 'o' is quite different from the multiplication operation for the scheme in [6]. Even so, our detail analysis shows that we can evaluate the security of the proposed scheme for multiplication in the same way as for addition. Hence, one probes entries along \mathcal{H}_i . The following equation is derived from the equation (1).

$$\begin{pmatrix} u_{1,1} \cdot u_{2,1} & g^{u_{2,3} \cdot v_1 + u_{1,1} \cdot v_2} \\ 0 & u_{1,3} \cdot u_{2,3} \end{pmatrix} \equiv \begin{pmatrix} u_{1,1} \cdot u_{2,1} & (y_1 \cdot u_{1,2}^{d_1})^{u_{2,3}} \cdot (y_2 \cdot u_{2,2}^{d_2})^{u_{1,1}} \\ 0 & u_{1,3} \cdot u_{2,3} \end{pmatrix}.$$

Concerning the (1,2)-element, $g^{u_{2,3} \cdot v_1^{(k)} + u_{1,1} \cdot v_2^{(k)}} = (y_1 \cdot u_{1,2}^{(k)d_1})^{u_{2,3}^{(k)}} \cdot (y_2 \cdot u_{2,2}^{(k)d_2})^{u_{1,1}^{(k)}}$ holds where k denotes k -th challenge in the multi-round identification scheme.

Then, we can calculate the secret parameter with the same success probability and performing time in addition. The whole proof is shown in Appendix A.

As we have seen for the case $N = 2$, there is no difference between the security evaluation result for the serial structure and that for the parallel structure, and we can discuss the security of the proposed scheme for arbitrary $N > 1$ without distinguishing the addition operation and the multiplication operation in our scheme.

Lemma 15 If finding a secret key x_i from a public key y_i is $(t(N), \epsilon(N))$ -secure, then a multi-round identification scheme is (t, ϵ) -secure, where

$$t(N) = (t + \phi_1) \frac{2^{(2N+1)} + 1}{3\epsilon} + \phi_2,$$

$$\epsilon(N) = \prod_{i=0}^N p_i(\epsilon).$$

Here,

$$p_0(\epsilon) = (1 - (1 - \epsilon)^{1/\epsilon}),$$

$$p_i(\epsilon) = \left(\frac{1}{2} \left(1 - \left(1 - \frac{\epsilon}{2^i}\right)^{2^i/\epsilon}\right)\right)^{2^{(i-1)}} \quad (i \geq 1).$$

Proof: The proof is by mathematical induction and shown in Appendix B.

From the lemma 15 one can says that even though the scheme in [6] and our scheme deal with different signer structures, the results of security analysis are same in both schemes.

4.5 Security of the Proposed Multisignature Scheme

Since lemma 10 and the analysis described in the previous subsection, security of our scheme is proven as follows.

Theorem 16 If finding a secret key x_i from a public key y_i is $(t(N), \epsilon(N))$ -secure, then the proposed multisignature scheme is $(t, l_{sig}, l_{H_1}, \dots, l_{H_N}, \epsilon)$ -secure, where

$$t(N) = (t + \phi_1 + \phi_3) \frac{2^{(2N+1)} + 1}{3\epsilon_3} + \phi_2$$

$$= (t + \phi_1 + \phi_3) \frac{2^{(2N+1)} + 1}{3(\epsilon_2 - \frac{l_{sig}}{l})} + \phi_2,$$

$$\epsilon(N) = \prod_{i=0}^N p_i(\epsilon_3).$$

Here, ϕ_1 is the verification time of the identification protocol, ϕ_2 is the calculate time of x in the final step, ϕ_3 is the simulation time of l_{sig} signatures. And,

$$\begin{aligned} p_0(\epsilon_3) &= (1 - (1 - \epsilon_3)^{1/\epsilon_3}) \\ &= (1 - (1 - (\epsilon_2 - \frac{l_{sig}}{l})^{1/\epsilon_3}))^{1/\epsilon_3}, \\ p_i(\epsilon_3) &= (\frac{1}{2}(1 - (1 - \frac{\epsilon_3}{2^i})^{2^i/\epsilon_3}))^{2^{(i-1)}} \quad (i \geq 1) \\ &= (\frac{1}{2}(1 - (1 - \frac{\epsilon_2 - \frac{l_{sig}}{l}}{2^i})^{2^i/\epsilon_3}))^{2^{(i-1)}}, \end{aligned}$$

where $\epsilon_3 = \epsilon_2 - \frac{l_{sig}}{l}$, ϵ_2 is based on ϵ_{H_i} , $\epsilon_{H_0} = \epsilon$, $\epsilon_{H_i} = \frac{\epsilon_{H_{i-1}} - \frac{1}{l}}{H_i}$ from Reduction Lemma of Multisignature.

4.6 Security of the Signing Order

We consider the security of the signing order of our scheme arising from non-commutativity of multiplication. Assume that $\sigma_{\tilde{A}B}(= \sigma_A \odot \sigma_B)$ is a valid multisignature that is generated by legitimate signers U_A and U_B for a message M and the signing order \mathbb{D}_i . Then, another multisignature $\sigma_{\tilde{B}A}(= \sigma_B \odot \sigma_A)$ for another signing order \mathbb{D}'_i are rejected with respect to the verification of the signing order \mathbb{D}_i with overwhelming probability.

Theorem 17 For a group of two signers, the proposed structured multisignature scheme resists against a signature forgery associated with the signing order.

Proof: Since the equation (1), assume that the following equation holds.

$$\begin{pmatrix} u_{A,1} \cdot U_{B,1} & g^{U_{B,3} \cdot v_A + u_{A,1} \cdot v_B} \\ 0 & u_{A,3} \cdot U_{B,3} \end{pmatrix} \equiv \begin{pmatrix} u_{A,1} \cdot U_{B,1} & (y_A \cdot u_{A,2}^{H_A(M)})^{U_{B,3}} \cdot (y_B \cdot U_{B,2}^{H_B(M)})^{u_{A,1}} \\ 0 & u_{A,3} \cdot U_{B,3} \end{pmatrix}.$$

Since the element (1, 2), $U_{B,3} \cdot v_A + u_{A,1} \cdot v_B = (x_A + r_{A,2}H_A(M))U_{B,3} + (x_B + r_B H_B(M))u_{A,1}$. Here, let $Z = U_{B,3} \cdot v_A + u_{A,1} \cdot v_B$, $X = (x_A + r_{A,2}H_A(M))U_{B,3}$ where assume that $X \neq 0$, and $Y = (x_B + r_B H_B(M))u_{A,1}$. For all $z \in \mathbb{Z}_l$, the probability of $Z = z$ is given as follows.

$$\begin{aligned} \Pr[Z = z] &= \Pr[(X \neq 0) \& (Y = Z - X)] \\ &= (1 - \Pr[X = 0]) \cdot (\Pr[Y = Z - X]) = (1 - \frac{1}{l}) \cdot \frac{1}{l} \end{aligned}$$

Here, $(1 - \frac{1}{l})$ is overwhelming probability since $\frac{1}{l}$ is negligible. Therefore, the probability is $\frac{1}{l}$. Thus,

$$\begin{aligned} \Pr[\sigma_{\tilde{B}A} \text{ is accepted with } \mathbb{D}_i | \sigma_{\tilde{A}B} \text{ is accepted with } \mathbb{D}_i] &\leq \frac{1}{l}. \\ \therefore \Pr[\sigma_{\tilde{B}A} \text{ is rejected with } \mathbb{D}_i | \sigma_{\tilde{A}B} \text{ is accepted with } \mathbb{D}_i] &\geq 1 - \frac{1}{l} \end{aligned}$$

Since $\frac{1}{t}$ is negligible, the probability is overwhelming. Thus, it is hard to change the signing order in our scheme.

5 Efficiency of the Proposed Scheme

We compare the proposed scheme with DLP-based schemes in [4,7,8,9,12] and a primitive scheme [10] with respect to the signature size and the computational cost for signature generation and verification. For the signature generation and verification cost, we evaluate the number of modulo- p multiplications. Here we adopt a primitive arithmetic of binary methods in [1] for powering operation. We set p as 512 bits and q as 160 bits.

Table 1. Performance evaluation for t signers

	# of multiplication (mod p)		Signature size (bit)
	U_i 's signature generation cost	Verification cost	
Primitive Scheme	211	$380t$	$320t$
Scheme [4]	210	$380t$	$512t+160$
Scheme [7]	380	380	672
Scheme [8]	210	$380t$	$512t+160$
Scheme [9]	230	$200(4t+1)$	$512(t+1)$
Scheme [12]	210	$400t$	$160(t+1)$
Our Scheme	230	$200(3t+1)$	$512(t+1)$

Table 1 shows the result for t signers. The signature size in the proposed scheme is larger than other schemes except the scheme in [9]. However, The signature generation cost is equal between our scheme and the schemes in [9], and the signature verification cost is reduced in our scheme as compared with the scheme in [9]. Furthermore, our scheme has order-flexibility [12] of the signing order among signers with same rank as the schemes in [8,12], and only our scheme is based on an algebraic structure of underlying algebraic operation except the scheme in [9].

6 Conclusion

We have proposed a structured multisignature scheme by utilizing a non-commutative ring homomorphism, which is more comprehensive in terms of the representation of the signers' group structure than the scheme in [9], and discussed its security about adaptive chosen message insider attack. Finally, we evaluated performance cost of our scheme. We plan to study the security against stronger attack model and improve the efficiency as a future work.

References

1. Donald Ervin Knuth, "The Art of Computer Programming 3rd ed, Vol.2, Seminumerical Algorithms ", Addison-Wesley, 1998.

2. Eikoh Chida, Hiroki Shizuya, Takao Nishizeki, "One-Way Functions over Finite Near-Rings", IEICE TRANS. FUNDAMENTALS, VOL.E78-A, NO.1, pp1-6, JANUARY 1995.
3. Eikoh Chida, Takao Nishizeki, Motoji Ohmori and Hiroki Shizuya, "On the One-Way Algebraic Homomorphism", IEICE TRANS. FUNDAMENTALS, Vol.E79-A, No.1, pp.1-8, JANUARY 1996.
4. Hiroshi Doi, Masahiro Mambo and Eiji Okamoto, "On the Security of the RSA-Based Multisignature Scheme for Various Group Structures ", Proc. ACISP2000, Lecture Notes in Computer Science 1841, pp.352-367, Springer-Verlag, 2000.
5. Kazuharu Itakura, Katsuhiko Nakamura, "A Public-key Cryptosystem Suitable for Digital Multi-signatures", Transactions of Information Processing Society of Japan, Vol.24, No.4, pp.474-480, JULY 1983.
6. Kazuo Ohta, Tatsuaki Okamoto, "Multi-Signature Schemes Secure against Active Insider Attacks", IEICE TRANS. FUNDAMENTALS, VOL.82-A, No.1, pp21-31, JANUARY 1999.
7. Mike Burmester, Yvo Desmedt, Hiroshi Doi, Masahiro Mambo, Eiji Okamoto, Mitsuru Tada, and Yuko Yoshifuji, "A structured ElGamal-type multisignature scheme", Proc. PKC2000, Lecture Notes in Computer Science 1751, pp.466-483, Springer-Verlag, 2000.
8. Mitsuru Tada, "A Secure Multisignature Scheme with Signing Order Verifiability", IEICE TRANS. FUNDAMENTALS, VOL.E86-A, No.1, pp.73-88, JANUARY 2003.
9. Motoji Ohmori, Eikoh Chida, Hiroki Shizuya, Takao Nishizeki, "A Note on the Multisignature over a Non-commutative Ring", TECHNICAL REPORT OF IEICE. IT95-50, ISEC95-45, SST95-111, pp1-6, MARCH 1996.
10. National Institute for Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB XX, draft, 1993.
11. P. Ribenboim, "The Book of Prime Number Records", Springer-Verlag, New York, 1988.
12. Shirow Mitomi, Atsuko Miyaji, "A Multisignature Scheme with Message Flexibility, Order Flexibility and Order Verifiability", Proc. ACISP 2000, Lecture Notes in Computer Science 1841, pp.298-312, Springer-Verlag, 2000.
13. Tatsuaki Okamoto, "A digital Multisignature Scheme Using Bijective Public-key Cryptosystems", ACM Trans. on Computer Systems, Vol.6, No.8, pp.432-441, 1988.

Appendix A: Proof of Lemma 14

Assume that A can break a multi-round identification scheme with (t, ϵ) . We construct a forger F which calculate a secret key $x(= x_1 + x_2)$ of two pieces of public key y_1 and y_2 with (t', ϵ') by using A . First, we consider the following probing steps of \mathcal{H} to find 1's along the rows in \mathcal{H} .

1. Probe random entries in \mathcal{H} to find an entry $a^{(0)}$ with 1. Here, we denote the rows where $a^{(0)}$ is located in \mathcal{H}_1 by $\mathcal{H}_1^{(0)}$ and in \mathcal{H}_2 by $\mathcal{H}_2^{(0)}$.
2. After $a^{(0)}$ is found, probe random entries along $\mathcal{H}_1^{(0)}$ to find another entry $a^{(1)}$ with 1. Here, we denote the rows where $a^{(1)}$ is located in \mathcal{H}_2 by $\mathcal{H}_2^{(1)}$.
3. After $a^{(0)}$ is found, probe random entries along $\mathcal{H}_2^{(0)}$ to find another entry $a^{(2)}$ with 1.

4. After $a^{(1)}$ is found, probe random entries along $\mathcal{H}_2^{(1)}$ to find another entry $a^{(3)}$ with 1.

Let p_1 be the success probability of step 1 with $\frac{1}{\epsilon}$ iteration. Since the fraction of 1's along \mathcal{H} , $p_1 \geq (1 - (1 - \epsilon)^{1/\epsilon})$. Let p_2 be the success probability of step 2 with $\frac{2}{\epsilon}$ iteration. Since the probability that $\mathcal{H}_1^{(0)}$ is heavy is at least $\frac{1}{2}$ by hierarchical heavy row lemma and the fraction of 1's along a heavy row is at least $\frac{\epsilon}{2}$, $p_2 \geq \frac{1}{2}(1 - (1 - \frac{\epsilon}{2})^{2/\epsilon})$. Let p_3 be the success probability of step 3 with $\frac{4}{\epsilon}$ iteration. Since the probability that $\mathcal{H}_2^{(0)}$ is heavy is at least $\frac{1}{2}$ by hierarchical heavy row lemma and the fraction of 1's along a heavy row is at least $\frac{\epsilon}{4}$, $p_3 \geq \frac{1}{2}(1 - (1 - \frac{\epsilon}{4})^{4/\epsilon})$. Let p_4 be the success probability of step 4 with $\frac{4}{\epsilon}$ iteration. Since the probability that $\mathcal{H}_2^{(1)}$ is heavy is at least $\frac{1}{2}$ by hierarchical heavy row lemma and the fraction of 1's along a heavy row is at least $\frac{\epsilon}{4}$, $p_4 \geq \frac{1}{2}(1 - (1 - \frac{\epsilon}{4})^{4/\epsilon})$.

Let $a^{(k)}$ be represented by $(u_{i_j}^{(k)}, d_i^{(k)}, y_i^{(k)})$. Since $a^{(k)}$ is an entry with 1, the following equation holds.

$$\tilde{\sigma}_2 \equiv \begin{pmatrix} u_{1,1} & y_1 \cdot u_{1,2}^{d_1} \\ 0 & u_{1,3} \end{pmatrix} * \begin{pmatrix} u_{2,1} & y_2 \cdot u_{2,2}^{d_2} \\ 0 & u_{2,3} \end{pmatrix}.$$

In addition,

$$\begin{pmatrix} u_{1,1} + u_{2,1} & g^{v_1 + v_2} \\ 0 & u_{1,3} + u_{2,3} \end{pmatrix} \equiv \begin{pmatrix} u_{1,1} + u_{2,1} & y_1 \cdot u_{1,2}^{d_1} \cdot y_2 \cdot u_{2,2}^{d_2} \\ 0 & u_{1,3} + u_{2,3} \end{pmatrix}.$$

In multiplication,

$$\begin{pmatrix} u_{1,1} \cdot u_{2,1} & g^{u_{2,3} \cdot v_1 + u_{1,1} \cdot v_2} \\ 0 & u_{1,3} \cdot u_{2,3} \end{pmatrix} \equiv \begin{pmatrix} u_{1,1} \cdot u_{2,1} & (y_1 \cdot u_{1,2}^{d_1})^{u_{2,3}} \cdot (y_2 \cdot u_{2,2}^{d_2})^{u_{1,1}} \\ 0 & u_{1,3} \cdot u_{2,3} \end{pmatrix}.$$

Since the element (1,2), $g^{v_1^{(k)} + v_2^{(k)}} = y_1 \cdot u_{1,2}^{(k)d_1^{(k)}} \cdot y_2 \cdot u_{2,2}^{(k)d_2^{(k)}}$ holds in addition and $g^{u_{2,3}^{(k)} \cdot v_1^{(k)} + u_{1,1}^{(k)} \cdot v_2^{(k)}} = (y_1 \cdot u_{1,2}^{(k)d_1^{(k)}})^{u_{2,3}^{(k)}} \cdot (y_2 \cdot u_{2,2}^{(k)d_2^{(k)}})^{u_{1,1}^{(k)}}$ holds in multiplication, respectively. Here, we assume that $u_{1,1}^{(0)} = u_{1,1}^{(1)} = u_{1,1}^{(2)} = u_{1,1}^{(3)} = u_{1,1}$ and $u_{2,3}^{(0)} = u_{2,3}^{(1)} = u_{2,3}^{(2)} = u_{2,3}^{(3)} = u_{2,3}$ by using the same random tape. 1's in the rows of $\mathcal{H}_1^{(0)}$, $\mathcal{H}_2^{(0)}$, and $\mathcal{H}_2^{(1)}$ give four equations and five unknown variables $x_1, x_2, r_{1,2}^{(0)}, r_{2,2}^{(0)}, r_{2,2}^{(1)}$. Here, x_1 and x_2 do not appear separately, but $x = x_1 + x_2 \pmod{l}$ in addition and $x = u_{2,3}x_1 + u_{1,1}x_2 \pmod{l}$ in multiplication, respectively. Thus, secret key x can be calculated as follows.

$$\text{In addition, } x = v_1^{(0)} + v_2^{(0)} - r_{1,2}^{(0)}d_1^{(0)} - r_{2,2}^{(0)}d_2^{(0)}.$$

$$\text{Here, } r_{1,2}^{(0)} = \frac{v_1^{(0)} + v_2^{(0)} - v_1^{(1)} - v_2^{(1)} - r_{2,2}^{(0)}d_2^{(0)} + r_{2,2}^{(1)}d_2^{(1)}}{d_1^{(0)} - d_1^{(1)}},$$

$$r_{2,2}^{(0)} = \frac{v_1^{(0)} + v_2^{(0)} - v_1^{(2)} - v_2^{(2)}}{d_2^{(0)} - d_2^{(2)}},$$

$$r_{2,2}^{(1)} = \frac{v_1^{(1)} + v_2^{(1)} - v_1^{(3)} - v_2^{(3)}}{d_2^{(1)} - d_2^{(3)}}.$$

In multiplication, $x = u_{2,3}(v_1^{(0)} - r_{1,2}^{(0)}d_1^{(0)}) + u_{1,1}(v_2^{(0)} - r_{2,2}^{(0)}d_2^{(0)})$.

$$\begin{aligned} \text{Here, } r_{1,2}^{(0)} &= \frac{u_{2,3}(v_1^{(0)} - v_1^{(1)}) + u_{1,1}(v_2^{(0)} - v_2^{(1)}) - u_{1,1}(r_{2,2}^{(0)}d_2^{(0)} - r_{2,2}^{(1)}d_2^{(1)})}{u_{2,3}(d_1^{(0)} - d_1^{(1)})}, \\ r_{2,2}^{(0)} &= \frac{u_{2,3}(v_1^{(0)} - v_1^{(2)}) + u_{1,1}(v_2^{(0)} - v_2^{(2)})}{u_{1,1}(d_2^{(0)} - d_2^{(2)})}, \\ r_{2,2}^{(1)} &= \frac{u_{2,3}(v_1^{(1)} - v_1^{(3)}) + u_{1,1}(v_2^{(1)} - v_2^{(3)})}{u_{1,1}(d_2^{(1)} - d_2^{(3)})}. \end{aligned}$$

Thus, t' and ϵ' are obtained as follows.

$$\begin{aligned} t' &= (t + \phi_1) \times \left(\frac{1}{\epsilon} + \frac{2}{\epsilon} + \frac{4}{\epsilon} + \frac{4}{\epsilon} \right) \\ &= (t + \phi_1) \frac{11}{\epsilon} \\ \epsilon' &= p_1 p_2 p_3 p_4 \\ &\geq ((1 - (1 - \epsilon)^{1/\epsilon})) \left(\frac{1}{2} (1 - (1 - \frac{\epsilon}{2})^{2/\epsilon}) \right) \left(\frac{1}{2} (1 - (1 - \frac{\epsilon}{4})^{4/\epsilon}) \right) \left(\frac{1}{2} (1 - (1 - \frac{\epsilon}{4})^{4/\epsilon}) \right) \\ &= \frac{1}{8} ((1 - (1 - \epsilon)^{1/\epsilon})) \left((1 - (1 - \frac{\epsilon}{2})^{2/\epsilon}) \right) \left(\frac{1}{2} (1 - (1 - \frac{\epsilon}{4})^{4/\epsilon}) \right)^2 \end{aligned}$$

Appendix B: Proof of Lemma 15

For $N = 2$, Lemma 14 is satisfied. For $N \geq 3$, assume that $t(N) = (t + \phi_1) \frac{1}{\epsilon} (1 + \sum_{i=1}^N 2^{2i-1}) + \phi_2 = (t + \phi_1) \frac{2^{(2N+1)+1}}{3\epsilon} + \phi_2$ holds because of Hierarchical Heavy Row Lemma. Here, the required time for \mathcal{H}_i is $(t + \phi_1) \frac{1}{\epsilon} 2^{2i-1}$ for all i . Then consider $t(N + 1)$.

$$\begin{aligned} t(N + 1) &= (t + \phi_1) \frac{1}{\epsilon} \left(1 + \sum_{i=1}^N 2^{2i-1} \right) + \phi_2 + \frac{t + \phi_1}{\epsilon} 2^{2(N+1)-1} \\ &= (t + \phi_1) \frac{1}{\epsilon} \left(1 + \sum_{i=1}^N 2^{2i-1} + 2^{2(N+1)-1} \right) + \phi_2 \\ &= (t + \phi_1) \frac{1}{\epsilon} \left(\frac{2^{(2N+1)} + 1}{3} + 2^{2N+1} \right) + \phi_2 \\ &= (t + \phi_1) \frac{1}{3\epsilon} (2^{(2N+1)} + 1 + 3 \cdot 2^{2N+1}) + \phi_2 \\ &= (t + \phi_1) \frac{1}{3\epsilon} (2^{(2N+3)} + 1) + \phi_2 \\ &= (t + \phi_1) \frac{1}{3\epsilon} (2^{2(N+1)+1} + 1) + \phi_2 \end{aligned}$$

Thus, the equation $t(N)$ holds for all integer $N > 1$. Similarly, assume that $\epsilon(N) = \prod_{i=0}^N p_i(\epsilon)$ holds. Then consider $\epsilon(N + 1)$.

$$\begin{aligned} \epsilon(N + 1) &= \prod_{i=0}^N p_i(\epsilon) \times \left(\frac{1}{2} \left(1 - \left(1 - \frac{\epsilon}{2^{i+1}} \right)^{2^{i+1}/\epsilon} \right) \right)^{2^{(i)}} \\ &= \prod_{i=0}^{N+1} p_i(\epsilon) \end{aligned}$$

Thus, the equation $\epsilon(N)$ holds for all integer $N > 1$.