リング署名における署名者の証明と匿名性破棄プロトコル

菊池浩明[†] 多田美奈子[††] 中西祥八郎[†††]

リング署名とは，グループメンバなら誰でも署名が可能で，かつ検証者に対して，匿名性を保証できるグループ署名方式の 1 つである．しかしこの匿名性が完全に保証されているため，署名後何らかの問題が発生し，どのメンバによる署名であるかを特定する必要がある場合にも，署名者の開示は不可能である．そこで本稿では，リング署名に管理者の存在を仮定して必要に応じて管理者または署名者本人が署名者を開示できるリング署名プロトコルを提案する．提案プロトコルの安全性は，離散対数問題の困難性と安全なハッシュ関数の存在に基づいている☆．

Proof of Signer and Privacy Revocation Protocol in Ring Signature

Hiroaki Kikuchi,[†] Minako Tada[††] and Shohachiro Nakanishi[†††]

A ring signature is a group signature scheme that allows a member of a group to sign onto the message so that the resulting signature does not reveal their identity to others. A disadvantage of ring signatures is the lack of group administrators who can identify the signer from a given signature when necessary. To address the issue of identification of the signer, we present new protocols for a ring signature. These offer improvements in two functions: 1) proof of signer; a signer is allowed to prove his or her identity when he or she wish to discard anonymity, 2) privacy revocation by revocation managers; a set of managers can identify the signer from a given signature only when they agree to revoke the anonymity. Our construction is based on the protocol of Abe, et al. (2002). The security of the proposed protocol is based on an assumption of the hardness of the discrete logarithm problem and a secure hash function.

1. はじめに

グループ署名とは，グループに属しているすべてのグループメンバがグループを代表しての署名が可能であり，なおかつどのメンバが署名したのかを秘密にできる署名方式である．これは 1991 年に Chaum らによって初めて提案された[2]．その後も Camenisch らによって効率的なグループ署名方式[4] が提案されている．これらの方式は，グループ管理者の存在を仮定しており，グループ管理者のみ署名者の開示が行うことができる．

一方，Rivest らによってリング署名（Ring Signature）が提案されている[7]．さらに，共通鍵暗号と落し戸つき一方向性置換関数を用いたプロトコル[7] を基に，大久保らによって離散対数問題に基づくプロトコル[6] が提案されている．これらの方式は，前述のグループ署名同様，匿名性を保証しながらグループの代表での署名が可能であるが，管理者を持たず，署名から署名者の同定を行うのは，たとえ署名者本人でも不可能である．このように，リング署名から真の署名者の証拠を示すことを，署名者の**開示**とよぶ．

署名者の開示の要求には次の 2 種類が考えられる．

(1) 署名者の証明
署名者自身が自分が署名したリング署名の署名者であることを第三者に証明する．これは，オークションなどで落札前は自分が入札者であることを秘密にしておき，落札後に自分が落札者であることを示したい場合などに有効である．

(2) 管理者による匿名性破棄
信頼できる管理者が署名者の協力なく，与えられた署名の匿名性を破棄して署名者を特定する．

† 東海大学電子情報学部情報メディア学科
Department of Information Media Technology, School of Information Technology and Electronics, Tokai University
†† 東芝ソリューション株式会社 SI 技術開発センタ
Systems Integration Technology Center, Toshiba Solutions Corporation
††† 東海大学電子情報学部情報科学科
Department of Human and Information Science, School of Information Technology and Electronics, Tokai University

☆ 本稿の初期のバージョンは，文献 10)，11) で発表している．

リング署名をグループ署名の 1 つとして用いるときなどに，この性質が求められる．リング署名に，グループ管理者の機能を追加することと考えてよい．

署名者が自身で匿名性を破棄する際には，自分の秘密情報を漏らさずに証明を行いたい．それを実現するには，リング署名生成時に行う乱数要素を応用することが考えられるが，リングを構成する他の署名者が署名者を偽ることが可能であるために不十分である．また，真の署名者が他の署名者になりすまして，署名の証明を行って陥れることができてもならない．そこで，これらの不正行為に対し，本稿では，文献 6) で提案されたプロトコルを基に改良したリング署名プロトコルを提案する．

本稿の構成は次のとおり．2 章では，文献 6) を説明する．3 章では，自己開示可能リング署名プロトコルと，開示可能なリング署名プロトコルを提案し，4 章で評価を行い，5 章でまとめる．

2. 基本プロトコル

本章では，提案プロトコルの基本となる大久保らによるリング署名[6] について説明する．本プロトコルは，離散対数問題に基づいている．

2.1 モ デ ル

エンティティを次のように示す．

$\mathcal{G}$ ：グループメンバの集合
$\mathcal{U}_j$ ：$\mathcal{G}$ に属するメンバ $(j = 1, \ldots, n)$
$\mathcal{U}_i$ ：署名者

グループメンバは，$q \mid p-1$ を満たす大きな素数 p, q と，Z_p^* の位数 q の部分群の生成元となる g を生成し，p, q, g を公開する☆．また，これを元に，グループメンバ $\mathcal{U}_j$ は $x_j \in Z_q$ を秘密鍵，$y_j = g^{x_j} \bmod p$ を公開鍵として生成し，y_j を公開する．

署名者 $\mathcal{U}_i$ は，n 個の公開鍵 $y_j (j = 1, \ldots, n)$ のうち，少なくとも 1 つのある y_i に対応する秘密鍵 x_i を知っていることを，i を秘密にしたまま証明し，これを署名とする．ここで，H を一方向性セキュアハッシュ関数とする．

2.2 プロトコル 0

文書 m に対する署名 $\sigma[m]$ は，以下の手順で生成する．

Step 1 （署名生成）i について，

$$T_i = g^{\alpha} \bmod p, \quad (1)$$
$$c_{i+1} = H(m \parallel T_i)$$

を求める．ただし，$\alpha \in_U Z_q$ とする．

Step 2 $j = i+1, \ldots, n, 1, \ldots, i-1$ について，$s_j \in_U Z_q$ をランダムに選び，

$$T_j = g^{s_j} y_j^{c_j} \bmod p,$$
$$c_{j+1} = H(m \parallel T_j)$$

を順次計算する．ここで，j が n を超えたとき Step 1 に戻る，すなわち，$n+1 = 1$ になっていることに注意されたし．

Step 3 （秘密鍵 x_i を知っている）i について，

$$s_i = \alpha - x_i c_i \bmod q \quad (2)$$

を計算する．m に対する署名 $\sigma[m]$ は $\sigma[m] = (c_1, s_1, s_2, \ldots, s_n)$ である．

Step 4 （署名検証）$j = 1, \ldots, n$ まで以下を繰り返す．

$$T_j = g^{s_j} y_j^{c_j} \bmod p$$
$$c_{j+1} = H(m \parallel T_j)$$

$c_1 = c_{n+1}$ ならば受理し，そうでなければ棄却する．

2.3 リング署名の安全性

セキュアなリング署名プロトコルが満たすべき要求条件として，次をあげる．

匿名性 リング署名から第三者が真の署名者を同定できないこと．

偽造不可性 リング署名を構成するグループ $\mathcal{G}$ のメンバ以外が署名の偽造をできないこと（必ず，n 人中の 1 人の秘密鍵を用いていること）．

自己開示性 正しい署名者ならば，かつ，その人に限り，自分が署名したリング署名から署名者であることを証明できること．正しい署名者であることが開示できることの必要十分条件になっていることに注意せよ．すなわち，$\mathcal{G}$ のメンバだが署名者でない人があたかも署名者であったかのように証明できてはならない．

ぬれ衣不能性 署名者が $\mathcal{G}$ の他のメンバが署名者の証明に成功する（署名者のぬれ衣を着せる）ようなリング署名を作れないこと．

追跡可能性 信頼できる管理者（グループの合意）のもとで，署名者の同意なくリング署名からその署名者を追跡できること．

2.4 ナイーブな署名者証明プロトコル

基本プロトコルは，リングを閉じてしまった後は，たとえ秘密情報を公開したとしても，その署名がどのメンバによるものであるかの証拠にはならない．以下に署名の証明ができない例を示す．

☆ (p, q, g) とハッシュ関数 H に関しては，各ユーザごとに各々で設定することが可能であるが，ここでは簡単のために共通とした．

命題 2.1 真の署名者 $\mathcal{U}_i$ ならば，式 (2) を満たす α を示すことができる．

しかし，この逆は必ずしも真ではない（すなわち，プロトコル 0 のリング署名は自己開示性を満たさない）．

命題 2.2 署名者 $\mathcal{U}_i$ によるリング署名 $\sigma[m]$ があるとき，$\mathcal{U}_j \in G$，$j \neq i$ の各々について，式 (2) を満たす（偽の）α_j は必ず存在して，一意に決まる．

（証明）$\mathcal{U}_j$ は，自分の秘密鍵 x_j を用いて，与えられた署名の s_j, c_j を満たすように，$\alpha_j = s_j + c_j x_j \pmod q$ を求める．いかなる s_i，c_j に対してもこの式で定まる α_j は必ず存在して一意である． □

$\mathcal{U}_j (j = 1, 2, 3)$ とする．真の署名者は $\mathcal{U}_2$ とし，2.1 節のプロトコルに従い，署名を生成する．$\mathcal{U}_2$ は，Step 1 で用いた α を署名の証拠として提示するかもしれない．しかし，真の署名者ではない別のメンバ $\mathcal{U}_3$ が秘密鍵 x_3 を用いると，$s_3 = \alpha' - x_3 c_3 \bmod q$ を満たすような α' は必ず存在して一意に決まる．これを用いて，次のような検証が成り立つ．

$$\begin{aligned} T_3 &= g^{s_3} y_3^{c_3} \bmod p \\ &= g^{\alpha' - x_3 c_3} y_3^{c_3} \bmod p \\ &= g^{\alpha'} \bmod p \end{aligned}$$

T_3 は真の署名者 $\mathcal{U}_2$ が行った証明と同じであり，調停者には α と α' のどちらが真の情報か（情報理論的に）区別がつかない．つまり，秘密情報を公開しても，署名の証拠になりえない．

3. 提案プロトコル

3.1 概　　要

前章の基本プロトコルでは，チャレンジをハッシュでつなぎ，最後に自分のみが知る秘密鍵によってリングを閉じて，リング署名を実現していた．そこで，我々は署名生成時に用いる T_j の生成順が，署名者を特定していることに着目し，この順序を示す情報を乱数である s_j へ埋め込むことで，署名者自身による開示を実現する．

本章では，まず初めに自己開示可能性を満たすプロトコルを示す．その後，管理者によって追跡可能な提案方式を示す．

3.2 自己開示可能リング署名

3.2.1 署 名 生 成

H_2 を一方向性，二次不可逆性，衝突困難性の性質を満たす安全なハッシュ関数と定義する．他のエンティティ，パラメータなどは，基本プロトコル同様．署名者 $\mathcal{U}_i$ は Step 2 において，$j = i+1, \ldots, n, 1, \ldots, i-1$ について，乱数 r_j を選び，それを用いて，

$$s_j = H_2(r_j, c_j) \tag{3}$$

を定め，T_j，c_{j+1} を同様に計算する．また，$r_1, \ldots, r_n$ を安全に管理しておく．その他，署名検証までは 2.1 節の基本プロトコル同様．

3.2.2 署名者の証明

署名者 $\mathcal{U}_i$ は問題の署名について，$r_1, \ldots, r_{i-1}, r_{r+1}, \ldots, r_n$ を示す．検証者は，$j = 1, \ldots, i-1, i+1, \ldots, n$ について，

$$s'_j = H_2(r_j, c_j)$$

を計算し，$s'_j = s_j$ ならば，署名者の証明を受理し，そうでなければ，棄却する．

3.3 安全性の考察

真の署名者ならば，s_i 以外は式 (3) を満たす $r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_n$ を必ず示すことができる．真の署名者 $\mathcal{U}_i$ が，ほかの署名者 $\mathcal{U}_j$ に署名者（の証拠）をなすりつけようと思っても，s_i と c_i から $s_i = H_2(r_i, c_i)$ を満たす r_i を作ることが H_2 の二次不可逆性に矛盾するので，失敗する．逆に，偽の署名者が署名者になりすますことも，同様にして不可能である．よって，提案プロトコルは自己開示性とぬれ衣不能性の両方を満たしている．

また与えられた署名の s_i が式 (2) と式 (3) のどちらで生成されているかは，ハッシュ関数の一方向性の仮定の下で，第三者には区別できない．よって，提案方式は匿名性を満たしている．

また，署名自体の偽造に対する安全性は，ベースとなるリング（Schnorr）署名のものと同等である．

ハッシュ関数の例には，メッセージダイジェストや離散対数問題，またはタイムスタンプなどがあげられる．ハッシュ関数を用いた場合は，検証するために証拠 $r_1, \ldots, r_n$ を公開しなくてはならない．しかしたとえ，この情報を用いても s_i の生成順序は変えられないので開示は安全である．一方，H として次の様な離散対数

$$H'_2(r_j, c_j) = g^{r_j c_j} \bmod p'$$

を用いると，知識の証明 $PK\{\alpha | H_2 = (g^{c_j})^{\alpha}\}$ によって証拠を隠蔽したまま開示することができる．

不正な署名者は式 (3) を守らないかもしれない．したがって，署名の乱用など悪質なケースが露呈した際には，特定の条件の下で署名者の協力なしでも署名の開示が行えることが必要とされる．そこで以降の方式では，署名開示の権限を持たせた管理者の存在を仮定した方式について述べる．

3.4 追跡可能リング署名

3.4.1 準　　備

新しいエンティティとして失効管理者 $\mathcal{RM}_1, \ldots,$

$\mathcal{RM}_l$ を設ける．失効管理者は l 人中，k 人で協力して，安全な方法で $k-1$ 次多項式 $f(x)$ を作り，公開鍵 $h=g^{f(0)}$ を公開し，各 $\mathcal{RM}_i$ へシェア $f(i)$ を秘密に分散する．他は，基本プロトコル同様．

3.4.2 署名生成

署名者 $\mathcal{U}_i$ は i について，

$$T_i = g^{\alpha} \bmod p,$$
$$c_{i+1} = H(m \parallel T_i),$$

また，同じ α を用いて，

$$U = h^{\alpha} \bmod p$$

を求める．ただし，$\alpha \in_U Z_q$ とする．その他，基本プロトコル同様．署名は，$(c_1, s_1, \ldots, s_n, U)$ とする．

3.4.3 知識証明

正しく情報を埋め込んだことの証拠として，リング署名を生成した後，ゼロ知識証明により

$$\begin{aligned} &\log_g T_1 = \log_h U \\ \vee &\log_g T_2 = \log_h U \\ &\quad\vdots \\ \vee &\log_g T_n = \log_h U \end{aligned}$$

であることを示し，これを知識の証明 SK☆として，署名に添付する．具体的な手順を次に示す．

Step 1 $j = 1, \ldots, i-1, i+1, \ldots, n$ について，乱数 $z_j \in_U Z_q^*$ と，$e_j \in \{0,1\}^u$（u はセキュリティパラメータ）を生成し，

$$a_j = g^{z_j} T_j^{e_j},$$
$$b_j = h^{z_j} U^{e_j}$$

を求める．また，真の署名の i については，乱数 r_i を選び，

$$a_i = g^{r_i},$$
$$b_i = h^{r_i}$$

とする．

Step 2 一方向性セキュアハッシュ関数 $F : \{0,1\}^* \to \{0,1\}^u$ を用い，

$$e = F(m \parallel g \parallel h \parallel a_1 \parallel b_1 \parallel \cdots \parallel a_n \parallel b_n),$$
$$e_i = \left(\bigoplus_{j \in \mathcal{G} \setminus \{i\}} e_j \right) \oplus e$$

を求める．

Step 3 i について，$z_i = r_i - \alpha e_i \bmod q$ を計算する．$SK = (e, e_1, a_1, b_1, z_1, \ldots, e_n, a_n, b_n, z_n)$ とする．

☆ ここでの知識の証明は，通常の対話的なゼロ知識証明ではなく，ハッシュ関数でチャレンジを生成することで非対話的にした形式である．これは，リング署名に SK を付加する必要があるので，オンラインでの検証者が仮定できないためである．

結果として，m についての署名は，$(c_1, s_1, \ldots, s_n, U, SK)$ となる．

3.4.4 署名検証

署名本体の検証は，基本プロトコル同様．SK の検証を次に示す．

$$\begin{aligned} e &= F(m \parallel g \parallel h \parallel a_1 \parallel b_1 \parallel \cdots \parallel a_n \parallel b_n) \\ &\stackrel{?}{=} e_1 \oplus \cdots \oplus e_n \end{aligned}$$

ここで，$j = 1, \ldots, n$ について，

$$a_j \stackrel{?}{=} g^{z_j} T_j^{e_j},$$
$$b_j \stackrel{?}{=} h^{z_j} U^{e_j}$$

を行う．すべての検証が成功した場合のみ，署名を受理し，失敗した場合棄却する．

3.4.5 署名開示

管理者 $\mathcal{RM}_i$ は自分の持つ分散情報 $f(i)$ を用いて，$j = 1, \ldots, n$ について $T_j^{f(i)}$ を求めてコミットした後に共有する．l 人中の任意の k 人（以降の説明では，$RM_1, \ldots, RM_k$ とする）が協力して Lagrange の補間法を用いて $T_j^{f(0)}$ を求め，

$$U = T_j^{f(0)} \bmod p$$

が成り立つ j を持つ $\mathcal{U}_j$ をさがす．以下に具体的な手順を示す．

$\mathcal{RM}_1, \cdots, \mathcal{RM}_k$ は，$j = 1, \ldots, n$ について，

$$T_j^{f(0)} = \prod_{1 \le i \le k} T_j^{f(i)\lambda(i)}$$

を求める．ここで，

$$\lambda(i) = \prod_{1 \le i' \le k, i' \ne i} \frac{i'}{i' - i} \bmod q \qquad (4)$$

とする．このうち，

$$U \stackrel{?}{=} T_j^{f(0)} \bmod p$$

が成り立つ j を持つ $\mathcal{U}_j$ が，署名者である．

3.5 安全性の考察

署名の偽造に対する安全性は，リング（Schnorr）署名と，知識証明の安全性については文献 3) と同等である．

この方式では，管理者が秘密を分散して持つことにより，署名の開示を行うときには管理者が協力する．また管理者を複数置くことにより，閾値までの不正な管理者による開示も防ぐことができる．よって，提案方式は追跡可能性を満たしている．

また，本署名開示の処理は第三者による検証が可能である．なぜならば，式 (4) における $\lambda(i)$ は誰もが計算

表 1 提案プロトコルの効率
Table 1 Performance of proposed protocol.

	基本	自己開示	追跡可能	
			署名のみ	署名+SK
署名長	$\|q\|(n+1)$	$\|q\|(n+1)$	$\|q\|(n+1)+\|p\|$	$\|p\|(2n+1)+\|q\|(n+1)$ $+u(n+1)$
検証コスト	$\mathcal{O}(n)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$	
$\mathcal{RM}$ の管理量	N/A	N/A	$\mathcal{O}(1)$	
開示コスト	N/A	N/A	$\mathcal{O}(n)$	

できる公開情報であり，$\mathcal{RM}_i$ が計算する $S_i = T_j^{f(i)}$ は，秘密の分散情報 $f(i)$ を漏らすことなく，知識の証明で

$$\log_{T_j} S_i = \log_g F_i$$

を示すことができるからである．ここで，F_i は RM_i についての公開情報であり，$F_i = g^{f(i)}$ と定める．したがって，仮に不正な $\mathcal{RM}_i$ が偽りの計算結果を提示しても，この証明に失敗するので検出することができる．

4. 提案プロトコルの関係について

ここでは，2 章の基本プロトコルと，3 章であげた 2 種類の提案方式について考察する．署名長，検証時の処理コスト，管理者の管理する秘密情報のサイズ，開示に要する計算のコストに関しての，両プロトコルの効率の比較を**表 1** に示す．ここで，$|p|$ は素数 p のビット長を表している．一般に，$|p| \gg |q|$ なので $|p|$ のサイズが増える知識の証明は大幅な通信量の増加を招くことが分かる．

自己開示可能リング署名のプロトコルは匿名性，偽造不可性，自己開示性，ぬれ衣不能性を成立させる．一方，追跡可能リング署名のプロトコルは，管理者による追跡可能性を満たしている．そして，これらは組み合わせて一緒に用いることが可能である．同時に用いることにより，安全なリング署名の性質をすべて満足したリング署名を実現できる．

逆に，どちらか 1 つだけを用いることもできる．たとえば，追跡可能のプロトコルは通信コストを上げるので，前者だけを使うのは現実的である．ただし，そのときにはどの安全性を保証するのかを認識しておく必要がある．たとえば，追跡可能リング署名だけを用いたときには，$\mathcal{G}$ のメンバ j が他人が行ったリング署名に対して，命題 2.2 の方法で α_j を逆算し，自分の $U' = g^{\alpha_j}$ を再計算して置き換えることで，真の署名者であるという主張を許してしまう☆．この攻撃を成功させるためには，U を U' に置き換える必要があり，容易に検出できるので現実的ではないが，他人に後から署名者の証明の権利を横取りされることを防止するためには，やはり自己開示のプロトコルもあわせて実行することが望ましい．

☆ α_j の逆算をしなくても，メッセージについて新たにリング署名を計算してもよい．

5. おわりに

本稿では，大久保らによる離散対数問題に基づくリング署名[6] を用いた，開示可能な方式を提案した．提案プロトコルは，自己開示性を満たすためのプロトコルと信頼できる管理者による署名者の追跡を可能とするプロトコルの 2 つからなっており，用途に応じてそれぞれ単独でも両方でも用いることができる．

本稿の趣旨は，匿名性を持つ署名技術に特有の署名者の開示の問題点を指摘することとその実現が可能であることを構成的に示すことである．それゆえに，文献 6) に基づいた構成方式を示したが，ここで示した証明プロトコルはチャレンジの生成順序を保証するための冗長性があれば他のリング署名にも同様にして適用可能である．たとえば，Abe らによる複数の署名方式を混在させたリング署名[12] や Bresson らによる落とし戸付き一方向性置換関数を用いたリング署名[1] にもほぼ同様にして適用できる．ただし，Rivest らによる共通鍵暗号と組み合わせたリング署名[7] への適用はそれほど自明ではない．これらへの拡張などを今後の課題とする．

参考文献

1) Bresson, E., Stern, J. and Szydlo, M.: Threshold Ring Signatures and Applications to Ad-hoc Groups, *Advances in Cryptology—CRYPTO 2002*, pp.465–480 (2002).
2) Chaum, D.L. and Van Heyst, E.: Group Signatures, *Advances in Cryptology—EUROCRYPTO '91*, pp.257–264 (1991).
3) Cramer, R., Damgård, I. and Schoenmakers, B.: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols, *Advances*

in Cryptology—CRYPTO '94, LNCS, Vol.839, pp.174–187 (1994).
4) Camenisch, J.L. and Stadler, M.A.: Efficient Group Signature Schemes for Large Groups, *Advances in Cryptology—CRYPTO '97*, pp.410–424 (1997).
5) 桑門，田中：署名者の匿名性を有するディジタル署名方式，情報処理学会コンピュータセキュリティ研究発表会-CSEC18-35，pp.239–244 (2002).
6) 大久保，阿部，鈴木，辻井：証明長が短い 1-out-of-n 証明，暗号と情報セキュリティシンポジウム-SCIS2002，pp.189–193 (2002).
7) Rivest, R., Shamir, A. and Tauman, Y.: How to leak a secret, *Advances in Cryptology—ASIACRYPT 2001*, LNCS, Vol.2248, pp.552–565 (2001).
8) 崔，菊池，中西：ブラインドグループ署名，電子情報通信学会情報セキュリティ研究会-ISEC (2000).
9) 菊池，多田，中西：Ring signature に基づいた k-out-of-n 証明の提案，コンピュータセキュリティシンポジウム（CSS 2002），pp.83–87 (2002).
10) 菊池，多田，中西：リング署名プロトコルにおける署名者開示，情報処理学会コンピュータセキュリティ研究会（CSEC-20-27），pp.149–153 (2003).
11) Kikuchi, H., Tada, M. and Nakanishi, S.: Proof of Signer and Privacy Revocation in Ring Signatures, *4th International Workshop on Information Security Application* (*WISA 2003*) (2003).
12) Abe, M., Ohkubo, M. and Suzuki, K.: 1-out-of-n Signatures from a Variety of Keys, *Advances in Cryptology—ASIACRYPT 2002*, LNCS, Vol.2501, pp.415–432 (2002).

(平成 15 年 11 月 28 日受付)
(平成 16 年 6 月 8 日採録)

菊池　浩明（正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学院博士前期課程修了．1990 年（株）富士通研究所入社．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授，1997 年カーネギーメロン大学計算機科学学部客員研究員．2000 年東海大学電子情報学部情報メディア学科助教授，現在に至る．博士（工学）．ファジィ論理，多値論理，ネットワークセキュリティに興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞，2004 年情報処理学会研究開発奨励賞受賞．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM 各会員．

多田美奈子（正会員）

2002 年東海大学工学部電気工学科卒業．2004 年同大学院工学研究科博士前期課程修了．2004 年東芝ソリューション（株）入社，現在に至る．暗号セキュリティの研究に従事．電子情報通信学会会員．

中西祥八郎

1967 年東海大学工学部電気工学科卒業．1969 年同大学院博士前期課程修了．同年東海大学工学部電気工学科助手．1971 年同専任講師，札幌校舎勤務，1973 年同湘南校舎勤務．1985 年同助教授．1991 年同教授，2000 年同電子情報学部情報科学科教授，現在に至る．工学博士．日本知能情報ファジィ学会，電気学会，計測自動制御学会，システム制御情報学会，日本神経回路学会，日本経営工学会，IEEE，IFSA 各会員．