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

Ring Signature Scheme with Deniability of Involved Entities

駒野　雄一　■ KOMANO Yuichi
加藤　岳久　■ KATO Takehisa
新保　淳　■ SHIMBO Atsushi
太田　和夫　■ OHTA Kazuo

通報者本人が露見することなく，組織内部の労働者が公益通報を行うことを保証する技術にリング署名方式がある。しかし，リング署名から署名者を特定することは原理的に不可能であるため，公益通報者を適切に保護することが困難であるほか，署名生成事実のない利用者が不当な不利益を被るおそれがあった。

東芝と国立大学法人 電気通信大学は，数学的に安全性を保証できる，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を開発した。この方式を用いることで，公益通報者の匿名性保護システムや利用者属性に応じた匿名サービス提供システムなどが構築できる。

With the enactment of the Whistleblower Protection Act, the confidentiality of whistleblowers is guaranteed and their rights have to be protected. In the case of using electronic documents as a means of whistleblowing, the ring signature scheme has been proposed because of the perfect anonymity of the signer of the document. However, the whistleblower cannot be adequately protected from oppression by this scheme and, in addition, the involved entities in the whistleblower's organization may be damaged by suspicions.

Toshiba and the University of Electro-Communications have developed a provably secure ring signature scheme with deniability of involved entities. This scheme also makes it possible to construct other applications that ensure users' privacy similarly to whistleblower protection.

1　まえがき

デジタル署名（以下，署名と呼ぶ）は，印鑑の機能を電子的に実現する技術であり，誰（署名者）が何（文書）を承認したかを保証する技術である。2001年に「電子署名及び認証業務に関する法律」（電子署名法）[1]が施行されて署名が法的な効力を持つようになり，契約文書を電子的に交わすことができるようになった。

署名方式では，その性質から，署名検証ではどの署名者が署名を生成したかが特定される。しかし，アプリケーションが多様化し，署名者が特定のグループに属していることが確認できれば必ずしも署名者そのものが特定できなくてもよいという場面が生じている。これらのアプリケーションには，グループ署名方式やリング署名方式に代表される匿名署名方式が用いられる。匿名署名方式の署名検証処理では，グループメンバーのひとりが生成した署名であることは検証できるが，署名を生成したメンバーは特定できない。

ここでは，既存の匿名署名方式を用いてそれらのアプリケーションを構成した場合の問題点を考察するとともに，それらの解決技術として東芝と国立大学法人 電気通信大学が開発した，署名生成事実のない利用者は否認できる新たなリング署名方式（以下，否認機能を持つリング署名方式と呼ぶ）とその応用例について述べる。

2　匿名署名方式と応用例

2.1　公益通報者保護システム

公益のために通報を行ったことを理由とする解雇などの不利益な取扱いから労働者を保護するために，「公益通報者保護法」[2]が2006年に施行された。公益通報は，事業者の法令違反などを，事業所で働く労働者が，不正の目的(注1)ではなく，事業者及び行政機関などに通報することをいう。

公益通報を電子的に実現する場合，事業所で働く労働者による通報であることを保証するために署名方式を用いることが考えられる。しかし，署名方式では後に署名者が特定されるため，心理的負担から通報を控える可能性がある。

署名方式の代わりに匿名署名方式を用いた匿名公益通報者保護システムでは，これらの潜在的な通報を引き出すことができる。また，公益通報者保護法は，匿名での通報であっても，何らかの事情により通報者が特定されて不利益な扱いを受けた場合には保護対象になると規定しており，匿名による通報にも一定の理解を与えている。

2.2　リング署名方式

リング署名方式は，通報システムへの応用を想定してRivestらにより提案された匿名署名方式である[3]。リング署名方式では，署名者は利用者を自由に指定してグループRを構成し(注2)，

（注1）　通報を手段とする金品の授受などの不当な利益目的，他人の財産上の損害や信用の失墜などの加害目的などを指す。

署名者自身の秘密鍵とRのメンバーの公開鍵を利用して，文書mに対するリング署名S_Rを生成する。S_Rの正当性はmとRのメンバーの公開鍵により検証される。署名検証では，RのメンバーのひとりがS_Rを生成したことは確認できるが，署名者を特定することは原理的にできない（完全な匿名性を保証する）。

2.3 リング署名方式を用いた匿名公益通報者保護システム

通報者U_1（署名者）が，同じ組織に所属する従業員U_3とU_4を選択してRを構成し，通報内容m（文書）に関するS_{134}を生成して内部通報窓口に通報する例を**図1**に示す。内部通報窓口は，U_1，U_3，U_4の誰かがS_{134}を生成したことを検証することで組織内部からの通報であることを確認できるが，U_1を特定することはできないため通報者の匿名性は保証される。

図1のシステムには，次のような問題点が挙げられる。

(1) U_1が通報者として疑われ不利益な取扱いを受けたとしても，署名者を特定できないため，U_1はみずからが保護対象であることを証明できない。

(2) U_3やU_4が通報者として疑われ不利益な取扱いを受けたとしても，署名者を特定できないため，U_3，U_4は疑いを晴らすことも保護を受けることもできない。

(3) 保護を受けることで補償などの利益がある場合に，U_3やU_4が通報者を名のり保護を求める可能性がある。

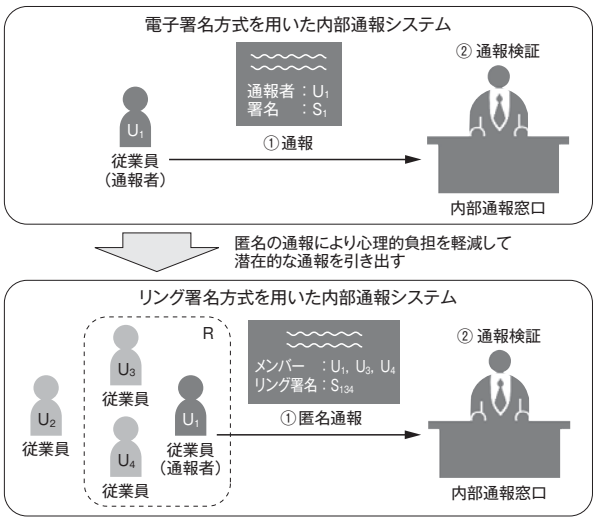

図1. リング署名方式を用いた公益通報者保護システム — U_1は，みずからの秘密鍵とU_3，U_4の公開鍵からリング署名S_{134}を生成する。S_{134}からはU_1を特定できない。組織内部の通報であることが確認でき，通報者の匿名性も保証される。

Whistleblower protection system using ring signature scheme

(注2) 各利用者は特定認証機関（認証局）に公開鍵を登録し，リング署名を生成する署名者は認証局から他の利用者の公開鍵を入手する。すなわちリング署名方式では，従来の公開鍵認証基盤（PKI）の上に，動的に特定の属性に応じたグループに対応する匿名署名を生成できる。一方，別の匿名署名方式であるグループ署名方式[4]では，グループの管理者がグループメンバーの署名鍵の設定に関与し，グループに対応する公開鍵を発行する。すなわち，従来のPKIとは異なる基盤を準備する必要がある。

2.4 リング署名方式の問題点と解決技術

前述の図1のシステムの問題点は，リング署名方式の完全な匿名性に起因する。須賀らは，解決手段として否認機能を持つリング署名方式の概念を導入した[5]が，安全性要件の定式化や，安全性を保証できる方式の構成が未解決であった。

3 否認機能を持つリング署名方式とその応用

3.1 否認機能を持つリング署名方式と安全性[6]

東芝と国立大学法人 電気通信大学は，否認機能を持つリング署名方式とその安全性要件を定式化し，安全性を保証できる方式を開発した。この方式では，従来のリング署名方式と同様に，署名者は利用者を自由に指定してグループRを構成し，署名者自身の秘密鍵とRのメンバーの公開鍵を利用して，文書mに対する否認機能を持つリング署名σ_Rを生成する。σ_Rの正当性は，mとRのメンバーの公開鍵により検証される。署名検証では，Rのメンバーのひとりがσ_Rを生成したことは確認できるが，署名者を特定することはできない。

否認機能を持つリング署名方式は，検証者と署名者及び利用者の対話による確認・否認処理機能を持つ。署名者は確認処理を実行することで検証者にσ_Rの生成事実を証明でき，利用者は否認処理を実行することで検証者にσ_Rの生成事実がないことを証明できる。ただし，署名者が否認処理を実行する，あるいは署名者ではない利用者が確認処理を実行したとしても，検証者を欺くことはできないように手順を構成する。

署名者U_1がふたりの利用者U_3とU_4を選んで，否認機能を持つリング署名σ_{134}を生成する例を**図2**に示す。

この方式では，確認・否認処理により署名者の候補を絞り込むことができる。この方式の匿名性は，署名者とひとり以上の利用者が確認・否認処理を実行していなければ署名者を特定することはできない，として定式化する。そのほかの安全性要件として，追跡可能性（確認処理で署名者候補が特定される）及び非転化性（署名生成事実を他人になすりつけることができない）を定式化した。

更に，ランダムオラクルモデル（理想的な一方向性ランダム

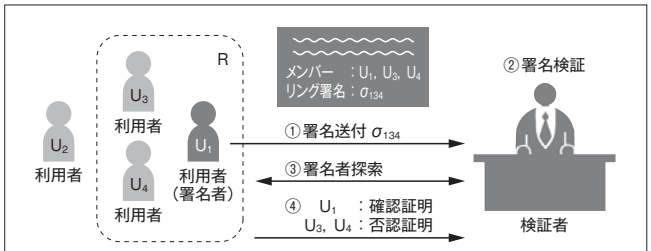

図2. 否認機能を持つリング署名方式 — U_1は署名生成事実を証明できるが否認できず，U_3とU_4は署名生成事実を否認できるが証明できない。

Proposed signature scheme

関数が存在すると仮定するモデル）において，ある種の問題が計算量的に困難であると仮定するとき数学的に安全性を保証できる具体的な方式を開発した。

3.2　否認機能を持つリング署名方式を用いた匿名公益通報者保護システム

この方式を用いた匿名公益通報者保護システムの構成例を**図3**に示す。通報者U_1（署名者）は，みずからの秘密鍵と事業所で働く労働者U_3，U_4の公開鍵を利用して通報（文書）に関するσ_{134}を生成し，内部通報窓口に匿名で情報を提供する。内部通報窓口は，σ_{134}を検証して事業所で働く労働者からの通報であることを確認した後，通報に関して調査・改善指導などを行う。なんらかの事情で通報者が特定されそうな場合には，U_1は確認処理により署名生成事実を証明して保護を求める。

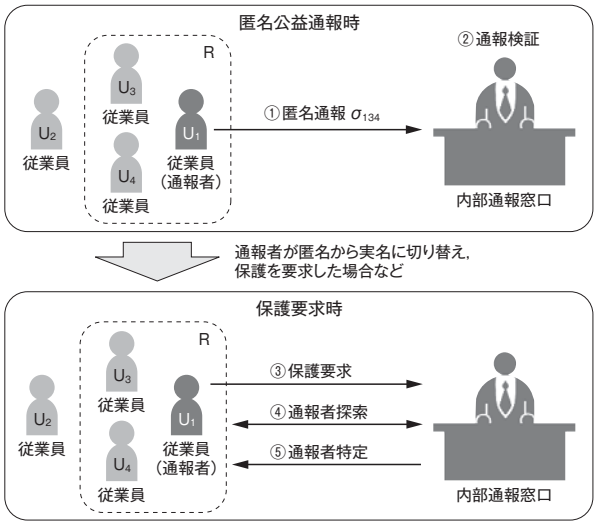

図3．否認機能を持つリング署名方式を用いた匿名公益通報者保護システム ― 不利益な取扱いを受けるおそれがある場合には，U_1は確認処理で通報事実を証明して保護を求める。

Whistleblower protection system using proposed signature scheme

このシステムには次のような利点がある。

(1)　グループメンバーの所属から，通報者が事業所で働く労働者であることが確認できる。

(2)　通報時の匿名性を保証することで，通報者の心理的負担を軽減して潜在的な通報を引き出すことができる。

(3)　不正な目的を持つ通報が行われた場合には，事業者はその不正を行政機関などに示し，確認・否認処理により通報者を特定できる。このため，不正な目的での通報を抑制できる。

(4)　通報者が特定されて不利益な取扱いを受けそうな場合，あるいは通報者ではない従業員が不当に不利益な取扱いを受けそうな場合，確認・否認処理により通報者を適切に特定して保護することができる。

署名者の匿名性を保証するグループ署名方式を利用しても類似のシステムを構築できるが，グループ署名方式ではグループ管理者が単独で署名者を特定できるため，(2)の通報者の心理的な負担は軽減できない。

4　そのほかの応用例

4.1　電子オークションシステム

Yahoo! JAPANや楽天市場™など，インターネット上において個人どうしで出品と応札を行うオークションが普及している。既存のシステムでは，参加者はID（識別番号）を利用して匿名でオークションに参加することができる。しかし，同一のIDを用いて応札を繰り返すと，応札履歴から好みや支払能力などがIDと関連付けられてしまい，応札者のプライバシーが損なわれる。

否認機能を持つリング署名方式を用いた，英国型匿名オークションシステム[7]を**図4**に示す。応札者U_1（署名者）は，公開掲示板に登録されている最高値の応札（1,500）に対応するσ_{123}を検証する。署名検証処理に合格した場合には，より高い応札金額（1,600）を設定し，みずからの秘密鍵とほかの利用者U_3，U_4の公開鍵を利用して応札金額（文書）に関するσ_{134}を生成し，公開掲示板に登録する。所定の時間が経過したら出品者は最高値の応札を決定し，確認・否認処理により落札者U_1を特定する。

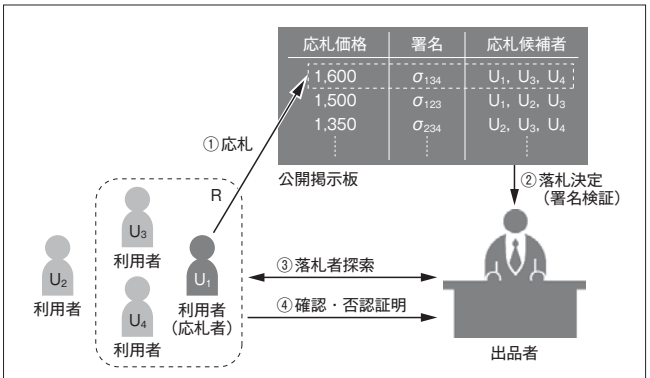

図4．電子オークションシステム ― 複数の応札間の対応付けが困難なまま匿名応札できる。落札者は確認・否認処理により特定される。

Electronic auction system

このシステムには次のような利点がある。

(1)　複数の応札を関連付けられない匿名応札を保証することで，利用者の心理的負担を軽減し，潜在的な応札を引き出すことができる。

(2)　落札者は確認処理により落札事実を証明することができる。落札者が名のり出ない場合には，応札候補者との間で確認・否認処理を行うことで落札者を特定できる。

一般論文

4.2　利用者属性に応じたサービス提供システム

東芝ソリューション（株）は，2002年に，購買者のプライバシー保護を実現する匿名認証システムを開発した[8], [9]。このシステムでは，購買者のプライバシーを保護しながら属性を証明する技術として，グループ署名方式を利用している。グループ署名方式は管理者に負荷と権限が集中するため，管理者の処理がシステムのボトルネックになり，管理者に対しては購買者のプライバシーが適切に保護されないおそれがあった。

今回，東芝と東芝ソリューション（株）は，否認機能を持つリング署名方式を利用し，利用者属性に応じたサービスを匿名で提供するシステム（**図5**）を考案した。

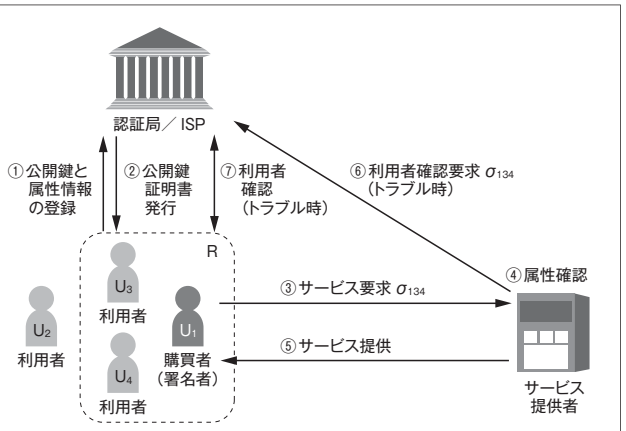

図5．利用者属性に応じたサービス提供システム — U_1は匿名のまま属性を証明してサービスを要求する。トラブル発生時には確認・否認処理で利用者を特定する。

Contents delivery system for attributed entities

インターネット サービス プロバイダー（ISP）は，利用者の公開鍵と属性情報を管理する。サービス提供者は，特定の属性を持つ利用者にだけサービスを提供する。購買者U_1（署名者）は，該当する属性を持つ利用者U_3，U_4の公開鍵を利用してσ_{134}を生成し，匿名通信路を介してサービス提供者にサービスを要求する。サービス提供者は，σ_{134}を検証して属性が確認できたら，同じ通信路でサービスを提供する。後にデータの破損などのトラブルが発覚し，購買者から補償を求められた場合には，サービス提供者はISPにσ_{134}を提示する。ISPは確認・否認処理を実行してU_1を要求者として特定し，サービス提供者とU_1で取り交わされる補償を仲介する。

このシステムには次のような利点がある。

（1）　受けたいサービスに応じて同一属性を持つ利用者を動的に選択し，単一の公開鍵証明書で多種類の属性証明書（署名）を生成できる。グループ署名を用いるシステムでは属性ごとにグループを用意する必要があり，属性の数だけ鍵を用意しなければならない。

（2）　サービス要求時の匿名性を保証することができるため，利用者の心理的な負担を減らすことができ，潜在的な要求を引き出すことができる。

（3）　問題発生時には，サービス提供者はISPを介して購買者を特定し，損害の補償を行うことができる。

5　あとがき

東芝と国立大学法人 電気通信大学が共同開発した，否認機能を持つリング署名方式と安全性，及びその応用例として利用者属性に応じたサービス提供システムについて述べた。今後は，これらのシステムを実用化するための詳細な検討と，プロトタイプシステムの開発を進めていく。

文　献

（1）　経済産業省．“電子署名及び認証業務に関する法律”．<http://www.meti.go.jp/policy/netsecurity/digitalsign-law.htm>，（参照2007-10-11）．

（2）　内閣府．“公益通報者保護制度ウェブサイト”．<http://www5.cao.go.jp/seikatsu/koueki/gaiyo/jobun.html>，（参照2007-10-11）．

（3）　Rivest, R.L., et al. “How to Leak a Secret”. ASIACRYPT 2001, LNCS 2248, Boyd, C., Springer, 2001, p.552－565.

（4）　Chaum, D.; van Heyst, E. “Group Signatures”. EUROCRYPT 1991, LNCS 547, Davies, D.W., Springer, p.257－265.

（5）　須賀祐治，ほか．“否認機能を持つリング署名方式”．2003年 暗号と情報セキュリティシンポジウム，6C-3，2003，p.435－440.

（6）　Komano, Y., et al. “Toward the Fair Anonymous Signatures: Deniable Ring Signatures”. IEICE Trans. on Fundamentals. **E90-A**, 1, 2007, p.54－64.

（7）　駒野雄一，ほか．“否認可能リング署名を用いた英国型匿名オークション方式”．2007年 暗号と情報セキュリティシンポジウム，3B4-3，2007，p.277.

（8）　加藤岳久，ほか．“個人情報保護を目的とした属性証明による認証システムの開発”．情報処理振興事業協会 2002年度成果報告集．＜http://www.ipa.go.jp/SPC/report/02fy-pro/index.htm＞，（参照2007-10-11）．

（9）　加藤岳久，ほか．匿名認証技術とその応用．東芝レビュー．**60**，6，2005，p.23－27.

駒野　雄一　KOMANO Yuichi, D.Sc.
研究開発センター コンピュータ・ネットワークラボラトリー，理博。暗号技術及び暗号応用システムの研究・開発に従事。国際暗号学会（IACR），電子情報通信学会会員。
Computer & Network Systems Lab.

加藤　岳久　KATO Takehisa
東芝ソリューション（株）IT技術研究所 研究開発部研究主務。プライバシー保護など情報セキュリティ全般の研究・開発に従事。電子情報通信学会，情報処理学会会員。
Toshiba Solutions Corp.

新保　　淳　SHIMBO Atsushi
研究開発センター コンピュータ・ネットワークラボラトリー主任研究員。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.

太田　和夫　OHTA Kazuo, D.Sc.
国立大学法人 電気通信大学 情報通信工学科 教授，理博。情報セキュリティ及び暗号理論の研究に従事。
国際暗号学会（IACR），電子情報通信学会会員。
The University of Electro-Communications