様式 C-19

科学研究費補助金研究成果報告書

平成　２２年　３月　１日現在

研究種目：若手研究（Ｂ）
研究期間：2007～2009
課題番号：19760256
研究課題名（和文）　完全なプライバシ保護を実現するグループ署名方式の提案とその実装

研究課題名（英文）　Proposal and Implementation of Group Signature Scheme with Complete Privacy　Protection

研究代表者
中西　透（NAKANISHI TORU）
岡山大学・大学院自然科学研究科・准教授
研究者番号：50304332

研究成果の概要（和文）：匿名認証技術であるグループ署名では、プライバシ管理者（PM）のみが署名作成者を特定可能とする性質を加えることにより、匿名利用者による不正行為を防止しようとしている。しかし、PM にはやはりプライバシ情報が蓄積されるため、プライバシ問題を完全に解決できていない。そこで本研究では、完全なプライバシ保護実現のために、PM を設置することなく、匿名不正者を排除可能なグループ署名方式の提案や PM なしの Web ベースの匿名認証システムの実装を行った。

研究成果の概要（英文）：In group signature schemes realizing anonymous authentications, only a Privacy Manager (PM) can trace the signer in order to protect anonymous signer's illegal acts. However, PM can collect the privacy of users, which means that the group signatures do not solve the privacy problem. In this study, to realize the complete privacy protection, we proposed a group signature scheme excluding anonymous illegal users without PM, and implemented a Web-based anonymous authentication system without PM.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,000,000	0	1,000,000
２００８年度	1,000,000	300,000	1,300,000
２００９年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,000,000	600,000	3,600,000

研究分野：情報セキュリティ
科研費の分科・細目：電気電子工学　通信・ネットワーク工学
キーワード：プライバシ保護、認証

１．研究開始当初の背景

インターネット・携帯電話網の急速な普及に伴い、社会のユビキタス化が進んでおり、いつでもどこからでもアクセスが可能となってきているが、基本的に誰でもがアクセス可能であるために、認証技術による不正アクセス防止が重要となる。しかし、現在一般的なID・パスワードによる認証、ディジタル署名による認証では、認証サーバに「誰がアクセスしたのか」というアクセス履歴が残ること

になる。ユビキタス社会においては、このような情報がいたるところで収集され蓄積されることにより、誰がどこで何をしていたということが追跡可能となり、プライバシ問題を引き起こす恐れがある。以上の背景から、ディジタル署名を拡張したグループ署名と呼ばれる匿名認証技術が盛んに研究され、実用化が目指されている。グループ署名では、ユーザは、予め認証サーバにグループのメンバーとして登録しておく。そして認証時には、ユーザは認証サーバに対して、匿名でグループに所属していることのみを証明する署名データを送信する。これにより、認証サーバは誰がアクセスしているかを知ることなく、グループ外の者による不正アクセスを防止でき、上記のプライバシ問題は解決可能となる。

しかし匿名でのサービス利用は、不正行為を誘発する恐れがある。例えば、電子掲示板サービス（BBS）では、匿名ユーザによる中傷的な書き込みの問題が頻発している。また、ネットオークションでも、不正な取引（支払い受け取り後に商品を送付しないなど）を誘発する可能性がある。そこでグループ署名では、特定のプライバシ管理者（以降、PM）のみが署名データから署名作成者を特定可能とする性質(追跡可能性)を加えることにより、この問題を解決しようとしている。しかしこの解決法では、PMにはやはりプライバシ情報が蓄積されるため、上記のプライバシ問題を完全に解決できているとはいい難い。

２．研究の目的

本研究では、完全なプライバシ保護を実現するために、PMを設置することなく、匿名不正者を排除可能なグループ署名方式の提案、実装、応用を研究目的とする。

３．研究の方法

PMなしでの匿名認証方式の概要を以下に示す。

認証時にユーザは、自分の秘密鍵からタグデータを生成し、グループ署名とともに送信する。認証サーバは、不正行為とみなされたアクセスからタグデータを取り出し、不正タグデータとして保存する。不正発生以降の認証では、ユーザは、「認証サーバから提示された不正タグデータを自分が作成していない」ことを証明する否認データを送信する。

不正行為を行なった者（不正タグデータの作成者）は否認データを作成できないため、不正者のアクセスを拒否できる。また、匿名性のため、正規ユーザのタグデータ・否認データは、余計な情報を漏らさないように構成する。このようなタグデータ・否認データの作成方法は知られていないが、近年研究が進んでいる楕円曲線暗号上で構成できるペアリングと呼ばれる双線形写像により実現できる。

(1)安全性の定式化

RSA暗号などの公開鍵暗号・認証技術では、満たすべき安全性を数学的に定式化し、構成した方式がその安全性を満たすことを数学的に証明する（証明可能安全性）。場当たり的に構築された認証方式では常に設計時に想定しなかった攻撃が発生する可能性があるが、証明可能安全性をもつ方式ではそのような問題がなく、高いレベルの安全性が保証される。本研究の方式は従来のグループ署名と匿名不正防止法が異なるため、安全性の明確化を目的として、安全性の定式化を行なう必要がある。重要な安全性として"匿名不正者の検出"と"匿名性"がある。"匿名不正者の検出"とは不正者とみなされた者による署名データを検出できる（すなわち不正者は認証を通過するデータを作成できない）性質であり"匿名性"とは署名データから署名作成者を特定できない性質である。結託攻撃も踏まえて攻撃者を

多項式時間チューリング機械でモデル化し、上記の性質を定義する。

(2) 署名方式の構築

定式化された安全性を満たす方式として、鍵生成処理、署名生成処理、タグデータ生成処理、否認データ生成処理のそれぞれについて、楕円曲線暗号とそれ上の双線形写像（ペアリング）をベースとして構築する。このとき、タグデータは匿名性をもつ必要があるが、タグデータと否認データが同じ署名者のものである場合には、否認できないことが必要となる。

(3) 安全性の検討

構築した方式が定式化した安全性を満たすことを数学的に証明する。この際、安全性の仮定として、ペアリングベース方式でよく用いられているStrong DH問題、Decisional Linear 問題を利用する。これらの問題は解くことが困難と一般的にみなされている問題である。安全性の証明では、構成した方式が安全性を満たさないこと、すなわちチューリング機械でモデル化された攻撃者が存在すると仮定し、その攻撃者をサブルーティンとして利用し上記の問題が解けることを示す。これにより、上記の問題の困難さの基で安全性が証明される。

(4) Webベース匿名認証システムの実装

グループ署名による匿名認証はWebサービスでのユーザ認証に応用できる。そこで、PMなしの方式を実装し、それをWebベースの認証システムに組み込む。そして認証速度を測定することにより、PMなし方式の有用性を確認する。

４．研究成果

(1) PM を利用しないグループ署名方式の提案

以下の着想に基づき、PMを利用することなく匿名の不正者を排除できる方式を提案した。

双線形写像とは、同じ素数位数 p の群 G, G_T 上で $e: G \times G \to G_T$ として定義され、任意の $u, v \in G$ に対して $e(u^a, v^b) = e(u, v)^{ab}$ を満たす。このような写像は、楕円曲線上で定義されるWeil, Tateペアリングにより実現できる。ベースとするグループ署名では、各ユーザの秘密鍵は Z_p のランダムな元 x として選ばれる。このとき、タグデータとして $f, g, h \in G$, 乱数 $\alpha \in Z_p$ に対して、$S = h^x g^\alpha$, $T = f^\alpha$ を計算する。タグデータは (f, g, h, S, T) である。一方、不正者のタグデータを $(\hat{f}, \hat{g}, \hat{h}, \hat{S}, \hat{T})$ とした場合、それに対する否認データは、乱数 $\beta \in Z_p$ に対して $D = e(\hat{f}^x, \hat{h})^\beta$, $E = \hat{f}^\beta$, $F = \hat{g}^\beta$ を計算し、(D, E, F) を否認データとする。

このとき、タグデータと否認データで使用されている秘密鍵 x が同一である場合、e が双線形写像であるために $e(E, \hat{S}) / e(\hat{T}, F) = D$ なる関係式が成立する。その理由を以下に示す。

$$
\begin{aligned}
&e(E, \hat{S}) / e(\hat{T}, F) = e(\hat{f}^\beta, \hat{h}^x \hat{g}^\alpha) / e(\hat{f}^\alpha, \hat{g}^\beta) \\
&= e(\hat{f}^\beta, \hat{h}^x) e(\hat{f}^\beta, \hat{g}^\alpha) / e(\hat{f}^\alpha, \hat{g}^\beta) \\
&= e(\hat{f}, \hat{h})^{\beta x} e(\hat{f}, \hat{g})^{\alpha\beta} / e(\hat{f}, \hat{g})^{\alpha\beta} = e(\hat{f}^x, \hat{h})^\beta \\
&= D
\end{aligned}
$$

鍵が同一でない場合は、この関係式が成立しない。ここで、ユーザが上記の式の通りに各データを計算したことを保証する必要がある。このために、ゼロ知識証明を利用する。ゼロ知識証明では、秘密情報(この場合は, x, α, β)を秘匿し

たまま離散対数型の関係式が成立することを証明できる。したがって、ユーザ・サーバ間でゼロ知識証明を利用することにより、不正なデータの計算を防止できる。以上のことから、否認データを作成した者が不正者であるかどうか判定できるため、“匿名不正者の検出”が満たされる。
一方、タグデータ及び否認データは乱数であるα,β乗した値により、秘密鍵xがマスクされており(離散対数であるx,α,βを求めるのは困難)、ゼロ知識証明も乱数α,β及び秘密鍵xを秘匿するため、通信されるデータからは秘密鍵xに関する情報が漏れない。すなわち“匿名性”が満足される。

また、従来のグループ署名を基に、安全性を定式的に定義し、Strong DH問題、Decisional Linear 問題を仮定して、安全性を数学的に証明した。

(2) PMを利用しない匿名認証システムの実装

Webベースにおいて匿名認証を行う場合、httpsプロトコルのSSL認証の部分に組み込むことが考えられる。しかし、ペアリング実装は現在研究が進んでいる分野でありSSLライブラリには組み込まれておらず、ペアリングベースの暗号技術をWebブラウザなどに組み込み実装することは容易でない。そこで、本研究では、ブラウザやWebサーバの外側にプロキシとして匿名認証を行うJavaベースのソフトウェアを実装した。

この動作概要は以下の通りである。まず、匿名認証が必要なURLへアクセスした際、ブラウザはプロキシへhttpsの中継を依頼する。すると、ブラウザ側のプロキシはサーバ側のプロキシを中継しWebサーバへ通信を行う。その際、両プロキシ間でSSLトンネルを張り、グループ署名を用いた匿名認証を行う。これに成功すると、Webサーバのレスポンスが両プロキシを経由してブラウザに返信される。それ以降は、プロキシはhttpを中継するのみとなる。

匿名認証方式としては、(1)で提案した方式よりも効率的な方式が同時期に以下で提案された。

Patrick P. Tsang, Man Ho Au, Apu Kapadia and Sean W. Smith,″Blacklistable Anonymous Credentials: Blocking Misbehaving Users Without TTPs,″ ACM CCS '07, Nov.2007.

この方式は、否認証明にペアリング計算を必要とせず(1)の方式よりも効率的となっている。(ただし、安全性仮定が異なるため、提案方式にも意味はある)

本研究では、上記の方式を、高速なペアリング・楕円曲線暗号ライブラリを用いて実装を行った。利用したライブラリは高速化のため、C言語を利用しており、Javaのプロキシプログラムからは、JNI(Java Native Interface)を経由して、暗号ライブラリに基づいた認証処理を呼び出すようにした。

そして、クライント及びサーバを通常のPC(C2D 2.53GHz, 3.0GHz)として、認証時間の測定を行った(通信は学内LAN)。その結果、認証時間は不正者の数に依存して線形で増加するという結果を得た。これは、PMなしの方式では、不正者のタグすべてに対して署名者は不正者でないことを証明することから、その計算量や否認データサイズが不正者数に依存するためである。上記の環境では、不正者数200、400、800の場合で認証時間がそれぞれ約4、7、13秒という結果であった。また、不正者数200、400、800の場合での、認証データサイズはそれぞれ、約30,60,110KBであった。データサイズはさほど大きくなく、認証時間中で計算時間が支配的であることが分かる。

測定結果より、不正者の数が少数であれば、十分実用的である。こうして、現状の方式を

利用する場合、ユーザ数が1000程度のグループウェアに適しているといえる。一方、YouTubeやWikipediaのようなインターネットレベルのサービスにおいては不正者数増加により認証時間の増加が大きな問題となる。このため、

> Patrick P. Tsang, Man Ho Au, Apu Kapadia and Sean W. Smith, ″PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication,″ ACM CCS '08, Oct. 2008. pp. 333-344. ACM, 2008.

で提案されているように、全期間の不正者を排除するのではなく一定期間内の不正者のみを排除可能とすることにより、不正者数に認証時間が線形で依存しない方式などの利用を検討していくことが今後の課題となる。

５．主な発表論文等

〔学会発表〕（計　4 件）

① Toru Nakanishi and Nobuo Funabiki: A Short Anonymously Revocable Group Signature Scheme from Decision Linear Assumption, In 3rd ACM Symposium on Information, Computer and Communications Security (ASIACCS'08), pp.337-340, March 2008 (Tokyo, Japan)

６．研究組織

(1)研究代表者

中西　透（NAKANISHI TORU）

岡山大学・大学院自然科学研究科・准教授

研究者番号：50304332