様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　25 年　4 月　12 日現在

機関番号：15301
研究種目：基盤研究(C)
研究期間：2010～2012
課題番号：22560378
研究課題名（和文）
スケーラブルな失効可能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 Revocable Group Signature Scheme with Scalability
研究代表者
中西　透（TORU NAKANISHI）
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）：グループ署名と呼ばれる匿名認証技術により、正規ユーザであることを匿名で認証でき、プライバシを保護できる。従来のグループ署名方式では、メンバー失効の困難さのため、ユーザ総数もしくは失効数に比例する計算量やデータ量を必要としていた。本研究では、計算量とデータ量の両面において効率的に失効可能な方式を構築し、ペアリングと呼ばれる暗号技術の高速化により、スケーラブルなシステム実装を実現した。

研究成果の概要（英文）：By anonymous authentications called group signatures, a user can be anonymously authenticated, and thus the privacy of users is protected. In conventional group signature schemes, the computational and/or communicational costs depending on the number of users and the number of revoked ones are required for member revocations. In this research, we constructed revocable schemes that are efficient on both costs, and realized scalable implementations by the fast pairing computations.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,200,000	360,000	1,560,000
２０１１年度	1,100,000	330,000	1,430,000
２０１２年度	1,100,000	330,000	1,430,000
総　計	3,400,000	1,020,000	4,420,000

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。

その実用化における重要な課題として、メンバー失効の効率的な実現がある。グループ署名では、署名データが匿名であり、従来のPKIのように、ID情報を利用した失効管理を行えない。そこで、匿名のまま失効可能な方式がいくつか提案されており、3つのタイプに分類できる。ここで、メンバー総数を N, 失効数を R とする。1つ目は検証者ローカル方式であり、署名者の負担がないという利点があるものの、検証者は O(R)の計算時間が必要となる。2つ目のタイプでは、署名・検証それぞれが O(1)のコストとなるものの、失効のたびに管理サーバでの失効者リストの作成に O(R)の計算が必要となる。3つ目のタイプはアキュムレータと呼ばれる技術を用いた方式であり、署名・検証コストおよび失効リスト作成コストが O(1)となるものの、公開鍵サイズが O(N)となる問題がある。以上のことから、従来提案された方式では、大規模なシステムにおいて N,R が増加した場合に効率的に処理できないという問題がある。

２．研究の目的

本研究では、大規模な環境において実用的なメンバー失効を実現するために、署名生成・検証・失効処理の計算量と公開鍵長がすべて効率的なスケーラブルな失効可能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

(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同様に安全性の定式化を行なう。重要な安全性として"偽造不能性(追跡可能性)"と"匿名性"がある。 "偽造不能性"とは、グループメンバーによる署名を偽造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。"偽造不能性"については、メンバー失効も考慮して定式化を行なう。

(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、失効データ生成処理、署名生成処理、署名検証処理、追跡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。

① Camenischらの方式をベースとする構成

PKC09 において Camenisch らにより提案された方式をベースとする。この方式では、アキュムレータにより、多数のデータを単一のデータへ変換する。すなわち、アキュムレータを f とすると、$f(x_1,\cdots x_n)=y$ となる。さらに、入力値 $x_1,\cdots x_k$ に対して、証拠と呼ばれる値 w_i へ変換する。このとき、関数 g に対して、$g(w_i,x_i)=y$ が成立する。こうして、各入力に対して、固定長の関係式を証明することにより、所属関係を証明できることになる。そしてグループ署名方式においては、所属証明書中の ID をアキュムレータの各入力値と対応付け、所属が有効なもののみをアキュムレートし、出力値を公開する。そしてグループ署名では、$g(w_i,x_i)=y$ をゼロ知識で証明する。失効されたメンバーはこの式を証明できないため、メンバー失効が実現される。しかし、問題点として、公開鍵が O(N)個のデータを必要とする(具体的には、上記の $x_1,\cdots x_n$ が公開鍵にあたる)ためスケーラビリティに問題がある。

そこで、本研究では、1つのグループを k 個のサブグループに分割することを考える。サブグループを $SG_1, \cdots, SG_k$ とする(k は $O(N^{1/2})$) 。このとき、各サブグループも $O(N^{1/2})$個のメンバーから成る。そして、各メンバーは二つの ID s_j, x_i で表し、所属証明書はこれら 2 ID の証明書とする($Cert(s_j, x_i)$)。アキュムレータについては、各サブグループ s_j ごとに、そのサブグループのすべてのメンバーの x_i に対して行い、アキュムレート値を y_jとする。さらに、この y_j に対してサブグループ証明書($Cert(s_j, y_j)$)を発行する。このとき、グループ署名は、$Cert(s_j, x_i)$の保有、$g(w_i,x_i)= y_j$の保証、$Cert(s_j, y_j)$の保有をゼロ知識証明する。s_j, x_i, y_jは秘匿されるため ID(サブグループ ID すらも)が秘匿され、匿名性が成り立つ。一方、y_jの正当性が証明書により保証されるため、異なるサブグループの使用などもできず、ユーザ失効の正当性が保障される。提案方式では、x_i が $O(N^{1/2})$個であるため、公開鍵サイズが $O(N^{1/2})$となっている。それに伴い、証拠 w_i,の計算量も $O(N^{1/2})$に軽減される。

② Libert らの方式をベースとする構成

本研究と平行して、Crypto2012 において、Libert らは効率的なメンバー失効法を提案している。この方式では、公開鍵サイズ O(log N)、秘密鍵サイズ O(1)、署名・検証コスト O(1)を達成している。しかし、失効リストサ

イズが失効数×定数となるが、定数部分がセキュリティパラメータに依存した署名長サイズとなるため、失効リストサイズも大きくなってしまうという問題がある。この方式では､失効メンバーの ID をビット列で表現し、各ビットの論理式を証明することにより、失効リスト中の各失効メンバーでないことを証明している。失効メンバー毎にその ID 情報の正当性を証明するためのディジタル署名を生成し、それを失効リストとしていることから、失効リストサイズが増加してしまう。本研究では、失効リストサイズの軽減する方式を実現するための手法について構築する。複数の失効情報をアキュームレータと呼ばれる技術により単一データにまとめ、署名することにより、失効リストの圧縮を行なう。このために、従来のアキュームレータの拡張を行ない、メンバーに割り当てた属性情報の CNF 論理式を単一のアキュームレータ情報により匿名で証明できるようにする。

(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、安全性の前提として、利用するアキュームレータやディジタル署名方式の安全性を仮定する。これらの安全性は解くことが困難と一般的にみなされている数学的問題に帰着されることが示されている。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することにより、前提としている方式が攻撃できることを示す。

(4) ペアリングの高速実装

本研究では、将来の安全性のことも踏まえ、楕円曲線暗号 200 ビット以上､ペアリング暗号を 2000 ビット以上で実現することを考え、それにもっとも適したものとして、埋め込み次数 12 の Barreto-Naehrig (BN) 曲線を用い、本研究のグループ署名に最適化した代数計算ライブラリを実装する。具体的に主として必要となるのは、拡大体と呼ぶ代数系における種々の演算（乗算など）、楕円曲線暗号におけるスカラー倍算（2 つの有理点群）、そしてペアリング計算になる。これまでに得られている成果および代数計算ライブラリをベースとしながら、本研究のグループ署名に対して改良、最適化することにより、更なる高速化を実現する。

(5)プロトタイプ実装

構築した方式の各処理を、(4)のライブラリを用いて実装し、性能評価を行なう。

(6) Webシステムへの実装

グループ署名による匿名認証の有用性を明かにするために、Web システムのミドルウェアとして実装し、具体的なアプリケーションにより有用性を示す。

４．研究成果

(1) Camenisch らの方式に対する拡張

Camenisch らの方式の問題であった O(N)の公開鍵サイズを、$O(N^{1/2})$に軽減した方式を構築し提案した。また、プロトタイプ実装を行ない、CPU: Intel Core2Duo E8400 の PC において署名・検証時間の測定を行なった。その結果を表 1 に示す。

表 1：署名・検証時間の比較

	署名時間	検証時間
従来法	84ms	133ms
提案法	178ms	258ms

この表から分かるように、従来方式と比較して、2 倍程度のオーバーヘッドがあるものの十分実用的な時間であることが確認できた。

公開鍵サイズの比較を図 1 に示す。この図から分かるように、メンバー数 50 万であっても、公開鍵サイズが 100KB に削減されており、従来方式と比較して十分に実用的であることが確認できた。

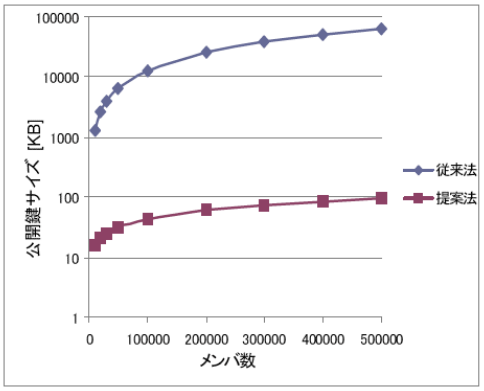

図 1：公開鍵サイズの比較

(2) Libert らの方式に対する拡張

Libert らの方式を拡張するために､属性の CNF 式を証明可能な匿名属性認証方式が必要となる。従来論理式を証明可能な方式が提案されていたが、証明データ作成時に証明する属性数に依存する計算量を必要としてしまう。本研究では、論理式中の AND の数のみに依存したべき乗計算量で十分な方式を提案した。これにより効率的に論理式を証明可能となる。その有効性を確認するため、Web シ

ステムとして認証プロトコルを実装し、属性数を変化させながら認証時間を測定した。その結果より、属性数が 1000 程度になっても 1 秒程度で動作することが確認でき、有用性が確認できた。これにより Libert の方式に本認証を適用した場合に実用的な時間で処理できることが期待できる。適用した方式の構築とその実装・評価は今後の課題とする。

(3) ペアリングの高速実装

上記の方式において、署名・検証時間の更なる高速化を実現するためには、これまで開発してきた代数計算ライブラリに含まれるペアリング計算の更なる高速化も重要となる。近年の研究で、ペアリング計算の高速化手法として、Devegili らによってツイスト曲線を用いた高速化手法が、Aranha らや光成らによって sparse multiplication 手法が提案されている。しかし、これらの手法は適用条件が異なるため、両立できない。そこで本研究では、独自の sparse multiplication 手法を提案することで、Devegili らの手法と sparse multiplication 手法の両立を達成した。上記以外にも、ペアリング計算に対して、Karabina が提案している Grobner 基底を応用した最終べきを組み込み、代数計算ライブラリ自身を 64 ビット PC に対応させた。その結果、ペアリング 1 回の計算を表 2 に示す時間で実行可能になった。

表 2：ペアリング計算の時間比較

	実装環境	計算時間
適用前	CPU: Pentium4 3.06GHz	9.9ms
適用後	CPU: Core2 Duo 2.66GHz	1.4ms

表 2 の結果は実装環境の異なるデータであるものの、本研究において、十分なペアリング計算の高速化が達成できているといえる。上記高速化手法の適用前後における署名・検証時間の評価については今後の課題とする。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計　13 件）

① 池太大貴, 中西透, 舩曳信生, ” アキュームレータを用いた失効可能グループ署名方式の公開鍵サイズの低減,” コンピュータセキュリティシンポジウム 2010(CSS2010), 2010 年 10 月 21 日, 岡山コンベンションセンター（岡山県）.

② 矢野真也, 中西透, 舩曳信生, ” プロキシを用いた匿名認証システムのユーザ登録機能及び追跡機能の実装,” コンピュータセキュリティシンポジウム 2010(CSS2010), 2010 年 10 月 20 日, 岡山コンベンションセンター（岡山県）.

③ 池太大貴, 中西透, 舩曳信生, ” 匿名属性認証における効率的な範囲証明プロトコルの提案,” 電子情報通信学会, ISEC 研究会, 2011 年 12 月 14 日, 機械振興会館（東京都）.

④ 野村智也, 中西透, 舩曳信生, ”管理者に対して強固な秘匿性を持つ評価システムの提案,” 電子情報通信学会, ISEC研究会, 2011 年 12 月 14 日, 機械振興会館（東京都）.

⑤ 森佑樹, 根角健太, 野上保之, “BN 曲線を用いたペアリングのNTLによるiPhone 実装,” The 29th Symposium on Cryptography and Information Security (SCIS 2012), 2012 年 1 月 30 日, 金沢エクセルホテル東急（石川県）.

⑥ Yuki Mori, Taichi Sumo, Kenta Nekado, Yasuyuki Nogami, Satoshi Uehara, “Memory Saving Implementation of Pollard,” The 27th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC2012), 2012 年 7 月 15 日, 札幌コンベンションセンター（北海道）.

⑦ 河野祐輝, 根角健太, 森佑樹, 有井智紀, 野上保之, “BN曲線におけるG_2上のρ法に関する効率的な代表元決定法,” 電子情報通信学会, 情報理論研究会, 2012 年 7 月 19 日, 豊田工業大学（愛知県）.

⑧ Nasima Begum, Toru Nakanishi, Nobuo Funabiki, “Efficient Proofs for CNF Formulas on Attributes in Pairing-Based Anonymous Credential System,” 電子情報通信学会, ISEC研究会, 2012 年 7 月 20 日, 北海道工業大学（北海道）.

⑨ 有井智紀, 根角健太, 野上保之, “ツイスト曲線上の有理点に対する有理点ノルムの性質とRho法への応用,” コンピュータセキュリティシンポジウム 2012(CSS2012), 2012 年 10 月 23 日, くにびきメッセ（島根県）.

⑩ 濱田雄治, 中西透, 渡邊寛, 舩曳信生, “CNF式に対する匿名属性認証システムのWeb実装,” 電子情報通信学会, ISEC 研究会, 2012 年 11 月 22 日, 静岡市産学交流センター（静岡県）.

⑪ Nasima Begum, Toru Nakanishi and Nobuo Funabiki: Efficient Proofs for CNF Formulas on Attributes in Pairing-Based Anonymous Credential System, Proc. 15th Annual International Conference on Information Security and Cryptology (ICISC 2012), Lecture Notes in

Computer Science, Vol.7839, Springer-Verlag, pp. 495-509, 2012年11月30日, Konkuk Univ.(韓国).

⑫ Nasima Begum, Toru Nakanishi, Nobuo Funabiki, “Implementation and Evaluation of an Pairing-Based Anonymous Credential System with Constant-Size Proofs and Efficient Proof Generations,” 3rd International Workshop on Advances in Networking and Computing (WANC2012), 2012年12月6日, 沖縄県男女共同参画センター(沖縄県).

⑬ 森佑樹, 赤木晶一, 根角健太, 野上保之, “BN 曲線を用いたペアリングのGMPによるiPhone 実装,” The 30th Symposium on Cryptography and Information Security (SCIS 2013), 2013年1月23日, ウェスティン都ホテル京都（京都府）.

６．研究組織

(1)研究代表者

中西　透（TORU NAKANISHI）

岡山大学・大学院自然科学研究科・准教授

研究者番号：50304332

(2)研究分担者

舩曳 信生（NOBUO FUNABIKI）

岡山大学・大学院自然科学研究科・教授

研究者番号：70263225

野上 保之（YASUYUKI NOGAMI）

岡山大学・大学院自然科学研究科・准教授

研究者番号：60314655