本資料について

- 本資料は下記論文を基にして作成されたものです。文章の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 題目：署名生成事実のない利用者は否認できるリング署名方式
- 著者：駒野 雄一, 加藤 岳久,新保 淳,太田 和夫（電気通信大学）
- 出展：東芝レビュー Vol.63 No.1
- 発表日：2008年

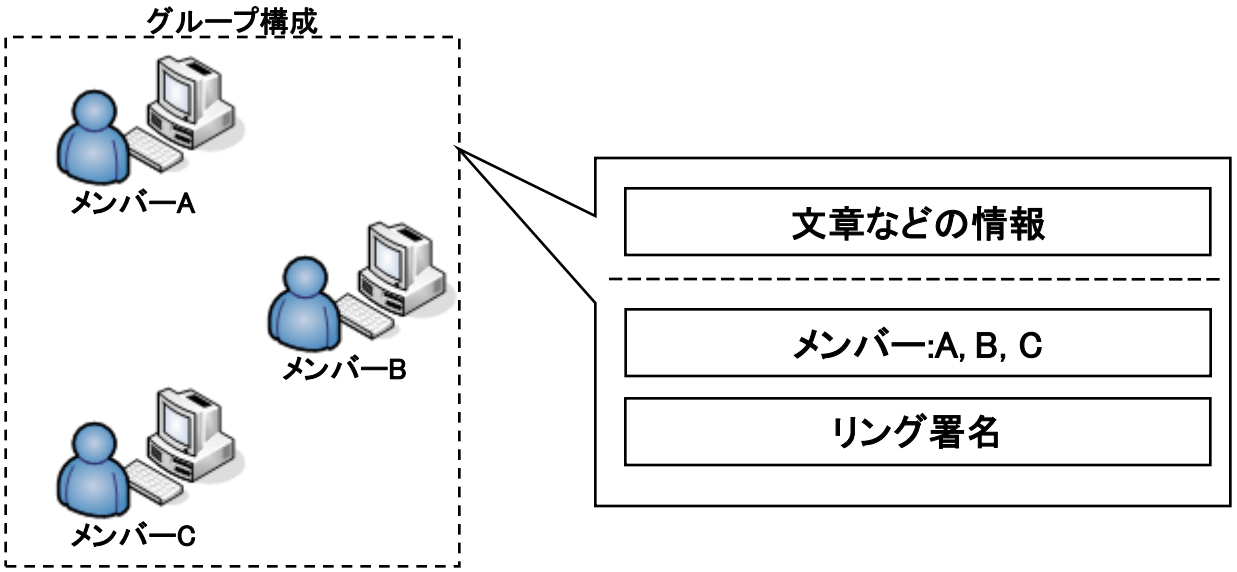
- 題目：リング署名における署名者の証明と匿名性破棄プロトコル
- 著者：菊池 浩明,多田 美奈子,中西 祥八郎（東海大学）
- 出展：情報処理学会論文誌 Vol.45 No.8
- 発表日： 2004年 8月

署名者の開示が可能なリング署名方式

名城大学理工学部
渡邊研究室
川島隆太

リング署名

- 匿名署名方式
  - グループを構成して署名することで、署名した人が所属するグループは検証できるが、署名をした人を特定できない

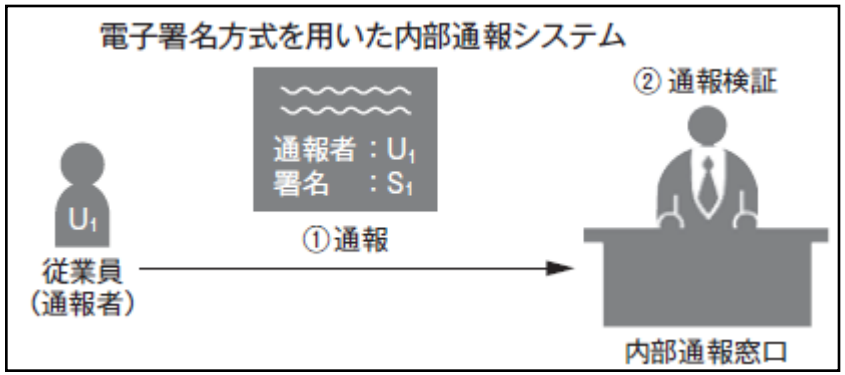


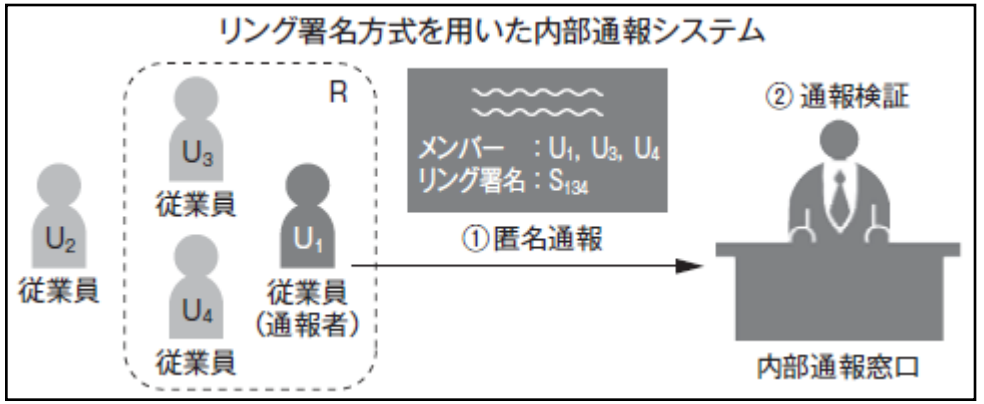
署名方法

- 署名者がリング署名方式の利用者を自由に指定してグループを構成
- 署名者自身の秘密鍵とグループメンバーの公開鍵を利用してリング署名を行う
  - 各メンバーは認証局に公開鍵を登録し、署名者は認証局から他のメンバーの公開鍵を入手する
  - PKIの上でグループに対応する匿名署名を生成可能

リング署名の利用例

- 匿名通報者保護システム
  - 組織に所属している者が内部告発などを行う際に、通報者が特定できないように匿名性を保証する目的で利用





リング署名の問題点

- 安全な匿名性に起因して、署名者を特定することができない
  - 保護システムでは、自分が通報したと証明できないため、保護対象であることを証明できない
  - リング署名の他のメンバーが通報者として疑われたとしても、署名者を特定できないため、疑いをはらすことができない
  - 保護を受けることで補償など利益がある場合に通報者以外のメンバーが通報者に成りすます可能性がある

署名者の開示

- 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
- 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

開示に伴い要求される安全性

- 匿名性
  - 第三者が証明者を特定できないこと
- 偽造不可性
  - リング署名を構成するグループのメンバー以外が署名の偽造をできないこと
- 自己開示性
  - 正しい署名者ならば、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

開示に伴い要求される安全性

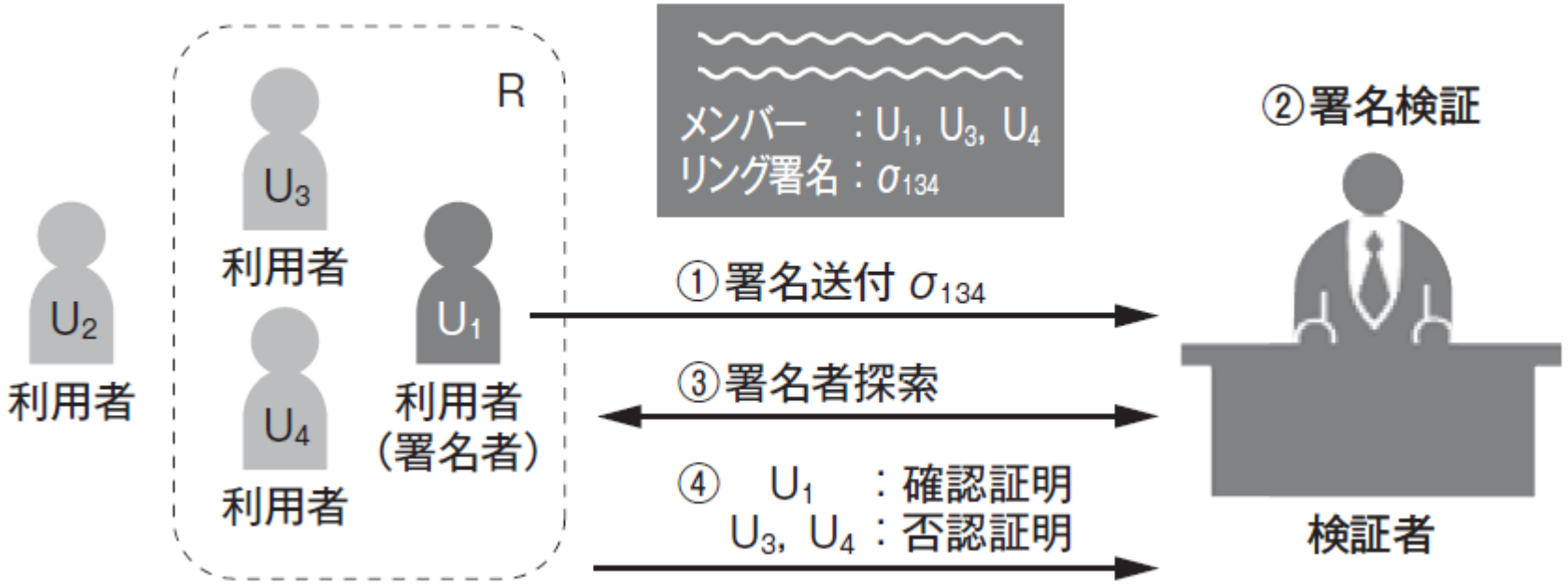
- ぬれ衣不能性
  - 署名者が他のメンバーが署名したようにみせかけるのをできなくすること
- 追跡可能性
  - 信頼できる管理者のもとで、署名者の同意なくリング署名からその署名者を追跡できること

否認機能を持つリング署名

- リング署名方式に検証者と署名者及び利用者の対話による確認・否認処理機能を持たせる
  - 署名者は確認処理を実行することで検証者に署名したことを証明（自己開示性、追跡可能性）
  - 利用者は否認処理を実行することで検証者に署名していないことを証明（ぬれ衣不能性）
  - 署名者とひとり以上の利用者が確認・否認処理を実行しない限り、署名者を特定できない（匿名性）

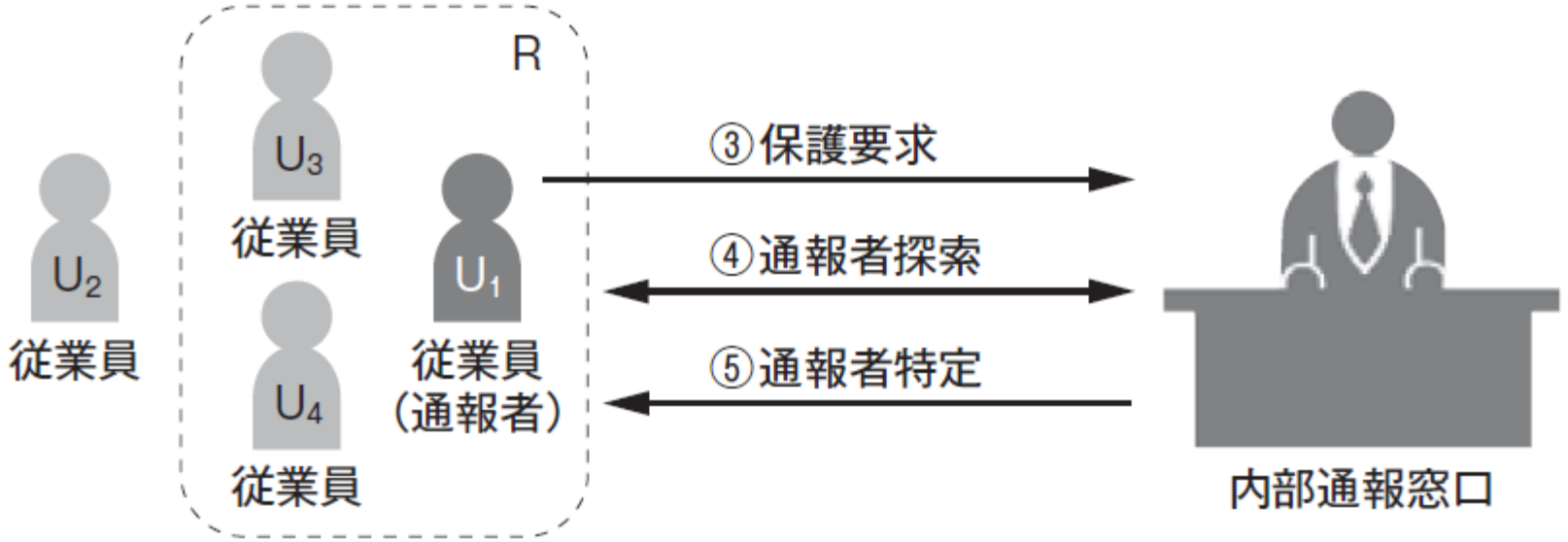
否認機能を持つリング署名

- 開示の流れ



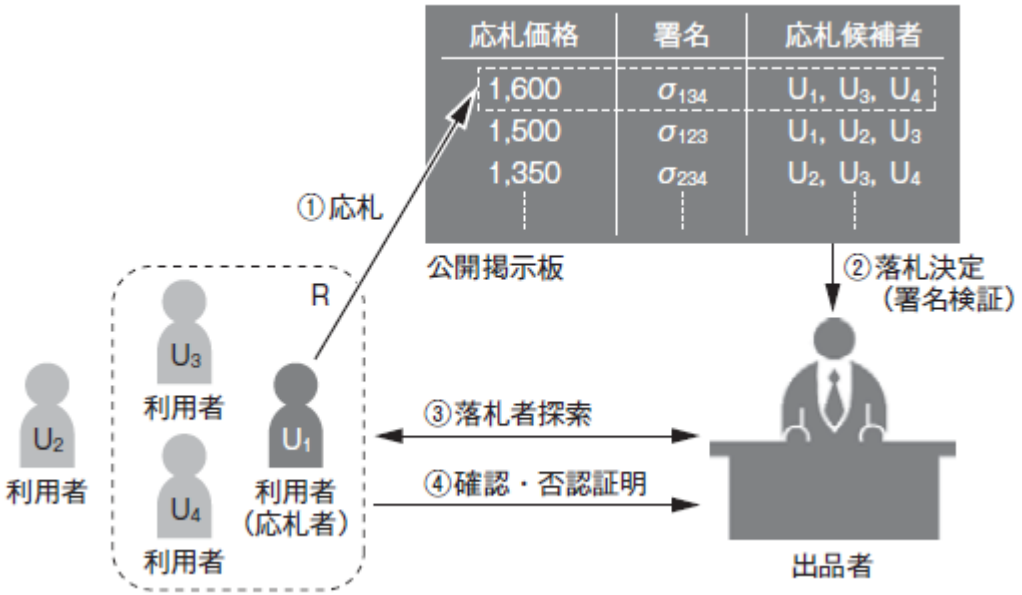
否認機能を持つリング署名の利用例

- 匿名通報者保護システム
  - 通報者が保護を求める場合に否認機能を利用



否認機能を持つリング署名の利用例

- 電子オークションシステム
  - 落札するまでは自分が入札者であることを秘密にでき、落札後に自分が落札者であると名乗りでることができる



まとめ

- 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
- 署名者の開示を目的とした機能を提案
- 開示を行えるようにすることで、リング署名の利用がしやすくなった

補足資料

- リング署名の基本プロトコル

G:グループメンバーの集合

U_j:Gに属するメンバー$(j=1,\ldots,n)$

U_i:署名者

グループメンバーは$q \mid p-1$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ー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U_iは、n個の公開鍵y_j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x_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

補足資料

- リング署名の基本プロトコル

Step1(署名生成) : iについて

$$T_i = g^{\alpha} \bmod p$$

$$c_{i+1} = H(m \| T_i)$$

を求める

ただし、$\alpha \in_U Z_q$とする

Step2 : $j = i+1,\ldots,n,1,\ldots,i-1$について

$s_j \in_U Z_q$をランダムに選び

$$T_j = g^{s_j} y_j^{c_j} \bmod p$$

$$c_{j+1} = H(m \| T_j)$$

を順次計算する

ここで、jがｎを越えた時Step1に戻る

補足資料

- リング署名の基本プロトコル

*Step*3: iについて

$s_i = \alpha - x_i c_i \bmod q$

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

$T_j = g^{s_j} y_j^{c_j} \bmod p$

$c_{j+1} = H(m \| T_j)$

$c_1 = c_{n+1}$ならば受理し、そうでなければ棄却する

補足資料

- 自己開示可能なリング署名のプロトコル

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U_iは$Step2$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

$$s_j = H_2(r_j, c_j)$$

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、署名検証までは基本プロトコル同様

補足資料

- 自己開示可能なリング署名のプロトコル

2.署名者の証明

署名者U_iは問題の署名について

$r_1,\ldots r_{i-1},r_{i+1},\ldots,r_n$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

補足資料

- 追跡可能なリング署名のプロトコル

  新しいエンティティとして失効管理者$RM_1,\ldots,RM_l$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

補足資料

- 追跡可能なリング署名のプロトコル

1.署名生成

署名者U_iはiについて

$$T_i = g^{\alpha} \bmod p$$

$$c_{i+1} = H(m \| T_i)$$

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

その他は基本プロトコルと同様

署名は$(c_1, s_1, \ldots, s_n, U)$とする

補足資料

- 追跡可能なリング署名のプロトコル

2.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

$$\log_g T_1 = \log_h U$$
$$\vee \log_g T_2 = \log_h U$$
$$\vdots$$
$$\vee \log_g T_n = \log_h U$$

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

補足資料

- 追跡可能なリング署名のプロトコル

*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

$$a_j = g^{z_j} T_j^{e_j}$$

$$b_j = h^{z_j} U_j^{e_j}$$

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

補足資料

- 追跡可能なリング署名のプロトコル

*Step*2: 一方向性セキュアハッシュ関数

$F:\{0,1\}^{*}\rightarrow\{0,1\}^{u}$を用い

$$e=F(m\|g\|h\|a_1\|b_1\|\cdots\|a_n\|b_n)$$

$$e_i=\left(\bigoplus_{j\in G\setminus\{i\}} e_j\right)\oplus e$$

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

結果として mについての書名は

$(c_1,s_1,\ldots,s_n,U,SK)$となる

補足資料

- 追跡可能なリング署名のプロトコル

3.署名検証

署名本体の検証は、基本プロトコル同様

*SK*の証明を示す

$$e = F(m \| g \| h \| a_1 \| b_1 \| \cdots \| a_n \| b_n)$$

$$\stackrel{?}{=} e_1 \oplus \cdots \oplus e_n$$

ここで、$j = 1,\ldots,n$について

$$a_j \stackrel{?}{=} g^{z_j} T_j^{e_j}$$

$$b_j \stackrel{?}{=} h^{z_j} U_j^{e_j}$$

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

補足資料

- 追跡可能なリング署名のプロトコル

4.署名開示

管理者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U_jをさがす

補足資料

- 追跡可能なリング署名のプロトコル

$RM_1,\ldots,RM_k$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

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

とする

このうち

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

が成り立つjを持つU_jが署名者である

補足資料

- 各プロトコルの効率
  - これらのプロトコルは組み合わせて用いることが可能
  - 自己開示と追跡可能のどちらかだけを用いることも可能

	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	$\mathcal{O}(n)$	