様々な署名構造に適用可能な RSA 型多重署名方式

土井 洋[†1] 満保雅浩[†2] 岡本栄司[†3,†4]

複数の署名者が同一文書に署名を行う場合，それぞれの署名者の立場や責任は一般に同一ではなく，立場や責任の違いが署名生成の処理順序の違いに反映されることがある．そのため，誰が署名生成に関与したかを確認できるだけでなく，署名生成の処理順序が確認できることも重要となると考えられる．本論文では，様々な署名構造に適用可能な RSA 型多重署名方式を提案する．署名生成の処理順序が重要な意味を持つ直列構造と，逆に署名生成の処理順序が意味を持たない並列構造を基本的な署名構造とし，さらにそれらを組み合わせた複雑な構造を考察対象とする．まず，署名構造と署名者の秘密鍵から定まる構造識別子を定義し，各署名者が構造識別子を RSA 署名のべき乗演算の指数部において順次構築する多重署名方式を提案する．次に，提案方式への攻撃と RSA 署名への攻撃との帰着関係を調べることにより，提案方式の安全性を評価する．最後に，提案方式を変形することによる問題点や秘密鍵の効率的な生成法について述べる．

RSA-based Multisignature Scheme for Various Group Structures

Hiroshi Doi,[†1] Masahiro Mambo[†2] and Eiji Okamoto[†3,†4]

When more than one user sign a single message, each signer is in a different position in a signing group and has a different responsibility, and the signing order often reflects the difference of signer's position or responsibility. With this respect, verifying the signing order as well as the signer's name is very important. In this paper, we propose a RSA-based multisignature scheme for various group structures composed of serial and parallel signing order. First, we introduce a structured group identity, SGID, determined by the group structure and the secret keys. Next, we describe a multisignature scheme using SGID and give reductions for the security of the proposed scheme. We also discuss properties of the improved scheme.

1. はじめに

多重署名方式はディジタル署名方式の一種であり，同一のメッセージに対し複数の署名者が署名を行う．その多くは RSA 署名[14]を応用した方式であり，大きく 2 種類に分類される．1 つはすべての署名者が法 n を共有する方式[1),8)]であり，もう 1 つはすべての署名者が各々異なった法を使用する方式[13)]である．ほかにも ElGamal 署名[9)]を応用した多重署名方式[16)]もある．

現実社会では，同一書類に複数の署名を行う際の各署名者の立場や責任は異なり，署名生成の処理順序（以下，署名順序）が各署名者の立場の違いを反映している場合が多い．例として，**図 1** の組織を考える．この組織では，ユーザ A，B，C はユーザ D の部下としてグループ G に属する．A，B，C は同等の立場で仕事を行い，D はグループ G の管理責任者として A，B，C の仕事の内容に責任を持つ．このとき，G に属する全ユーザ A，B，C が書類に署名した後に，D が管理責任者として最後に書類に署名することが考えられる．これは，D が管理責任者として G の作業を監督したことを，G と D の署名順序により表現しているとも見なせる．よって，このような署名順序の違いを重視するセキュリティ・ポリシーを組織として採用した場合には，D が A，B，C よりも先に署名した書類は無効と見なし，同等の立場にある A，B，C が共同で生成した署名については，G 内での署名順序の違いにより意味が生じないようにすることが考えられる．

署名順序の重要性に注目すると，署名者グループの構造（以下，グループの構造）は大きく 2 つに分類できる．1 つは，G 内の各ユーザのように，署名順序が意味を持たない並列構造である．もう 1 つは，G と D の関係のように，署名順序が重要となる直列構造である．なお，グループの構造はグループに属するユーザ

†1 岡山大学理学部数学科
Department of Mathematics, Faculty of Science, Okayama University
†2 東北大学情報処理教育センター&情報科学研究科
Education Center for Information Processing and Graduate School of Information Sciences, Tohoku University
†3 ウィスコンシン大学暗号セキュリティセンター
Center for Cryptography, Computer and Network Security, University of Wisconsin, Milwaukee
†4 東邦大学理学部
Faculty of Science, Toho University

図 1 署名者の立場の違い
Fig. 1 Different position in a signing group.

の人数とグループ間の順序を規定する．最小のグループは 1 名のユーザのグループである．グループの構造に署名者を割り当てることにより，署名者の構造（以下，署名構造）が決まる．署名構造が分かれば，グループの構造，署名者の名前，さらには，グループの構造での署名者の割り当て方が判明する．

署名順序や署名構造については，一部の文献[2)~5)]を除いてあまり注意が払われていない．文献 3)~5) では RSA 署名を応用した方式が示されているが，安全性の評価は十分とはいえない．また，文献 4)，5) では ElGamal 型署名（DSA 署名[7]，Schnorr 署名[15)]）を応用した方式も示されているが，この方式では署名長の増加が問題となる．一方，文献 2) では変形 ElGamal 署名[16)]を応用した方式が示されており，署名長の増加もなく，安全性の証明もなされている．

本論文では，文献 3)~5) での考察を基に RSA 署名を応用した多重署名方式を提案し，安全性の評価を行う．提案する多重署名方式では，署名構造と署名者の秘密鍵から定まる構造識別子が重要な役割を果たし，各署名者がこの構造識別子を RSA 署名のべき乗演算の指数部において順次構築する．署名構造については，基本的な署名構造である直列構造と並列構造を組み合わせた，より複雑な署名構造を考察対象とする．文献 3)~5) では構造識別子の定義が曖昧であったのに対して，本論文では，直列構造と並列構造に対応する基本演算を用いて，構造識別子を帰納的に定義する．この厳密な定義により，安全性の評価に関する多くの証明を得られる．

以下，2 章では，本論文で使用する記号や署名順序に関する定義を行い，さらに安全性に関する仮定を示す．3 章では，構造識別子の定義を行い，その性質を記述する．4 章で様々な署名構造に適用可能な RSA 型多重署名方式を提案し，5 章で提案方式の安全性について評価する．6 章では，秘密鍵の簡略化や閾値署名[8)]の手法を適用する際の問題点を示す．7 章では，hash 関数を利用した秘密鍵の効率的な生成法[4),5)]について述べ，8 章で本論文をまとめる．

2. 定義と仮定

2.1 記　　号

署名者を $A, B, C, \ldots, U$ で表す．署名対象 M とは，メッセージを適切な hash 関数で変換した値である．識別子（以下，ID）とは，各ユーザ U が所有する 2 組の乱数であり，ユーザ U の識別子は小文字を用いて (u_1, u_2) と書く．この値がユーザの秘密情報である場合は，単に秘密鍵と呼ぶ．一方，公開情報の場合は (U_1, U_2) と大文字で記述する．署名構造の情報を ISG（Information of Structured Group），署名構造と ID から定まる構造識別子を SGID（Structured Group Identity）と書く．特定の ISG や SGID を意味する場合は，斜体に添字を付けて $ISG_S, ISG_1, \ldots$ や $SGID_S, SGID_1, \ldots$ と記述する．構造識別子 $SGID_S$ は，与えられた署名構造 ISG_S と ID 等，つまり $ISG_S, (u_1, u_2), \ldots$ から定まるので，$SGID(ISG_S, (u_1, u_2), \ldots)$ と記述することもある．

正整数 k に対して，$\mathbf{Z}_k$ や $\mathbf{Z}_k^*$ は $\mathbf{Z}_k = \{i \in \mathbf{Z} | 0 \leq i < k\}$，$\mathbf{Z}_k^* = \{i \in \mathbf{Z}_k | \gcd(i, k) = 1\}$ と定義される．また，計算機で扱える整数は有限であるため，ある正整数 K を用いた，$\mathbf{Z}_{\pm K} = \{i \in \mathbf{Z} | -K \leq i < K\}$ に属する整数を計算機で扱える整数とする．p，q を素数，n を 2 つの素数 p，q の積とする．なお，以後明記しない場合でも，n，p，q は RSA 署名の安全性のための様々な条件[12)]を満たすとする．$e \in \mathbf{Z}_{\phi(n)}^*$ を RSA 署名の公開鍵，$d \in \mathbf{Z}_{\phi(n)}^*$ を RSA 署名の秘密鍵とする．なお，$ed \equiv 1 \pmod{\phi(n)}$ である．

2.2 署名順序の概念

まず，本論文で提案する多重署名方式の概要を説明する．なお，その詳細は 4 章に記述する．

提案方式では，まず，最初の署名者 A が，署名対象 M に対する署名 S_A を計算する．この S_A を A の中間署名と呼ぶ．次に，2 番目の署名者 B が，M と中間署名 S_A を用いて，B の中間署名 S_B を出力する．以下，3 番目以降の署名者がこの作業を繰り返す．全署名者がこの手順に従うと，最終的な多重署名（以下，多重署名）S が出力される．

S から署名順序を確認できる安全な多重署名方式の構成が目標であるが，次の例のように，結託と署名順序には関連性があり，考察が必要である．

例 1 H を信頼のおける署名者とし，A，B が結託したとする．もし A，B が署名鍵を交換すれば，B，H，A の順に署名生成処理を行っても，H が署名順序 A，H，B 用の処理だと見なして署名生成を行う限り，署名順序 A，H，B の多重署名 S を偽造できる． [例終]

この例において，H が受け取った中間署名は，A の署名鍵を使って生成されており，本来の署名順序 A，H，B に従って生成された中間署名と一致する．この

ように，署名者が結託して秘密鍵を交換し，本来の署名順序に従って秘密鍵を使用すると，受理される多重署名を生成できる．全署名者が結託した場合には，同様の理由により署名順序は意味を持たなくなる．以上の考察を基に，署名順序を考慮した多重署名 S の正当性について定義する．

定義 1 M に対する，ある署名構造 ISG_1 での多重署名を S とする．S は，次の項目を満たすとき，正当であるという．なお，ISG_1 に属する H をプロトコルを順守する信頼のおける署名者とする．

(V1) ISG_1 に属する全署名者がプロトコルを順守した場合には，S が作成される．

(V2) H が M に対する署名生成に参加しない限り，M に対する ISG_1 での多重署名 S は生成されない．

(V3) S を作る際に H が受け取った中間署名は，本来の署名順序に従って生成された中間署名と同一である．ただし，結託者が存在する場合は，結託者間ではプロトコルが順守されているとは限らない． ■

本論文では，S の検証アルゴリズムを与え，S がその検査に合格した場合は，S が正当であることを証明する．3 章の議論から，署名構造や秘密鍵が異なるのに構造識別子が一致する確率は低いため，S に対する検証を行うことは，実質的に，鍵の使用順序を検証することになる．よって，署名検証者は少なくとも，「正当な署名者が存在すれば，その署名者が本来の署名順序に従った正しい中間署名に対して署名を行ったこと」を検証可能である．

さて，各署名者は署名生成処理以前に，署名を施す署名構造を何らかの形で知らなくてはならない．また，直前に署名したユーザの名前を確認できるか否かも安全性に関係する．すなわち，直前に署名したユーザの名前を確認できると，署名生成を行う署名構造との違いを発見でき，偽造を防ぐ手がかりになることがある．たとえば，例 1 において，H が B の名前を確認できれば，偽造は成功しない．

本論文では，強い攻撃モデルでの安全性を考察するため，特に言及しなければ，直前に位置するユーザ（攻撃者の場合も考えられる）が次の署名者に署名構造に関する情報を与えるとする．さらに，直前に署名したユーザの名前を確認できないものとする．なお，実際の運用上はその他の形態もありうる．

2.3 安全性に関する仮定

RSA 署名に関する安全性と，出力分布が一様となる乱数生成器の存在を以下のように仮定する．提案方式の安全性は，攻撃を関数として記述し，定義 2，3 に示す困難と仮定する問題との帰着関係を調べることにより評価する．本論文では，文献 2) と同様，平均的多項式時間 Turing 帰着可能であるときは $\leq_T^{ep}$ を，多項式時間真理値表帰着可能であるときは $\leq_{1-tt}^{p}$ を用いて関数の帰着関係を調べる．

定義 2 $\mathtt{RSAPhi}(e,n)$ を次の入出力を持つ関数と定義する．

入力 確認鍵 e と法 n.

出力 $e \in \mathbf{Z}^*_{\phi(n)}$ と $n \in \mathbf{N}_{>1}$ を満たす入力に対して，$a^m \equiv 1 \pmod n$ を満たす $m \in \mathbf{Z}_{\pm K}$ が存在すれば，m を出力する．ただし，a は $\mathbf{Z}^*_n$ の任意の元である． ■

定義 3 $\mathtt{RSASig}(M,e,n)$ を次の入出力を持つ関数と定義する．

入力 署名対象 M，確認鍵 e，および，法 n.

出力 $M \in \mathbf{Z}^*_n$，$e \in \mathbf{Z}^*_{\phi(n)}$，および，$n \in \mathbf{N}_{>1}$ を満たす入力に対して，$S^e \equiv M \pmod n$ を満たす $S \in \mathbf{Z}^*_n$ が存在すれば，S を出力する． ■

仮定 1 関数 RSAPhi，および，RSASig の計算を実行することは計算量的に困難である．なお，RSAPhi に関しては，文献 10) pp.94–95 を参照のこと． ■

仮定 2 任意の正整数 k に対して，出力範囲が $\mathbf{Z}_k$ で分布が一様となる乱数生成器が存在する． ■

3. 構造識別子

本章では，署名構造と ID から定まる構造識別子を定義する．署名順序を問わない署名者同士を 1 つのグループとすると，グループ内の順序には影響を受けないが，グループ単位で順序が異なると値が変わるように構造識別子を定義する．

3.1 構造識別子の定義

すべての構造識別子 SGID からなる集合を SGID 空間 Ω，すべての識別子 ID からなる集合を ID 空間 Λ とする．ID 空間が与えられたとき，SGID 空間を次のように定義する．

定義 4 $s \in \mathbf{Z}_{\phi(n)}$ と $\Lambda \subseteq \mathbf{Z}_{\phi(n)} \times \mathbf{Z}^*_{\phi(n)}$ が与えられたとき，SGID 空間 $\Omega \subseteq \mathbf{Z}_{\phi(n)}$ を以下のように帰納的に定義する．

(i) 任意の $(u_1,u_2) \in \Lambda$ に対して，$(s+u_1)u_2 \pmod{\phi(n)} \in \Omega$.

(ii) 任意の $x \in \Omega$，および，任意の $(u_1,u_2) \in \Lambda$ に対して，$(x+u_1)u_2 \pmod{\phi(n)} \in \Omega$.

(iii) 各々任意の $x,y \in \Omega$ に対して，$x+y \pmod{\phi(n)} \in \Omega$. ■

構造識別子 $SGID_S$ は，たとえば，$((s+a_1)a_2 + (s+b_1)b_2 + c_1)c_2 \pmod{\phi(n)}$ のように表現できる．

$\phi(n)$ の値が分かれば法をとることができるが，4 章で述べるように，提案方式では署名者や攻撃者は $\phi(n)$ の値を知らない．彼らが知ることができる値は，法をとる前の $\mathbf{Z}_{\pm K}$ 上の値である．$\mathbf{Z}_{\pm K}$ 上の値として扱うことを強調する場合は，$SGID_S \in \mathbf{Z}_{\pm K}$ と明示する．明示しない場合は，$\mathbf{Z}_{\phi(n)}$ 上の元とする．

SGID に関する性質をいくつか示しておく．

補題 1 $s = 1$，$\Lambda = \mathbf{Z}_{\phi(n)} \times \mathbf{Z}^*_{\phi(n)}$ とすると $\Omega = \mathbf{Z}_{\phi(n)}$.

証明: 適当な $u_2 \in \mathbf{Z}^*_{\phi(n)}$ を固定する．任意の $z \in \mathbf{Z}_{\phi(n)}$ に対して，u_1 を $zu_2^{-1} - 1 \,(\mathrm{mod}\ \phi(n))$ とすれば，定義 4 より $z = (1 + u_1)u_2 \in \Omega$．よって $\mathbf{Z}_{\phi(n)} \subseteq \Omega$．一方，定義 4 より $\Omega \subseteq \mathbf{Z}_{\phi(n)}$ となるので，$\Omega = \mathbf{Z}_{\phi(n)}$ が得られる． □

補題 1 は，ID 空間を最大にとると，SGID 空間も最大となることを主張している．本論文では，以下 $s = 1$ とし，$\Lambda = \mathbf{Z}_{\phi(n)} \times \mathbf{Z}^*_{\phi(n)}$，$\Omega = \mathbf{Z}_{\phi(n)}$ とする．

次に，(a_1, a_2) 以外の全 ID を集めた場合に，SGID をどのように表現できるかを，補題 2 で示す．

補題 2 ある署名構造 ISG_S が与えられたとする．定義 4 に従い，帰納的に $SGID_S$ を構築する際，$(a_1, a_2) \in \Lambda$ が使用されたとする．$SGID_S \in \mathbf{Z}_{\pm K}$ は，

$$(X + a_1)a_2 Y + Z \qquad (1)$$

と表現できる．ここで，$X, Y, Z \in \mathbf{Z}_{\pm K}$ であり，特に $X, Y > 0$，$Z \geq 0$.

証明: 法 $\phi(n)$ を知らなくても，定義 4 を帰納的に使うことにより，$\mathbf{Z}_{\pm K}$ 上の演算として，式 (1) の形に変形できる．また，$s = 1$，$(u_1, u_2) \in \Lambda$ としているので，$X, Y > 0$，$Z \geq 0$ は明らかである． □

なお，補題 2 は，攻撃者のように $\phi(n)$ の値を知らない状況での SGID の表現について述べていることになる．

さて，$(u_1, u_2) \in \Lambda$ を 2 組の乱数とし，定義 4 に示したように帰納的に SGID を構築したとする．SGID は $\mathbf{Z}_{\phi(n)}$ に一様に分布するので，次の定理が成り立つ．

定理 1 c を任意に与えられた定数とする．さらに，署名構造 ISG_1，ID を 2 組の乱数 $(u_{1,1}, u_{1,2}), \ldots$ とし，これらから定まる SGID を $SGID_1$ とする．すると，

$$P(SGID_1 \equiv c \,(\mathrm{mod}\ \phi(n))) = \frac{1}{\phi(n)}$$

である． □

n を RSA 署名の法とすると，$\phi(n)$ は十分大きな値であり，$1/\phi(n)$ は無視できるほど小さい．このことを利用して，多重署名方式を構築する．

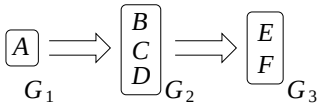

図 2 一般的な構造
Fig. 2 General group structure.

3.2 直列構造

直列構造では，署名順序が変われば構造識別子が変わり，結果として多重署名が変わるという性質が必要である．定義 4 に従う，最も単純な直列構造の例を示す．

例 2 A，B がこの順に署名する署名構造 ISG_S を考える．この場合，$SGID_S$ は $((1+a_1)a_2+b_1)b_2 (\mathrm{mod}\ \phi(n))$ となる．逆に B，A の順に署名する署名構造 ISG_R では，$SGID_R$ は $((1 + b_1)b_2 + a_1)a_2 \ (\mathrm{mod}\ \phi(n))$ となる． [例終]

3.1 節で示したように，ランダムに選ばれた (a_1, a_2) と (b_1, b_2) に対して，

$$((1 + a_1)a_2 + b_1)b_2 \equiv ((1 + b_1)b_2 + a_1)a_2 \qquad (2)$$

が法 $\phi(n)$ で成り立つ確率は低い．このため，定義 4 (ii) により生成された構造識別子は，直列構造の構造識別子に必要な性質を満たす．

3.3 並列構造

並列構造では署名順序を問わない．同一の並列構造に含まれる署名者は，並行して署名を行うことができる．つまり，構造識別子は個々の構造識別子の集め方や署名順序に依存しない．以下に例を示す．

例 3 A，B が並行して署名する署名構造 ISG_P を考える．この場合，$SGID_P$ は $(1 + a_1)a_2 + (1 + b_1)b_2 \,(\mathrm{mod}\ \phi(n))$ となる． [例終]

3.4 一般的な構造

直列，および，並列構造を組み合わせた署名構造 ISG_G を考える．**図 2** の例では，署名者は 3 つのグループ G_1，G_2，G_3 に分類され，同一グループ内では署名順序は問わないが，G_1，G_2，G_3 の間では署名順序を考慮する．

例 4 署名構造 ISG_G に対して，$SGID_G$ は，定義 4 に従い，次の手順で作成される．

G_1 の構造識別子 A の ID を使った $SGID_A$ は，
$(1 + a_1)a_2 \,(\mathrm{mod}\ \phi(n))$
となる．G_1 の構造識別子 $SGID_1$ は $SGID_A$ である．

G_2 の構造識別子 $U \in \{B, C, D\}$ の ID を使った $SGID_U$ は，$(SGID_1 + u_1)u_2 \,(\mathrm{mod}\ \phi(n))$ となる．G_2 の構造識別子 $SGID_2$ はそれらの和

$$\sum_{U\in\{B,C,D\}} SGID_U \pmod{\phi(n)}$$

である．

G_3 の構造識別子 E の ID を使った $SGID_E$ は，$(SGID_2 + e_1)e_2 \pmod{\phi(n)}$ となる．$SGID_F$ も同様で，G_3 の構造識別子 $SGID_3$ はそれらの和

$$SGID_E + SGID_F \pmod{\phi(n)}$$

である．

$SGID_3$ が，署名構造 ISG_G と署名者 $A,\ldots,F$ の ID から定まる構造識別子 $SGID_G$ である．また，$SGID_G$ を展開すると法 $\phi(n)$ で

$$\sum_{T\in G_3}\sum_{U\in G_2}(((1+a_1)a_2+u_1)u_2+t_1)t_2$$

となる．ここで，$G_2=\{B,C,D\}$，$G_3=\{E,F\}$ である．

なお，(b_1,b_2) 以外を定数として扱い，$SGID_G$ を補題 2 で示したように $(X+b_1)b_2Y+Z$ と表現すれば，

$$X=(1+a_1)a_2$$
$$Y=e_2+f_2$$
$$Z=e_1e_2+f_1f_2+\sum_{T\in G_3}\sum_{U\in G_2'}((X+u_1)u_2+t_1)t_2$$

となる．ここで，$G_2'=\{C,D\}$ である． [例終]

4. 提案する RSA 型多重署名方式

提案する方式では，信頼のおけるセンタの存在を仮定する．センタは新たな署名構造に対して 4.1 節に示す鍵の作成と配布を行う．その後，各署名者は 4.2 節に示すプロトコルに従って多重署名を作成する．センタの鍵配布は，署名構造ごとに最初に 1 度行うだけでよく，配布された鍵は再利用可能である．また，鍵配布が終了すればセンタは不要となる．

4.1 センタの鍵配布

署名構造 ISG_S が与えられたとき，センタは次の処理を行う．

(D1) RSA 署名の安全性のための様々な条件[12]を満たす 2 つの素数 p，q を生成し，その積 n を公開する．p，q は秘密情報であるが，鍵配布終了後は保持する必要はない．

(D2) 各署名者の秘密鍵として乱数 $(u_1,u_2)\in\Lambda$ を生成し，各署名者に安全に配布する．ただし，(u_1,u_2) は $u_1\in\mathbf{Z}_{\phi(n)}$，$u_2\in\mathbf{Z}^*_{\phi(n)}$ を満たすまで何度も生成する．

(D3) 署名構造 ISG_S と秘密鍵 $(u_1,u_2),\ldots$ から $SGID_S$ を求める．そして，

$$(SGID_S+v_1)v_2\equiv 1 \pmod{\phi(n)}$$

を満たす $(v_1,v_2)\in\Lambda$ を計算の後，公開する．実際には，$v_2\in\mathbf{Z}^*_{\phi(n)}$ を乱数として生成し，v_1 を $v_2^{-1}-SGID_S \pmod{\phi(n)}$ とすればよい．

上記に示したように，センタが配布する公開鍵は n，v_1，v_2 である．5.4 節でも述べるように，法 n は署名構造が異なれば変更しなくてはならない．

4.2 署名プロトコル

グループ G_i に属する署名者 U は，自分より前に署名すべき署名者により生成された中間署名 W と署名対象 M に対し，自己の秘密鍵 (u_1,u_2) を用いて署名を行う．ここで，G_i の署名構造内での位置により，次のように処理が分かれる．

G_i の署名順序が先頭である場合は，中間署名が存在しないので，$W=M$ とおく．一方，G_i の署名順序が先頭でない場合は，中間署名 W が存在するので，W をそのまま使う．このとき，グループ G_i での署名者 U の署名の順番に関係なく，U の署名生成処理は

$$(WM^{u_1})^{u_2} \pmod{n}$$

となる．G_i の全署名者が署名を作成した後，それらを乗じた

$$\prod_{U\in G_i}(WM^{u_1})^{u_2} \pmod{n}$$

をグループ G_i の中間署名 S_{G_i} とし．次のグループに渡す．

4.3 確認プロトコル

最終グループが出力した署名 S_S を最終的な多重署名とする．多重署名の検証は，

$$(S_SM^{v_1})^{v_2}\equiv M \pmod{n} \qquad (3)$$

により確認する．ISG_S に属する全署名者がプロトコルを順守すれば，$S_S\equiv M^{SGID_S} \pmod{n}$ となるので，式 (3) は成立し，S_S は受理される．

なお，式 (3) を確認するための計算量は署名者数に関係なく一定である．

4.4 プロトコルの具体例

例 4 で示した署名構造 ISG_G における署名作成手順と確認手順を示す．

鍵配布 まず，2 つの素数 p，q を生成し，n を求める．次に，$A,\ldots,F$ に対して秘密鍵を生成し，配布する．さらに，署名構造 ISG_G と秘密鍵 $(a_1,a_2),\ldots,(f_1,f_2)$ から $SGID_G$ を計算した後，

$$(SGID_G+v_1)v_2\equiv 1 \pmod{\phi(n)}$$

を満たす v_1，v_2 を計算し，n，v_1，v_2 を公開する．

G_1 の署名 最初のグループ G_1 には，署名者は A しかいない．A の作成する署名は $(MM^{a_1})^{a_2} \pmod{n}$ となる．これが G_1 の中間署名 S_1 である．

G_2 の署名 2番目のグループ G_2 の署名者 B，C，D は S_1 を受け取り，プロトコルに従い署名を生成する．たとえば，B の署名は $(S_1M^{b_1})^{b_2} (\mathrm{mod}\ n)$ となる．B，C，D の署名を乗じた

$$\prod_{U\in\{B,C,D\}} (S_1M^{u_1})^{u_2} \ (\mathrm{mod}\ n)$$

が G_2 の中間署名 S_2 である．

G_3 の署名 G_2 と同様の処理により，E，F の署名を乗じた

$$\prod_{U\in\{E,F\}} (S_2M^{u_1})^{u_2} \ (\mathrm{mod}\ n)$$

が G_3 の中間署名 S_3 である．G_3 は最終グループであるので，S_3 が署名構造 ISG_G での M に対する多重署名 S_G である．

確認 $(S_GM^{v_1})^{v_2} \equiv M \ (\mathrm{mod}\ n)$ が成立しているかどうかを確認する．プロトコルに従って作成された多重署名ならば，$S_G \equiv M^{SGID_G} \ (\mathrm{mod}\ n)$ であるから，S_G は受理される．

5. 安全性の評価

提案方式の安全性の評価を行う前に，安全性の仮定と攻撃モデルに関して記述する．

まず，提案方式では信頼のおけるセンタの存在を仮定する．さらに，H をプロトコルを順守する信頼のおける署名者とする．また，強い攻撃モデルでの安全性を考察するため，攻撃者は署名構造に関する情報を H に与えることができると仮定し，かつ，署名者 H は直前に署名したユーザの名前を確認できないと仮定する．本章では，このような状況の下で，センタと信頼のおける署名者 H を除いた全ユーザが結託する状況での安全性を考察する．

本章で証明する安全性は，次の項目である．

単一署名者の場合 単一署名者のみの署名構造を考え，RSA 署名の変形版としての安全性を評価する．

署名の偽造 H が参加していないにもかかわらず H の介在が必要な署名を偽造する．

署名構造の偽造 提案署名では H が中間署名 W の正当性を確認できない．そこで，攻撃者は H に不適切な中間署名 W を渡し，H はプロトコルに従って中間署名 $(WM^{h_1})^{h_2}$ を生成する．攻撃者はこれを利用して，最終的に受理される多重署名を偽造する．なお，本論文では，このような偽造方法の一種である，「オリジナルとは異なる署名構造や秘密鍵を出力する」攻撃についてのみ考察する．

異なる署名構造に対する攻撃 署名構造 ISG_1 に関する情報を利用して，他の署名構造 ISG_2 の署名を偽造する．

提案方式の大前提として，「秘密鍵が暴露しない」ことが必要ある．「秘密鍵の暴露」が困難であることを示すには，「署名の偽造」が困難であることを示せばよい．なぜなら，詳細に吟味すると，「秘密鍵の暴露」が「署名の偽造」よりも困難であることが導けるからである．実際，H の秘密鍵を暴露することができれば，H 以外の全署名者の結託により，$SGID_1$ を計算できるので，署名の偽造も容易となる．5.2 節で，「署名の偽造」が困難であることを証明するため，本章では「秘密鍵の暴露」については考察しない．

さて，以上の各項目を評価することは，署名構造 ISG_1 での M に対する多重署名 S の正当性を評価することにつながる．定義 1 (V1) は信頼のおけるセンタが確認鍵を生成することから保障される．定義 1 (V2), (V3) は，ISG_1 の法 n での演算のみを考えるか否かで議論が異なる．前者の場合，定義 1 (V2) については 5.2 節に「署名の偽造」として，定義 1 (V3) については 5.3 節に「署名構造の偽造」として考察する．後者の場合は，定義 1 (V2), (V3) のいずれの場合でも同様な議論が成り立つので，まとめて 5.4 節に「異なる署名構造に対する攻撃」として考察する．

なお，3 章で，署名構造や秘密鍵が異なるのに構造識別子が一致する確率を無視できることを記述した．この条件は直列構造の多重署名を実現するために必要であり，5.2 節や 5.3 節の議論の前提ともなっている．

3.1 節で記述したように，$\Lambda = \mathbf{Z}_{\phi(n)} \times \mathbf{Z}^*_{\phi(n)}$，$\Omega = \mathbf{Z}_{\phi(n)}$ とおく．したがって，秘密鍵 (u_1, u_2)，および，確認鍵 (v_1, v_2) はいずれも Λ の元である．また，一般に $\phi(n) \geq \ln(2) \cdot n/\ln(2n)$ が成り立つ．そこで $\rho = \lfloor \ln(2) \cdot n/\ln(2n) \rfloor$ とおく．さらに，本章では明記しない限り合同式の法は $\phi(n)$ とする．署名に参加する署名者数については，署名生成処理が実行可能な時間で終わらなくてはならないため，$|n|$ の多項式オーダと仮定する．

さて，H 以外の全署名者が結託すると，補題 2 より，H の秘密鍵 (h_1, h_2) を含む次の合同式が成り立つことが分かる．

$$((X + h_1)h_2Y + Z + v_1)v_2 \equiv 1. \qquad (4)$$

ただし，$(h_1, h_2), (v_1, v_2) \in \Lambda, X, Y, Z \in \mathbf{Z}_{\pm K}$ であり，X，Y，Z，v_1，v_2 は定数として与えられている．結託者は $\phi(n)$ を知らないので，$X, Y, Z \in \mathbf{Z}_{\phi(n)}$ とは限らない．なお，X，Y，Z，v_1，v_2 を得たとしても，式 (4) を満たす (h_1, h_2) は法 $\phi(n)$ で一意に定まらない．実際，次の補題が成り立つ．

補題 3 式 (4) を満たす H の秘密鍵 (h_1, h_2) は法 $\phi(n)$ で一意に定まらず，$\phi(\phi(n))$ 組存在する．

証明： H の秘密鍵 (h_1, h_2) を使い，$c = (X + h_1)h_2$ とおく．任意の $x_2 \in \mathbf{Z}^*_{\phi(n)}$ に対して，x_1 を $x_2^{-1}c - X \pmod{\phi(n)}$ とすれば，(x_1, x_2) は $c \equiv (X + x_1)x_2$ を満たす．$x_2 \in \mathbf{Z}^*_{\phi(n)}$ を満たす x_2 は $\phi(\phi(n))$ 組存在し，これらの (x_1, x_2) は，式 (4) を満たす．また以上は，$x_1' \in \mathbf{Z}_{\phi(n)} \setminus \left\{ x_2^{-1}c - X \pmod{\phi(n)} | x_2 \in \mathbf{Z}^*_{\phi(n)} \right\}$ を満たす x_1' が解の一部とならないことも意味する． □

なお，本論文では，式 (4) を満たす (x_1, x_2) を代用鍵と呼ぶことにする．

5.1 単一署名者の場合

ISG_0 を単一署名者 H のみから構成される署名構造とすると，結託は存在せず，署名構造も一意に定まる．この状況での，公開情報から多重署名を偽造する関数 PROPSig1 を定義し，RSASig との帰着関係を示す．

定義 5 PROPSig1(M, v_1, v_2, n) を次の入出力を持つ関数と定義する．

入力 署名対象 M，確認鍵 (v_1, v_2)，および，法 n．

出力 $M \in \mathbf{Z}^*_n, (v_1, v_2) \in \Lambda$，$n \in \mathbf{N}_{>1}$ を満たす入力に対して，$(SM^{v_1})^{v_2} \equiv M \pmod{n}$ を満たす $S \in \mathbf{Z}^*_n$ が存在すれば S を出力し，その他の場合は $\perp$ を出力する． ■

注)「その他の場合」とは，入力が $M \in \mathbf{Z}^*_n$，$(v_1, v_2) \in \Lambda$，$n \in \mathbf{N}_{>1}$を満たさない場合，および，$M \in \mathbf{Z}^*_n$，$(v_1, v_2) \in \Lambda$，$n \in \mathbf{N}_{>1}$を満たすものの，$(SM^{v_1})^{v_2} \equiv M \pmod{n}$ を満たす $S \in \mathbf{Z}^*_n$が存在しない場合に該当する．以後の関数の定義においても，「その他の場合」とは同様の場合を意味する．

定理 2 RSASig $\leq^p_{1-tt}$ PROPSig1.

証明： RSASig への入力を M，e，n とする．まず，$v_1 \in \mathbf{Z}_\rho$ を，仮定 2 で存在を仮定した乱数生成器を使って出力する．そして，PROPSig1(M, v_1, e, n) を計算する．v_1 は $v_1 \in \mathbf{Z}_{\phi(n)}$ を満たすため，もし M，e，n が $M \in \mathbf{Z}^*_n$，$e \in \mathbf{Z}^*_{\phi(n)}$ と $n \in \mathbf{N}_{>1}$ を満足するならば，PROPSig1 は $M^{d-v_1} \pmod{n}$ を S として出力する．$SM^{v_1} \pmod{n}$ を RSASig の出力とすればよい． □

この節の議論は，5.2 節の議論の特殊な場合に該当する．

5.2 署名の偽造

署名構造 ISG_1 に属する H が署名生成に参加しないにもかかわらず，ISG_1 に対する多重署名が偽造されるという状況が考えられる．そこで，公開情報と H 以外の全署名者の秘密鍵を使って多重署名を偽造する関数 PROPSig を定義する．

定義 6 PROPSig$(M, ISG_1, u_{i,1}, u_{i,2}, \ldots, v_1, v_2, n)$ を次の入出力を持つ関数と定義する．

入力 署名対象 M，署名構造 ISG_1，H を除く全署名者の秘密鍵 $(u_{i,1}, u_{i,2})$，確認鍵 (v_1, v_2)，および，法 n．

出力 $M \in \mathbf{Z}^*_n$，$(u_{i,1}, u_{i,2}), \ldots, (v_1, v_2) \in \Lambda$，$n \in \mathbf{N}_{>1}$ を満たす入力に対して，$(SM^{v_1})^{v_2} \equiv M \pmod{n}$ を満たす $S \in \mathbf{Z}^*_n$ が存在すれば S を出力し，その他の場合は $\perp$ を出力する． ■

次の定理が示すように，多重署名を偽造する関数 PROPSig を計算することは，少なくとも関数 RSASig を計算するほど困難である．

定理 3 RSASig $\leq^{ep}_T$ PROPSig.

証明： RSASig の入力を M，e，n とする．まず，H を含む適当な署名構造 ISG_1 を選ぶ．次に，仮定 2 で存在を仮定した乱数生成器を使って，H 以外の署名者の秘密鍵 $u_{i,1}, u_{i,2} \in \mathbf{Z}_\rho$，および，$x \in \mathbf{Z}_\rho$ を生成する．そして，PROPSig$(M, ISG_1, u_{i,1}, u_{i,2}, \ldots, x, e, n)$ を計算する．以上の処理を S が出力されるまで繰り返す．ここで，

$$\frac{\phi(\rho)}{\rho} \geq \frac{\ln(2) \cdot \rho}{\ln(2\rho) \cdot \rho} = \frac{\ln(2)}{\ln(2\rho)}$$

となるので，署名生成に参加する署名者数を α とすると，$(\ln(2\rho)/\ln(2))^\alpha$ 回試行すれば，α 人のすべての署名者に対して $u_{i,2} \in \mathbf{Z}^*_{\phi(n)}$ となる $u_{i,2}$ を生成できる (実際，期待値が 1 となる)．なお，ρ が $O(n/\ln(n))$ であるので，$(\ln(2\rho)/\ln(2))^\alpha$ は $O((\ln(n) - \ln(\ln(n)))^\alpha)$ となり，$|n|$ の多項式で表現される．また，生成した $u_{i,1}, x$ は $u_{i,1}, x \in \mathbf{Z}_{\phi(n)}$ を満たす．よって，e，n が $e \in \mathbf{Z}^*_{\phi(n)}$，$n \in \mathbf{N}_{>1}$ を満たすならば，平均的に $|n|$ の多項式オーダの試行により，PROPSig は $M^{d-x} \pmod{n}$ を S として出力する．$SM^x \pmod{n}$ を RSASig の出力とすればよい． □

5.3 署名構造の偽造

署名構造 ISG_1 に属する H 以外の全署名者が結託して，署名構造を偽造する攻撃について考察する．まず，公開情報と H 以外の全署名者の秘密鍵 $(u_{i,1}, u_{i,2}), \ldots$ を使って，H を含む署名構造 ISG_2 と H 以外の秘密鍵 $(u'_{i,1}, u'_{i,2}), \ldots$ を出力する関数 ChangeKey を定義する．

定義 7 ChangeKey$(ISG_1, u_{i,1}, u_{i,2}, \ldots, \eta, v_1, v_2, n)$ を次の入出力を持つ関数と定義する．

入力 署名構造 ISG_1，H を除く全署名者の秘密鍵 $(u_{i,1}, u_{i,2})$，代用鍵の個数 η，確認鍵 (v_1, v_2)，および，法 n．

出力 $(u_{i,1},u_{i,2}),\ldots,(v_1,v_2)\in\Lambda$，$n\in\mathbf{N}_{>1}$，かつ，

$$((X+h_1)h_2Y+Z+v_1)v_2\equiv 1 \qquad (5)$$

を満たす入力が与えられたとき，式 (5) を満たす η 組の代用鍵 (h'_1,h'_2) に対して，

$$((X'+h'_1)h'_2Y'+Z'+v_1)v_2\equiv 1 \qquad (6)$$

を満たす署名構造 ISG_2 と H を除く全署名者の秘密鍵 $(u'_{i,1},u'_{i,2})\in\mathbf{Z}_{\pm K}\times\mathbf{Z}_{\pm K}$ の組の中で，$X\neq X'$ となるものが存在すれば，その組 $ISG_2,(u'_{i,1},u'_{i,2}),\ldots$ を出力し，存在しない場合は $\perp$ を出力する．ここで，補題 2 より $SGID_1$ は，未知定数である H の秘密鍵 $(h_1,h_2)\in\Lambda$ を使い，$(X+h_1)h_2Y+Z$ と表現できることを利用して，式 (5) の $X,Y,Z\in\mathbf{Z}_{\pm K}$ を求めた．また，式 (6) の $X',Y',Z'\in\mathbf{Z}_{\pm K}$ も同様であるが，攻撃者の秘密鍵 $(u'_{i,1},u'_{i,2})$ は Λ に属する必要はない．代用鍵 (h'_1,h'_2) は H の秘密鍵 (h_1,h_2) と同一となる場合も含める． ■

なお，2.2 節で示した手法を用いれば，$X'=X$ となる中間署名を用いた偽造が可能であるが，本論文では，定義 1 の意味で正当な多重署名を生成可能であるかを議論しているため，定義 7 では $X'\neq X$ を取り上げている．

さて，もし ChangeKey の計算が容易ならば，攻撃者はプロトコルを逸脱して生成された中間署名に対して H に署名させることにより，多重署名を偽造できる．実際，ChangeKey$(ISG_1,u_{i,1},u_{i,2},\ldots,\eta,v_1,v_2,n)$ の出力結果から，式 (6) の X'，Y'，Z' を計算できる．すると，代用鍵 (h'_1,h'_2) が H の秘密鍵 (h_1,h_2) と一致する場合，次のように多重署名を偽造できる．

(C1) $M^{X'}\pmod n$ を H に渡す．

(C2) H は $(M^{X'}M^{h_1})^{h_2}\pmod n$ を計算し，自分の中間署名 S_H として次の署名者に渡す．

(C3) S_H を使い $S_H^{Y'}M^{Z'}\pmod n$ を計算し，これを多重署名 S_1 とする．

この S_1 は，(v_1,v_2) で受理される多重署名であるが，H の受け取った中間署名 $M^{X'}$ はプロトコルを順守した中間署名ではない．

さて，補題 3 より，式 (5) を満たす代用鍵の候補は $\phi(\phi(n))$ 組存在する．したがって，ChangeKey を利用した偽造攻撃は，ChangeKey が何組 (η 組) の代用鍵に対して出力を求めるかにより，次のように分類できる．

A) 2 組以上 ($\eta\geq 2$) の代用鍵に対する出力．

B) 1 組 ($\eta=1$) の代用鍵に対する出力．

さらに A) と B) の特別な場合を考える．

A') すべて ($\eta=\phi(\phi(n))$) の代用鍵に対する出力．

B') 真の秘密鍵に対する出力．

さて，A') の場合は，ChangeKey の出力を使って必ず偽造に成功する．しかし，η の値が小さくなればなるほど偽造に成功する確率は小さくなる．B) の場合は，ChangeKey の出力を利用した攻撃が成功する確率は $1/\phi(\phi(n))$ であり，実際には脅威とはならない．一方，B') の場合は ChangeKey の出力を利用した攻撃が必ず成功するが，そのためには秘密鍵の候補を減らすための情報が必要となる．

本論文では ChangeKey を利用した偽造について，A) と B') の場合について評価する．なお，A') の場合は A) に含まれる．

5.3.1 複数の候補における攻撃

代用鍵が複数存在することに関連して，次の補題が成り立つ．

補題 4 式 (5) を満たす 2 組以上の (h'_1,h'_2) に対して，式 (6) を満たす 1 組の $X'(\neq X),Y',Z'$ を見つけることができれば，$\phi(n)$ の倍数を入手できる．ここで，$X',Y',Z'\in\mathbf{Z}_{\pm K}$．

証明： $\bar{Z}=1-Zv_2-v_1v_2$，$\bar{Z}'=1-Z'v_2-v_1v_2$ とおいて式 (5)，(6) を整理すると，各々

$$h'_1h'_2Yv_2\equiv\bar{Z}-Xh'_2Yv_2$$
$$h'_1h'_2Y'v_2\equiv\bar{Z}'-X'h'_2Y'v_2$$

と変形できる．前者に Y'，後者に Y を乗じて $h'_1h'_2$ を含む項を消去すると，さらに

$$(\bar{Z}-Xh'_2Yv_2)Y'\equiv(\bar{Z}'-X'h'_2Y'v_2)Y$$

と変形できる．これを整理すると，

$$(X'-X)h'_2v_2YY'\equiv\bar{Z}'Y-\bar{Z}Y'$$

となる．h'_2 が仮定より $\mathbf{Z}^*_{\phi(n)}$ の 2 組以上の元をとりうるのに対して，右辺は定数である．つまり，この恒等式が成立するためには，$(X'-X)v_2YY'\equiv 0$ でなくてはならない．ここで仮定より，$X'-X\neq 0$ である．また，補題 2 より $Y>0$ であり，$v_2\in\mathbf{Z}^*_\phi(n)$ より $v_2>0$ でもある．よって，$Y'=0$ ならば式 (6) より $(Z'+v_1)v_2-1$ が，$Y'\neq 0$ ならば $(X'-X)v_2YY'$ が 0 以外の $\phi(n)$ の倍数となる． □

定義 8 ChangeKeyA$(ISG_1,u_{i,1},u_{i,2},\ldots,\eta,v_1,v_2,n)$ は，$\eta\geq 2$ という条件を付け加えた ChangeKey である． ■

定理 4 RSAPhi $\leq_T^{ep}$ ChangeKeyA.

証明： RSAPhi の入力を e，n とする．まず，H を含む適当な署名構造 ISG_1 を選ぶ．次に，定理 3 と同様に，H 以外の署名者の秘密鍵 $u_{i,1},u_{i,2}\in\mathbf{Z}_\rho$，および，$x\in\mathbf{Z}_\rho$ を生成する．そして，$ISG_2,(u'_{i,1},u'_{i,2}),\ldots$ が出力されるまで ChangeKeyA$(ISG_1,u_{i,1},u_{i,2},\ldots,\eta,x,e,n)$ を繰り返し計算する．

出力として，$ISG_2, (u'_{i,1}, u'_{i,2}), \ldots$ を得たら，式 (6) の $X', Y', Z' \in \mathbf{Z}_{\pm K}$ を計算する．また，入力値 $ISG_1, (u_{i,1}, u_{i,2}), \ldots$ から，式 (5) の $X, Y, Z \in \mathbf{Z}_{\pm K}$ を計算することもできる．このように求めた $X, Y, Z, X', Y', Z' \in \mathbf{Z}_{\pm K}$ は，補題 4 の入力条件を満たすため，補題 4 より $\phi(n)$ の倍数を得ることができる．よって，それを RSAPhi の出力とすればよい． □

5.3.2 単一の候補における攻撃

さて，B') の場合には，ChangeKey の出力を得ることができれば偽造攻撃が必ず成功するが，そのためには秘密鍵の候補を減らすための情報が必要となる．そこで，攻撃者は任意のメッセージ M_i，任意の中間署名 W_i，および，H の中間署名 $S_i \equiv (W_i M_i^{h_1})^{h_2} \pmod n$ の組 (M_i, W_i, S_i) を多項式オーダの個数だけ得ることができると仮定する．次に，ChangeKeyB′Info を定義する．

定義 9 ChangeKeyB′Info$(ISG_1, u_{i,1}, u_{i,2}, \ldots, 1, v_1, v_2, n, (M_i, W_i, S_i), \ldots)$ は，$\eta = 1$，$(h'_1, h'_2) = (h_1, h_2)$ という条件のほかに，多項式オーダの個数の多重署名の組 (M_i, W_i, S_i) を入力に加えた ChangeKey である． ■

定理 5 攻撃者は多重署名と同一法 n の任意の RSA 署名を得ることができると仮定する．すると，

RSAPhi $\leq_T^{ep}$ ChangeKeyB′Info.

証明： RSAPhi の入力を e，n とし，d を $ed \equiv 1 \pmod{\phi(n)}$ を満たす RSA 署名の秘密鍵とする．

まず，H を含む適当な署名構造 ISG_1 を選ぶ．H 以外の署名者の秘密鍵 $(u_{i,1}, u_{i,2})$ は，定理 3 と同様に生成する．補題 2 より，$SGID_1$ は $(X + h_1)h_2 Y + Z$ と表現でき，この Y が $\gcd(Y, e) = 1$ となるまで $ISG_1, (u_{i,1}, u_{i,2}), \ldots$ を繰り返し生成する．$\gcd(Y, e) = 1$ となれば，拡張ユークリッド互除法を用いて $ek - xY = 1$ となる正整数 k，x を求められる．

次に，ChangeKeyB′Info に与える入力を，署名構造 ISG_1，秘密鍵 $(u_{i,1}, u_{i,2}), \ldots$，確認鍵 $(v_1, v_2) = (k - Z, e)$，法 n，および，多項式オーダの多重署名の組 (M_i, W_i, S_i) とする．H の秘密鍵を $(h_1, h_2) = (-X - d, x)$ とすれば，$ed \equiv 1$ という関係より，この (h_1, h_2) と (v_1, v_2) が式 (5) を満たすことは簡単に確かめられる．また，複数の RSA 署名 M_i^d を入手すれば，(M_i, W_i, S_i) は任意の W_i を用いて

$$\begin{aligned} S_i &\equiv (W_i M_i^{-X-d})^x \\ &\equiv (W_i M_i^{-X} (M_i^d)^{-1})^x \pmod n \end{aligned}$$

と求めることができる．このように入力を選びながら，定理 3 や定理 4 と同様に $ISG_2, (u'_{i,1}, u'_{i,2}), \ldots$ が得られるまで，

ChangeKeyB′Info ($ISG_1, u_{i,1}, u_{i,2}, \ldots, 1, v_1, v_2, n, (M_i, W_i, S_i), \ldots$)

を繰り返し計算する．つまり，式 (6) を満たす X'，Y'，Z' を得るまで，ChangeKeyB′Info の計算を繰り返す．なお，$\gcd(Y, e) = 1$ が成立するまでの，および，ChangeKeyB′Info が答えを出力するまでの試行回数は，定理 3 と同様に $|n|$ の多項式時間と評価できる．

このとき，$(h_1, h_2) = (-X - d, x)$ を利用すると，

$$((X' + (-X - d))xY' + Z' + k - Z)e \equiv 1$$

となり，これを整理すると

$$((X' - X)xY' + Z' - Z + k)e - xY' - 1 \equiv 0$$

となる．ここで左辺を L とおく．もし，$L \neq 0$ となれば，L は 0 でない $\phi(n)$ の倍数である．もし $L = 0$ となった場合は，$L \neq 0$ となるまで，この手続きを繰り返せばよい．

なお，$X', Y', Z' \in \mathbf{Z}_{\pm K}$ がランダムに出力されるとすると，$X' > X$，$Y' > 0$，$Z' > Z + k$ となる確率は各々 1/4，1/2，1/4 である．実際，$\mathbf{Z}_{\pm K}$ から X' をランダムにとり，X を正の乱数として評価すると，$|X'| > |X|$ となる確率は 1/2，X' が正である確率は 1/2 であること等から分かる．さて，$X' > X$，$Y' > 0$，$Z' > Z + k$ の場合は $L > 0$ となることから，ChangeKeyB′Info の出力結果を 32 組集めれば，$L > 0$ となるものが存在することが期待できる．この L を RSAPhi の出力とすればよい． □

5.4 異なる署名構造に対する攻撃

署名構造 ISG_1 に関する情報を利用した，他の署名構造 ISG_2 での署名の偽造等の攻撃について考察する．まず，ISG_1 の全署名者が結託し，さらに ISG_2 の H を除く全署名者が結託する場合を考える．ISG_1，ISG_2 の公開鍵を，各々 $(v_{1,1}, v_{1,2}, n_1)$，$(v_{2,1}, v_{2,2}, n_2)$ とする．ISG_1 の全署名者が結託しているので $\phi(n_1)$ の倍数を得ることは可能である．しかし，提案方式では署名構造や署名者が異なれば法は異なる．つまり $n_1 \neq n_2$ である．したがって ISG_1 の情報から別の署名構造 ISG_2 の情報を得ることはできないと考えられる．なお，提案方式のベースとなった RSA 署名でも共通法 n を用いると安全性は保証されない[11),12)]．

同様に，ある署名構造 ISG_1 における H の中間署名を，別の署名構造 ISG_2 の中間署名として利用する攻撃は，演算の法が異なることから，成立しないと考えられる．たとえば，$SGID_1 = SGID_2 \in \mathbf{Z}_{\pm K}$ となったとする．このとき，ISG_1，および，ISG_2 での M に対する多重署名は，各々 $M^{SGID_1} \pmod{n_1}$，

$M^{SGID_2} \pmod{n_2}$ となる．しかし，演算の法が異なるため，これらの多重署名は異なる値となる．

6. 提案方式の変形版と問題点

提案方式に対する鍵の簡略化や閾値署名への応用は，一見可能と思えるが，実は安全性に問題がある．本章では秘密鍵の簡略化と閾値署名方式への応用に関する問題点を指摘する．

6.1 秘密鍵の簡略化に関する問題

本方式では，署名者 U の秘密鍵 (u_1, u_2) を 2 組の乱数として与えているが，$u_1 = 1$ のように，前者を定数とする[3]と，5.3 節で示した署名順序の偽造攻撃が成立する．

例 5 F，H，F' がこの順に署名する署名構造を考える．F，H，F' の秘密鍵を各々 $(1, f_2)$，$(1, h_2)$，$(1, f_2')$ とする．たとえば，$2f_2 + 1 = 3k$ の場合，F，F' が結託することにより，次に示す攻撃が成立する．

(F1) F は $M^2 \pmod{n}$ を中間署名 S_F として H に渡す．

(F2) H はプロトコルに従って $(S_F M)^{h_2} \pmod{n}$ を作成し，中間署名 S_H として F' に渡す．

(F3) F' は $(S_H^k M)^{f_2'} \pmod{n}$ を作成し，多重署名 $S_{F'}$ とする．

(F4) $S_{F'} \equiv M^{(((1+1)f_2+1)h_2+1)f_2'} \pmod{n}$ であるので，$S_{F'}$ は多重署名として受理される．[例終]

この例は定義 1 (V3) に反する．なお，本論文で提案した方式では，定理 4 および定理 5 より，このような攻撃は成立しない．

6.2 閾値法の適用に関する問題

文献 8) に示されている閾値法を提案方式に適用することには問題がある．署名構造 ISG_G（図 2）の一部である G_2 に対して $(2, 3)$ 閾値法を適用した場合を考える．すると，G_2 の任意の 2 ユーザにより G_2 の中間署名を構築するという応用が考えられるが，実は結託に弱い[4]．なぜなら，この応用では，署名構造 ISG_G の一部である G_2 の全ユーザが結託すると，$\phi(n)$ の倍数を得ることができるからである．実際，G_2 の全ユーザが結託すると，法 $\phi(n)$ で合同な秘密情報を 3 組得ることができるため，それらの差から高確率で $\phi(n)$ の倍数を得ることができる．

なお，この問題は署名構造の一部に閾値法を適用するために発生する．文献 8) で示されている方法は，G_2 だけを考慮するものであり，閾値以上のユーザ B，C，D が結託すれば署名が生成されるのは当然である．しかし，G_2 を含む署名構造 ISG_G を考えた場合，さらに A，E，F が参加したときにのみ，多重署名が生成されなくてはならない．

7. 秘密鍵の効率的な生成法

提案方式では，署名構造ごとに異なる法 n を作り，署名構造に属する全署名者に秘密鍵を配布しなくてはならない．そこで，hash 関数の存在を仮定して，秘密鍵の効率的な生成法を示す．

7.1 用語と仮定

N を RSA 署名の法 n のサイズとする．現在では，$N = 1024$ がよく使われている．

以下に述べる hash 関数の存在を仮定する．

定義 10 関数 $\mathtt{hash}(a)$ を次の入出力を持つ関数と定義する．

入力 $a \in \mathbf{Z}_{\pm K}$．

出力 $v \in \mathbf{Z}_{2^N}$．

hash は汎用一方向性ハッシュ関数であり，出力値は $\mathbf{Z}_{2^N}$ に一様に分布すると仮定する． ■

また，必要に応じて a を $a_1, a_2 \in \mathbf{Z}_{\pm K}$ を連結したものと見なし，2 入力であることを明示するために $\mathtt{hash}(a_1, a_2)$ と記述する．

7.2 ID を利用した多重署名方式

センタと 1 組の秘密鍵 $(\bar{u_1}, \bar{u_2})$ を共有している署名者 U が，hash 関数を用いて，署名構造ごとに新しい秘密鍵をセンタと共有する方法を示す．

まず，センタは自然数 t を公開する．t の値は署名構造に属する最大署名者数を評価して，後述の補題 5 や例 6 で示すように決定する．また $\beta(t)$ を t 以下の素数の積とする．各ユーザ U は個人情報 ID_U（メールアドレス等）を公開しているとする．

U は個人情報 ID_U と hash 関数を使って $U_1 = \mathtt{hash}(ID_U)$ と $U_2 = \mathtt{hash}(U_1)$ を計算する．なお，全ユーザは同様の作業により (U_1, U_2) を得ることができるので，(U_1, U_2) は公開情報と見なしてよい．

次に，U とセンタは署名構造 ISG_1 に対する秘密鍵を次のように計算する．

(S1) ISG_1 に属する全署名者の $(U_{i,1}, U_{i,2})$ を使って，

$$SGID(ISG_1, (U_{i,1}, U_{i,2}), \ldots) \in \mathbf{Z}_{\pm K}$$

を計算し $SGID_1$ とする．この計算は，署名構造 ISG_1 を知っている全ユーザが実行可能である．

(S2) 下記の手順で，(u_1, u_2) を計算する．

$$u_1 = \mathtt{hash}(SGID_1, \bar{u_1})$$
$$u_2 = \min\{i \geq \mathtt{hash}(SGID_1, \bar{u_2}) | \gcd(i, \beta(t)) = 1, i \in \mathbf{N}\}.$$

(u_1, u_2) は秘密鍵 $(\bar{u_1}, \bar{u_2})$ を知るセンタと U しか作成できない．つまり，このプロトコルを使うことで，

センタと署名者 U は秘密鍵 (u_1, u_2) を共有できる．また，(u_1, u_2) には $SGID_1$ が反映されている．すなわち，署名構造が異なるごとに，異なる秘密鍵を得ることができる．

なお，センタが作成する n は，$u_2 \in \mathbf{Z}^*_{\phi(n)}$ という条件を満たさなくてはならない．そこで，センタは下記手順で n を作成する．

(N1) 上述の (S1)–(S2) の処理により，署名構造に属する全署名者の秘密鍵 (u_1, u_2) を計算する．

(N2) RSA 署名の条件を満たす n を生成する．

(N3) 署名構造 ISG_1 に属する署名者 U の秘密鍵 u_2 が $\gcd(u_2, \phi(n)) > 1$ となった場合は，(N2) に戻る．全署名者の秘密鍵 u_2 に対して，$\gcd(u_2, \phi(n)) = 1$ となった場合は n を出力する．

u_2 が偶数ならば $\gcd(u_2, \phi(n)) \geq 2$ となるが，(S2) に示した u_2 の生成手順より，$\gcd(u_2, \beta(t)) = 1$ を満たすので，u_2 は偶数ではない．そこで (N2)–(N3) を繰り返せば，n を得ることができる．最後に (N2)–(N3) の繰返し回数を評価する．

補題 5 N を法 n のサイズ，t をセンタが公開した自然数，$T = |t|$ とし，署名構造に参加する署名者の上限を α とする．(N2)–(N3) を w 回繰り返した場合，n が出力される確率は $1 - (N\alpha/tT)^w$ と評価できる．

証明： $\phi(n) < n$ であるから $|\phi(n)| \leq N$ としてよい．議論を簡単にするため，$t = 2^T - 1$ とおく．すると $|t| = T$ である．また，hash 関数の定義から $|u_2| = N$ と仮定してよい．さて，u_2 の素因数分解を $\prod p_i$（ただし p_i は素数で重複を許す）とおく．(S2) に示した u_2 の生成手順より，u_2 は t 以下の素因子を持たない．つまり，u_2 のすべての素因子 p_i について $p_i > t$，すなわち $|p_i| \geq T$ である．よって，u_2 の素因子の数を M とすると，$M \leq N/T$ であることも分かる．

まず，u_2 の素因子 p_i に関して $\gcd(p_i, \phi(n)) = 1$ となる確率を評価する．これは $\phi(n)$ を乱数と見なせば $1 - 1/p_i$ と評価できる．したがって，

$$P(\gcd(u_2, \phi(n)) = 1) = \prod_{i \in \{1,\ldots,M\}} (1 - 1/p_i)$$

となる．この値は，$M = N/T$，つまり u_2 のすべての素因子について $|p_i| = T$ のとき最小になる．よって，$P(\gcd(u_2, \phi(n)) = 1)$ が最小となる場合，その確率は $(1 - 1/2^T)^{N/T}$ であり，$1/2^T$ が十分小さく，$N/T < 2^T$ ととれば，展開した最初の 2 項を用いて，$1 - N/T2^T$ と近似できる．α 組の秘密鍵 u_2 すべてに関して，$\gcd(u_2, \phi(n)) = 1$ となる確率は $(1 - N/T2^T)^\alpha$ であり，$N/T2^T$ が十分小さく，$\alpha < T2^T/N$ ととれば，$1 - N\alpha/T2^T$ と近似できる．

逆に，$\gcd(u_2, \phi(n)) > 1$ となる確率は $N\alpha/T2^T$ であり，(N2)–(N3) を w 回繰り返してもすべて失敗する確率は $(N\alpha/T2^T)^w$ である．つまり，w 回繰り返した場合，n が出力される確率は $1 - (N\alpha/tT)^w$ と評価できる． □

例 6 $N = 1024$, $\alpha = 20$ とする．$t = 8191$ ととれば，$T = 13$ となり，補題 5 の証明中の近似の条件（$1/2^T$，$N/T2^T$ が十分小さく，$N/T < 2^T$，$\alpha < T2^T/N$）を満たす．$N\alpha/tT = 0.19$ であるから，(N2)–(N3) を 1 回（$w = 1$）だけ実行した場合，n を得る確率は 0.81 となる．同じ条件で (N2)–(N3) を 3 回（$w = 3$）繰り返した場合，n を得る確率は 0.99 となる． [例終]

なお，適切な n を得る確率は $\phi(n)$ の素因子にも大きく依存する．たとえば，法 n を，$n = pq$，$p = 2p' + 1$，$q = 2q' + 1$（p，q，p'，q' は素数）ととれば，$\phi(n) = 4p'q'$ となる．$t = 2$ とおき，(S2) に従い u_2 を作成すれば，p'，q' はいずれも大きな素数であることから，$\gcd(u_2, \phi(n)) > 1$ となる確率は無視できるほど小さくなり，(N2)–(N3) を繰り返す必要はない．

8. 終わりに

本論文では署名構造と秘密鍵から定まる構造識別子を定義し，それを応用して様々な署名構造に適用可能な RSA 型多重署名方式を提案した．さらに，センタと信頼のおける署名者 H を除く全署名者が結託するという仮定の下に，様々な攻撃に対する安全性の評価を行った．署名の偽造（5.2 節）については，署名を偽造する関数と RSA 署名を偽造する関数との帰着関係を明らかにした．一方，署名構造の偽造（5.3 節）については，オリジナルとは異なる署名構造や秘密鍵を出力する攻撃についてのみ，それらを出力する関数と RSA 署名を偽造する関数との帰着関係を示した．なお，署名構造の偽造については，より一般化した「不適切な中間署名 W に対する H の中間署名を利用して，多重署名を偽造する」攻撃についての安全性を示さなくてはならない．現在のところ，この攻撃と RSA 署名を偽造する関数との帰着関係は，5.3 節の A') に相当する場合しか示されていない[6]．

さらに，一見可能に思える鍵の簡略化や，閾値署名への応用に関する問題点も指摘した．最後に，現実的な問題として，秘密鍵の効率的な生成法を示した．

謝辞 的確なコメントをくださった査読者の方々に感謝いたします．

参考文献

1) Boyd, C.: Some Applications of Multiple

Key Ciphers, *Advances in Cryptology – Eurocrypt'88*, LNCS, Vol.330, pp.455–467, Springer-Verlag (1988).
2) Burmester, M., Desmedt, Y., Doi, H., Mambo, M., Okamoto, E., Tada, M. and Yoshifuji, Y.: A Structured ElGamal-Type Multisignature Scheme, *Public Key Cryptography*, LNCS, Vol.1751, pp.466–482, Springer-Verlag (2000).
3) 土井 洋, 岡本栄司, 満保雅浩, 植松友彦：署名順序指定可能な多重署名方式, 1994 年 暗号と情報セキュリティシンポジウム講演論文集, SCIS94-2A (1994).
4) Doi, H., Okamoto, E. and Mambo, M.: Multisignature Schemes for Various Group Structures, *Proc. 36th Annual Allerton Conference on Communication, Control and Computing*, pp.713–722 (1999).
5) Doi, H., Okamoto, E. and Mambo, M.: Multisignature Schemes Using Structured Group ID, *Proc. 1st Japan-Singapore Joint Workshop on Information Security* (*JWIS'98*), pp.45–50 (1998).
6) Doi, H., Mambo, M. and Okamoto, E.: On the Security of the RSA-Based Multisignature Scheme for Various Group Structures, *Information Security and Privacy*, LNCS, Vol.1841, Springer-Verlag (2000).
7) Debating Encryption Standards, *Comm. ACM*, Vol.35, No.7, pp.32–54 (1992).
8) Dsemedt, Y. and Frankel, Y.: Shared generation of authenticators and signatures, *Advances in Cryptology – Crypto '91*, LNCS, Vol.576, pp.457–469, Springer-Verlag (1991).
9) ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory*, Vol.IT-31, No.4, pp.469–472 (1985).
10) Koblitz, N.: *A Course in Number Theory and Cryptography*, 2nd edition, GTM, Vol.114, Springer-Verlag (1994).
11) Moore, J.H.: Protocol Failures in Cryptosystems, *Proc. IEEE*, Vol.76, No.5, pp.594–602 (1988).
12) 岡本栄司：暗号理論入門, 共立出版 (1993).
13) Okamoto, T.: A Digital Multisignature Scheme Using Bijective Public-Key Cryptosystems, *ACM Trans. Computer Systems*, Vol.6, No.8, pp.432–441 (1988).
14) Rivest, R.L., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
15) Schnorr, C.P.: Efficient identification and signatures for smart cards, *Advances in Cryptology – Crypto '89*, LNCS, Vol.435, pp.239–252, Springer-Verlag (1990).
16) Yen, S. and Laih, C.: New Digital Signature Scheme Based on Discrete Logarithm, *Electronics Letters*, Vol.29, No.12, pp.1120–1121 (1993).

(平成 11 年 12 月 6 日受付)
(平成 12 年 6 月 1 日採録)

土井 洋（正会員）

昭和 63 年岡山大学理学部数学科卒業．同年日立ソフトウェアエンジニアリング（株）入社．平成 6 年北陸先端科学技術大学院大学情報科学研究科情報システム学専攻博士前期課程修了．現在岡山大学大学院自然科学研究科博士課程在学中．数論，暗号理論の研究に従事．

満保 雅浩（正会員）

昭和 64 年金沢大学工学部電気・情報工学科卒業．平成 2 年東京工業大学理工学研究科電気・電子工学専攻修士課程修了．平成 5 年同博士課程修了．博士（工学）．平成 5〜9 年北陸先端科学技術大学院大学情報科学研究科助手．平成 9 年より東北大学情報処理教育センター&情報科学研究科助教授．情報セキュリティの研究に従事．

岡本 栄司（正会員）

昭和 48 年東京工業大学工学部電子工学科卒業．昭和 53 年東京工業大学理工学研究科電子工学専攻博士課程修了．工学博士．同年日本電気（株）中央研究所入社．平成 3 年北陸先端科学技術大学院大学情報科学研究科教授．平成 11 年よりウィスコンシン大学暗号セキュリティセンター兼東邦大学理学部教授．グラフ理論，通信理論，数理計画，アルゴリズム，情報セキュリティをはじめとする情報数理システムの教育・研究に従事．平成 2 年電子通信学会論文賞，平成 5 年情報処理学会ベストオーサ賞受賞．著書「暗号理論入門」「電子マネー」等．IEEE シニア会員．ACM，IACR（International Association for Cryptologic Research），電子情報通信学会，情報理論とその応用学会，応用数理学会，日本セキュリティ・マネージメント学会各会員．