コンピュータセキュリティ 14－9
(2001. 7. 25)

意思付多重署名方式についての研究

河内 恵 多田 充 宮地 充子

北陸先端科学技術大学院大学 情報科学研究科
〒923-1292 石川県 能美郡 辰口町 旭台 1-1
TEL: 0761-51-1405
FAX: 0761-51-1405
E-mail: {kei-k, mt, miyaji}@jaist.ac.jp

あらまし ：署名者の意思を反映する事ができ，しかも効率的で安全性の証明も可能な意思付多重署名方式を提案する．署名者の意思とは，各署名者が文書に署名をする際，新たに付加して送ることのできるある種の情報である．しかし現在までに，効率性を悪化させることなく新たな情報を付加することのできる多重署名方式は未だ提案されていない．まず，既存の多重署名モデルを利用しこの概念を実現する方式をPrimitiveモデルと呼び，その後，署名サイズや検証コストにおいてPrimitiveモデルよりも優れた方式を意思付提案意思付多重署名モデルとして提案する．この意思付多重署名方式のベースとなる意思付複数ラウンド認証方式が健全性とゼロ知識性を兼ね備えているならば，安全性を証明することができる．

キーワード ：多重署名方式, 署名者の意思, ID reduction

Study of multi-signature schemes with signers' intentions

Kei KAWAUCHI Mitsuru TADA Atsuko MIYAJI

School of Information Science,
Japan Advanced Institute of Science and Technology (JAIST)
1-1, Asahidai, Tatsunokuchi, Nomi, Ishikawa, 923-1292, JAPAN
TEL: +81-761-51-1405
FAX: +81-761-51-1405
E-mail: {kei-k, mt, miyaji}@jaist.ac.jp

Abstract : In this paper, we propose multisignature schemes, in which each signer can express her *intention* associating with the message to be signed, moreover, proposed scheme is efficiency and provable security. 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 multisignature scheme dealing with signers' intentions without loss of efficiency. First, we consider a multisignature scheme realizing the concept of signers' intentions by utilizing existing models, and name it *Primitive model*. After that, we introduce our multisignature model with siners' intentions which is more efficient in view of the computational cost for verification and in view of the signature size than primitive model. A multisignature scheme with signers' intentions derived from our model is shown to be provably secure if the multi-round identification schemes with signers' intentions is based, provides soundness and zero-knowledge property.

Key words : multi-signature, signer's intention, ID reduction technique

1 Introduction

多重署名方式とは複数の署名者が参加する場合に，署名サイズや検証式の計算コストにおいて効率的に取り扱うことができるという特徴を持つ．そのため以下のような状況下において，多重署名方式は非常に有効であるといえる．

- 大学の構内にて，クラブやサークルのメンバーに対し，イベント開催の情報を伝えるポスターをよく目にすることが，そのポスターにはメンバーに対し”イベントに参加する場合は名前を書いておいて欲しい”との要求が出されているとしよう．

今，我々がそのイベントをまとめあげる幹事であったと仮定しよう．そのポスターにはメンバーの名前だけしか書かれていないので，幹事は，その名前を書いた人のみ”参加の意思”を表しているもと判断する．しかし，名前を書いていないメンバーが，イベントに参加したくないのか? それともそのポスターの存在に気が付いていない為に名前がないのか? を幹事は判断することができない．そのような曖昧が発生しないためにも，幹事はこのようにポスターを変更するであろう．”メンバーは全員，自分の名前とともに参加意思の有無も記入するように!”と．

各署名者の署名と，その署名者の意思を反映することのできる機能付多重署名方式は未だ提案されていない．そこで署名者の意思を表すための1つ目の提案としては，それぞれの署名者に対し2つの公開鍵を与えてしまうという解決法が挙げられる．1つの公開鍵が Yes という意思を表し，もう一方の公開鍵が No という意思を表すのである．しかし各署名者にとっては意思の数だけの公開鍵が必要となるため鍵管理を難しくするだけに良き解決法とはいえない．2つ目の提案としては，幹事が事前に Yes と No を表す2つの文書を用意し，各署名者は自分の意思を表す方の文書に対して多重署名を行い意思を表現するという方法も考えられる．この方法であると各署名者の意思は Yes と No の2種類しかないが，一般化して考えると，署名者は集合 $\boldsymbol{I} := \{I_1, \ldots, I_N\}$ $(N \geq 2)$ の中から自らのとりうる意思の種類を選んでくることとなり，各署名者 P_i のとりうる意思は $\alpha_\ell = I_\ell (\ell \in [1, N])$ と表すことができる．(例えば，意思のとりうる種類が Yes と No の場合，I_1, I_2 と表せられる．) このように複数の意思の種類数だけの文書が生成され，その結果，複数の多重署名が作られるような解決法を Primitive モデルと呼ぶことにする．

3つ目の提案としては，鍵管理が1つだけで済み，各署名者の意思を反映した文書に対して多重署名を生成することのできる多重署名モデルを提案する．意思のとりうる種類の数を N 個とすれば　第1の解決法において各署名者は N 個の鍵管理が必要となり，第2の解決法，Primitive モデルにおいては，署名サイズも検証コストも N 倍かかることとなる．一方，我々の提案モデルは，署名サイズは N から独立し，その結果検証コストも Primitive モデルに比べて小さくなる．従って，我々の提案モデルから引き出される意思付多重署名方式は上記のような解決法に比べ非常に効率的であると言える．

提案モデルの安全性を証明するための便宜上，2つの意思付複数ラウンド認証方式を考える．これらの認証方式各々を ID-A, ID-B と呼ぶ．意思付多重署名の安全性の証明が ID-A と ID-B に帰着することができる．具体的に述べると，もし ID-A が健全性を持ち，ID-B がゼロ知識性を持っているならば，[4] による ID 帰着のテクニックによって，意思付多重署名方式は適応的選択文書内部文書攻撃に対しても安全であるということが証明できる．

関連する研究分野としては，[4], [6] において様々な種類の多重署名方式を見ることができる．署名者の署名順序の検証を保障できる方式としては [2] があり，文書を柔軟に取り扱え，かつ署名順序の保障している方式としては [3] が挙げられる．

2 Preliminaries

まず最初に我々がこの論文中にて使用する表記と記号についての定義を行う．n組の$(a_1,\ldots,a_n)$をボールド体の文字を使用して$\boldsymbol{a}$と表す．n組の$\boldsymbol{a}(=(a_1,\ldots,a_n))$と整数$i\in[1,n]$を用いて，$i$組の$(a_1,\ldots,a_i)$を$\boldsymbol{a}_{[i]}$と表す．また$k$組の$(a_1,\ldots,a_k)$と$\ell$組の$(b_1,\ldots,b_\ell)$を用いて$(a_1,\ldots,a_k)\oplus(b_1,\ldots,b_\ell)$が表しているものはそれら2つの連結であり，$(k+\ell)$組の$(a_1,\ldots,a_k,b_1,\ldots,b_\ell)$でもある．

多重署名モデル　多重署名とは，同一の文書mに対して，複数(n人)の署名者が署名を施す署名方式である．しかしそれは，普通の(1人の署名者による)単独署名方式をn回適用することでも実現できるので，一般的に署名サイズがLとなる単独署名方式を多重署名方式に拡張する場合，その多重署名方式においてはn人の署名者による署名サイズはnLより小さくなければならない．多重署名方式においてn人の署名者$P_1,\ldots,P_n$が参加し，そして各署名者P_iは公開鍵pk_iを公開し，秘密鍵sk_iを保有するとともに公開ランダムオラクル関数[1] $f_i:\{0,1\}^*\to\mathcal{E}$を持つ．$\boldsymbol{P}$は集合$\{P_1,\ldots,P_n\}$を表し，以下に一般化したgenericな多重署名方式のモデルを示す．

Model.1 (多重署名モデル)

鍵生成： 各署名者P_iは鍵生成アルゴリズム$\mathcal{G}$に1^kを入力して，公開鍵と秘密鍵のペア(pk_i,sk_i)を生成する．ここで$\boldsymbol{pk}$は$\{pk_1,\ldots,pk_n\}$を表す．

署名生成： 署名者の集合$\boldsymbol{P}$が文書mに対して多重署名を施すと仮定する．各$i\in[1,n]$は次の手続きを実行する．

- P_iはP_{i-1}から$(\boldsymbol{x}_{[i-1]},y_{i-1})$と$m$を受け取り，$x_i:=\mathtt{Cmt}(r_i,sk_i)$，$e_i:=f_i(\boldsymbol{x}_{[i]},m)$，$y_i:=\mathtt{Sig}(sk_i,r_i,e_i,y_{i-1})$を計算する．そして$(\boldsymbol{x}_{[i]},y_i)$と$m$を$P_{i+1}$に送る．ここで$\mathtt{Cmt}$と$\mathtt{Sig}$は多項式時間で計算可能な関数である．もちろん$P_{n+1}$は検証者$V$である．

検証： 検証者Vは，受け取ったmと$(\boldsymbol{x},y_n)$から$i\in[1,n]$について$e_i:=f_i(\boldsymbol{x}_{[i]},m)$を計算し，そして$v:=\mathtt{Ver}(\boldsymbol{pk},m,\boldsymbol{x},\boldsymbol{e},y_n$により検証を行う．$\mathtt{Ver}$も多項式時間で計算可能な関数で値域は$\{0,1\}$であるとする．もしに$V$が多重署名を受け入れたときは$v=1$であり，$v=0$の時は拒絶したときを表す．

3 Primitive モデル

1章にて意思付多重署名方式が求められるような状況の一例を示した．本章ではgenericな多重署名方式に基づいて，意思付多重署名を実現するPrimitiveモデルについて説明する．実現する方法としては，同種の意思をもった署名者によって一つずつの多重署名が作られ，結果として意思の種類数だけ多重署名が行われることになる．以下に一般化したモデルを示す．

Model.2 (Primitive モデル) 各署名者P_iは文書mに対して，それぞれの意思α_iを自らの意思として表したいと仮定する．それぞれの意思のとりうる範囲は集合$\boldsymbol{I}:=\{I_1,\ldots,I_N\}$の中からである．$\ell\in[1,N]$において，$m_\ell$は意思$I_\ell$を含んだ文書$m$に対応している．

鍵生成： Model.1と同様に生成する．

署名生成： 署名者の集合$\boldsymbol{P}$が意思付文書$\{m_\ell\}$に対して多重署名を施すと仮定し，$y_0^{(I_1)},\ldots,y_0^{(I_N)}$の初期値を与えられているとする．各$i\in[1,n]$は次の手続きを実行する．

- P_i は P_{i-1} から $(\boldsymbol{x}_{[i-1]}, y_{i-1}^{(I_1)}, \ldots, y_{i-1}^{(I_N)})$, $\{m_\ell\}$ と $\boldsymbol{\alpha}_{[i-1]}$ を受け取る．P_i は自分の意思を $\alpha_i \in \boldsymbol{I}$ から選ぶ．ここで $\alpha_i = I_\ell$ である．P_i は乱数 r_i を用いて $x_i := \mathtt{Cmt}(r_i, sk_i)$，$f_i$ を用いて $e_i := f_i(\boldsymbol{x}_{[i]}^{(I_\ell)}, m_\ell)$，そして $y_i^{(I_\ell)} := \mathtt{Sig}(sk_i, r_i, e_i, y_{i-1}^{(I_\ell)})$ を計算する．ここで $\boldsymbol{x}_{[i]}^{(I_\ell)}$ は $\oplus_{j\le i, \alpha_j \le I_\ell}(x_j)$ と定義する．全ての $I_{\ell'} \in \boldsymbol{I}\backslash\{I_\ell\}$ について $y_i^{(I_{\ell'})} := y_{i-1}^{(I_{\ell'})}$ を行う．P_i は $(\boldsymbol{x}_{[i]}, y_i^{(I_1)}, \ldots, y_i^{(I_N)})$, $\{m_\ell\}$ と $\boldsymbol{\alpha}_{[i]}$ を P_{i+1} に送る．もちろん P_{n+1} は検証者 V である．

検証: 検証者 V は，受け取った $(\boldsymbol{x}, y_n^{(I_1)}, \ldots, y_n^{(I_N)})$, $\{m_\ell\}$ から $i \in [1,n]$ について $e_i := f_i(\boldsymbol{x}_{[i]}^{(I_\ell)}, m_\ell)$ を計算し，そして各 $\ell \in [1,N]$ について $v^{(I_\ell)} := \mathtt{Ver}(\boldsymbol{pk}^{(I_\ell)}, m_\ell, \boldsymbol{x}^{(I_\ell)}, \boldsymbol{e}^{(I_\ell)}, y_n^{(I_\ell)})$ により検証を行う．ここで $I_\ell \in \boldsymbol{I}$ 毎に，集合 $\boldsymbol{pk}^{(I_\ell)}$ は $\oplus_{\alpha_i = I_\ell}(pk_i)$ と定義される．$\boldsymbol{x}^{(I_\ell)}$ と $\boldsymbol{e}^{(I_\ell)}$ も $\boldsymbol{pk}^{(I_\ell)}$ と同様に定義できる．V が多重署名を受け入れたときは $v^{(I_\ell)} = 1$ $(\ell \in [1,N])$ であり，$v =^{(I_\ell)} 0$ の時は拒絶したときである．

Primitive モデルでは，従来の多重署名を意思毎に実現するので，総署名サイズは N 倍となり，多重署名の検証は N 回必要となる．

4 提案意思付多重署名モデル

前の章で議論した Primitive モデルを基礎とする多重署名方式は，意思の種類の数 N が増加してくると効率が極めて悪くなってしまう．しかし我々が提案する意思付多重署名モデルによって効率的な意思付多重署名方式を引き出すことができる．このモデルでは，署名サイズ N から独立している．

Model.3 (意思付多重署名モデル) 各署名者 P_i がメッセージ m に対して彼らの意思 α_i を要求していると仮定し，そして彼らの意思のとりうる集合を $\boldsymbol{I} := \{I_1, \ldots, I_N\}$ とする．

鍵生成： Model.1 と同様に生成する．

署名生成： 各 $i \in [1,n]$ は次の手続きを実行する．ここで $y_0 = 0$ の初期値を与えられているものとする．

- P_i は P_{i-1} から $(\boldsymbol{x}_{[i-1]}, y_{i-1})$，$m$ と $\boldsymbol{\alpha}_{[i-1]}$ を受け取ったのち自らの意思 $\alpha_i \in \boldsymbol{I}$ を選び，そして乱数 r_i を用いて $x_i := \mathtt{Cmt}(r_i, sk_i, \alpha_i)$，$e_i := f_i(\boldsymbol{x}_{[i]}, m, \boldsymbol{\alpha}_{[i]})$ と $y_i := \mathtt{Sig}(sk_i, r_i, e_i, \boldsymbol{\alpha}_{[i]}, y_{i-1})$ を計算する．そして $(\boldsymbol{x}_{[i]}, y_i)$，$m$ と $\boldsymbol{\alpha}_{[i]}$ を P_{i+1} に送る．もちろん P_{n+1} は検証者 V である．

検証： 検証者 V は，受け取った $(\boldsymbol{x}, y_n)$，m と $\boldsymbol{\alpha}$ から $i \in [1,n]$ について $e_i := f_i(\boldsymbol{x}_{[i]}, m, \boldsymbol{\alpha}_{[i]})$ を計算し，$v := \mathtt{Ver}(\boldsymbol{pk}, m, \boldsymbol{x}, \boldsymbol{e}, y_n, \boldsymbol{\alpha})$ により検証する．もし $v = 1$ となれば検証者は署名者の意思を受け入れ，それ以外は拒絶する．

このモデルから引き出される多重署名方式は，Primitive モデルを基礎とする多重署名方式に比べて総署名サイズを小さくすることができる．それ故に多重署名の検証の計算量のコストも小さくすることができる．

5 提案モデルから引き出される認証方式の安全性

提案モデルから引き出される意思付多重署名方式の安全性を議論するために，能動的攻撃者 $\mathcal{A}_\mathrm{a}$ を仮定する．$\mathcal{A}_\mathrm{a}$ はランダムオラクル関数 $f_1, \ldots, f_n$ にアクセスすることができる確率的な多項

式チューリングマシンで P_{i_j} $(i \in [1,n])$ を除く正当な署名者と共謀して $j \in [1,Q]$ 回目に P_{i_j} に $(m, \boldsymbol{x}_{[i_j-1]}, \boldsymbol{e}_{[i_j-1]}, y_{i_j-1}, \boldsymbol{\alpha}_{[i_j-1]})$ と α_i を送ることでの P_{i_j} の正当な意思付署名 $(m, \boldsymbol{x}_{[i_j]}, \boldsymbol{e}_{[i_j]}, y_{i_j}, \boldsymbol{\alpha}_{[i_j]})$ を得ることができる．攻撃モデルを強くするために，$\mathcal{A}_{\mathrm{a}}$ は $\mathcal{A}_{\mathrm{a}}$ の選んだ意思に対して P_{i_j} に署名を施してもらえるように頼むことができると仮定する．ここで Q とはセキュリティパラメーター k 上の多項式に拘束されているパラメーターである．一方，受動的攻撃者 $\mathcal{A}_{\mathrm{p}}$ はランダムオラクル関数 $f_1, \ldots, f_n$ にアクセスすることができる確率的チューリングマシンであり，公開されている情報のみを使用できるとする．

5.1 意思付複数ラウンド認証モデル

[4] によって与えられた多重署名方式の安全性は，多重署名方式から引き出される複数ラウンドの認証方式の安全性に帰着することができると示されている．その意味するところは，もし複数ラウンド認証方式がどんな多項式時間の攻撃者に対しても安全であるということが示せれば，ID 帰着補題によって，どんな適応的選択文書内部攻撃を行う多項式時間の攻撃者がいたとしても，署名の存在的偽造すらできないという，多重署名方式の安全性を示すことができる．我々の提案モデルから引き出された意思付多重署名方式の安全性は，数種類の複数ラウンド認証方式の安全性に帰着することができる．それを示す前に，まず 2 種類の複数ラウンド認証モデルを紹介する．これらはお互いわずかに異なっているだけで，我々の提案モデルから引き出される意思付多重署名方式の安全性を証明する際に必要なモデルである．

Model.4 (意思逐次公開型複数ラウンド認証モデル： ID-A)

鍵生成： 証明者 P は n 組の公開鍵と秘密鍵を $(pk_i, sk_i\ (i \in [1,n]))$ を生成する．ここで $\boldsymbol{pk}$ と $\boldsymbol{sk}$ はそれぞれ $\{pk_1, \ldots, pk_n\}$ と $\{sk_1, \ldots, sk_n\}$ を表す．

認証： 証明者 P と検証者 V は以下のやりとりを $i \in [1,n]$ 実行する．

- P は自分の意志 $\alpha_i \in \boldsymbol{I}$ を選び，そして乱数 r_i を用いてコミットメント $x_i := \mathtt{Cmt}(r_i, sk_i, \alpha_i)$ を計算し，x_i と α_i を V に送る．V はランダムに取り出したチャレンジ $e_i \in \mathcal{E}$ を P に送る．

P は返答 $y := \mathtt{Ans}(\boldsymbol{sk}, \boldsymbol{r}, \boldsymbol{e}, \boldsymbol{\alpha})$ を計算し V に送る．ここで Ans という関数は Sig と同一の働きをする．

検証： 受け取った $(\boldsymbol{x}, y)$ と $\boldsymbol{pk}, \boldsymbol{e}, \boldsymbol{\alpha}$ から，V は $v := \mathtt{Ver}(\boldsymbol{pk}, \boldsymbol{x}, \boldsymbol{e}, y, \boldsymbol{\alpha})$ を計算し，その時 $v = 1$ ならば検証者は受け入れ，それ以外は拒絶する．

Model.5 (意思事前公開型複数ラウンド認証モデル： ID-B)

鍵生成: Model.4 と同様に生成する．

意思表明： 証明者 P は $\boldsymbol{I}$ から $\alpha_1, \ldots, \alpha_n$ を選び出し (この分布は一様でなくても良い) そして $\boldsymbol{\alpha}$ を公開情報として公開する．

認証： 証明者 P と検証者 V は以下のやりとりを $i \in [1,n]$ 実行する．

- 乱数 r_i と事前に公開した意思の順序に基づいた $\alpha_i \in \boldsymbol{I}$ を用いて P はコミットメント $x_i := \mathtt{Cmt}(r_i, sk_i, \alpha_i)$ を計算し，x_i と α_i を V に送る．V はランダムに取り出したチャレンジ $e_i \in \mathcal{E}$ を P に送る．

P は返答 $y := \mathtt{Ans}(\boldsymbol{sk}, \boldsymbol{r}, \boldsymbol{e}, \boldsymbol{\alpha})$ を計算し V に送る．

検証： Model.4 と同様に検証する．

5.2 ID 帰着補題

もし，ID-A が健全性を持っていて，そして ID-B がゼロ知識性の性質を持っていたとき，提案モデルから引き出される意思付多重署名方式はどのような能動的攻撃者に対しても安全であると示すことができる．

補題 5.1 ID-B がゼロ知識性を持っていると仮定する．もし意思付多重署名方式において存在的偽造をすることのできる能動的攻撃者 $\mathcal{A}_{\mathrm{a}}$ が存在したならば，同じく意思付多重署名方式において存在的偽造をすることのできる受動的攻撃者 $\mathcal{A}_{\mathrm{p}}$ が存在する．

証明 (概要) ID-B がゼロ知識性を持っていると仮定していることから，秘密鍵 $\boldsymbol{sk}$ を知ることなく意思付多重署名方式をシミュレートすることのできる確率的な多項式シミュレーター $\mathcal{S}$ が存在する．そして $\mathcal{S}$ は，各秘密鍵 sk_i を持つ各々の正当な署名者 $\boldsymbol{P}$ の意思付署名と区別のできない意思付署名を作り出すことができる．つまり $\mathcal{S}$ は，正当な署名者 $\boldsymbol{P}$ の動きをそのままシミュレートできるということになる．すなわち能動的攻撃者 $\mathcal{A}_{\mathrm{a}}$ とシミュレーター $\mathcal{S}$ の 2 つから受動的攻撃者 $\mathcal{A}_{\mathrm{p}}$ を構成することができるのである．

補題 5.2 もし意思付多重署名方式において存在的偽造をすることのできる受動的攻撃者 $\mathcal{A}_{\mathrm{p}}$ が存在するならば，ID-A のモデルから引き出される複数ラウンドの意思逐次公開認証方式において 秘密鍵 $\boldsymbol{sk}$ を持たずとも検証者 V を騙すことができる多項式攻撃者 $\mathcal{A}_{\text{id-A}}$ が存在する．

証明 (概要) 以下に従って $\mathcal{A}_{\mathrm{p}}$ を使用することで $\mathcal{A}_{\text{id-A}}$ を構成することができる．$\mathcal{A}_{\text{id-A}}$ は公開鍵 $\boldsymbol{pk}$ を $\mathcal{A}_{\mathrm{p}}$ に渡し，各 $i \in [1,n]$ 回実行する．$\mathcal{A}_{\mathrm{p}}$ はランダムオラクル f_i に聞いているつもりで $\mathcal{A}_{\text{id-A}}$ に質問 $\mathcal{Q}_i = (x_i, m, \alpha_i)$ を与え，$\mathcal{A}_{\text{id-A}}$ は (x_i, α_i) を V へ送る．V から送られてきたチャレンジ e_i を，$\mathcal{A}_{\text{id-A}}$ は $\mathcal{Q}_i$ のハッシュ値として $\mathcal{A}_{\mathrm{p}}$ に送る．そして n 回のやりとりが終了した後，$\mathcal{A}_{\mathrm{p}}$ によって与えられた y を $\mathcal{A}_{\text{id-A}}$ は V へと送る．この y は意思 $\boldsymbol{\alpha}$ に関しての意思付多重署名方式の検証式を満たし，また意思 $\boldsymbol{\alpha}$ に関しての複数ラウンド意思逐次公開型認証方式の検証式も満たしている．

この補題 5.1，5.2 から以下の ID 帰着補題を得られる．

補題 5.3 ID-A が健全性を，ID-B がゼロ知識性を持っていたとき，提案モデルから引き出される意思付多重署名方式はいかなる能動的攻撃者に対しても安全であるといえる．

6 Conclusion

我々は，署名者の意思という概念を提案し，そして意思付多重署名方式のモデルを与えた．提案モデルから引き出される意思付多重署名方式の安全性を示すために，2 つの認証モデル ID-A と ID-B を提供した．そして，もし ID-A が健全性を，ID-B がゼロ知識性を持っているのならば，我々の提案モデルからの意思付多重署名方式はいかなる能動的多項式時間の攻撃者に対して安全であるということが判明する．そして，もし我々の提案モデルが sensitive な帰着を持っていると仮定するならば，[5] で紹介されている鍵生成過程も含んだ能動的な攻撃者に対して安全な意思付多重署名方式を作ることができるようになる．

参考文献

[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] 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.

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

[5] 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.

[6] 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.