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２４年 ４月１９日現在

機関番号：１５３０１
研究種目：基盤研究（Ｂ）
研究期間：2009～2011
課題番号：21300004
研究課題名（和文）
ユビキタス環境における実用的な組織間匿名認証の研究開発およびその実証検証
研究課題名（英文）
Development of a Practical Inter-organization Anonymous Authentication under Ubiquitous Environment and its Experimental Study

研究代表者
森川　良孝（MORIKAWA　YOSHITAKA）
岡山大学・大学院自然科学研究科・教授
研究者番号：30033252

研究成果の概要（和文）：
無線 LAN などネットワークを用いるサービスでは、正規ユーザの特定と不正アクセスの防止が不可欠であり、個人情報の保護も要求される。本研究では、大学間無線 LAN ローミングを想定し、高度かつ複雑な匿名認証機能を要求する組織間ネットワーク連携の実現に向けて、楕円ペアリング暗号をベースとした匿名認証技術などセキュリティ要素技術の研究開発および実際に用いることを想定したネットワークプロトコルの開発およびその実証検証を行った。

研究成果の概要（英文）：
This study first researched an efficient anonymous authentication technique based on elliptic curve pairing cryptography. Then, a network protocol based on the anonymous authentication was designed and its practicality was successfully examined. The result of this study will be applied to an advanced but complicated inter-organization network cooperation that requires anonymous authentication such as the wireless LAN roaming between universities.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	3,000,000	900,000	3,900,000
２０１０年度	2,500,000	750,000	3,250,000
２０１１年度	2,300,000	690,000	2,990,000
総　計	7,800,000	2,340,000	10,140,000

研究分野：工学
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：匿名認証, グループ署名, 楕円曲線, ペアリング, UPKI, ネットワークサービス

１．研究開始当初の背景

無線LAN・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いる。いつでも、どこからでもインターネット上のサービスへのアクセスが可能となってきており、とりわけ誰でもがアクセス可能な環境においては、認証技術による正規ユーザの特定、不正アクセスの防止が必要不可欠である。しかしながら、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ユーザ認証では、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となり、プライバシ問題を引き起こす恐れがある。例えばUPKI（University Public Key Infrastructure：https://upki-portal.nii.ac.jp/）のような大学間ネットワーク連携においては、ネットワークに接続することによるユーザへのサービスの提供を大学の壁を越えて実現したいその一方で、アクセスしたユーザの個人情報をアクセスが発生した組織自身が、そのユーザのID・パスワードなどに付随する個人情報まで含めて厳密に管理することは極めて面倒であり、加えてそのような個人情報が各組織に対してアクセス履歴などの形で残りうるということは、まさにプライバシ漏洩の危険性が非常に高まるということに直結するものである。このような背景から、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が解決できる（この際、匿名での不正なサービス利用を防止できなければならないが、グループ署名では、特定の管理者のみは署名者を特定できるため問題とならない）。しかしながら、よく知られているようにグループ署名技術は、難解な数学理論を用いているため、複雑で計算時間の掛かる暗号化処理が必要となる。この結果、快適な処理時間をもって実用に供するような認証システムの実現には至っていない。

このグループ署名による匿名認証の実用化に向けて我々のグループでは、楕円曲線暗号およびペアリングと呼ぶ双線形写像を利用した匿名認証基盤の研究プロジェクトを進めてきた(総務省受託研究SCOPE若手ICT)。この研究プロジェクトでは、その実現に必須となる双線形性を有するペアリングと呼ぶ写像および楕円曲線暗号の高速化を達成し、それをベースとしてペアリング計算を利用したグループ署名方式に対してユーザ失効を効率的に実現することを目的としており、すでに世界最高速レベルの認証処理を実現している。本研究開発では、これをユビキタス環境における無線LANプロトコルなどに搭載して、ネットワークアプリケーションにおける高度な匿名認証技術の実現のために活用する。

２．研究の目的

前述のような研究背景のもと、本申請の研究期間においては、以下に示す幾つかの課題の解決、機能の拡張を達成し、UPKIにおける大学間無線LANローミングのように高度な匿名認証機能を必要とするような、組織間ネットワーク連携の実現に向けての要素技術の研究開発および実際に用いることを想定した実証検証を行う。

(1) ベースとなるペアリング処理の実装および高速化

① ペアリングフレンドリ曲線の生成

本研究開発で実装するグループ署名では、素数位数のペアリングフレンドリと呼ばれる楕円曲線（ペアリングと呼ぶ双線形写像を実現する特殊な楕円曲線のこと）に加えて、大きな素数の積で与えられる合成数位数のペアリングフレンドリ曲線を用いてペアリングおよび楕円曲線暗号を実装する必要がある。そのため、そのような特殊な楕円曲線の組織的な構成法を新たに考案し、その生成アルゴリズムを開発する。

②合成数位数ペアリングフレンドリ曲線によるペアリング計算および楕円曲線暗号の高速化

「ペアリング」の上位層に位置するグループ署名技術においては、楕円曲線暗号における暗号化の処理やペアリング計算を数多く必要とする。これまで、素数位数のペアリングフレンドリ曲線を用いたペアリング計算処理および楕円曲線暗号における暗号化などの処理の高速化については、世界最高速レベルを達成しており、その際に得られた知見やテクニックを援用する。今回ターゲットとする合成数位数ペアリングフレンドリ曲線に対しても数学理論に基づく（高速化手法の開発）研究を行い、それに基づいてペアリング計算処理および楕円曲線暗号における暗号化処理の効率の良い計算アルゴリズムを開発する。

(2) グループ署名方式の安全性の向上と高機能化

① 鍵漏洩に対して安全な方式への拡張

従来のグループ署名方式では、ユーザの秘密鍵の秘匿性に依存しているため、秘密鍵が漏洩すると、なりすましが可能となってしまう。一方通常の署名方式においては、秘密鍵を更新することにより、鍵漏洩時でも漏洩以前の期間の秘密鍵により署名した情報の正当性は保証される方式(forward-secure方式)が提案されている。しかし、グループ署名は複雑なアルゴリズムとなっており、実用的なforward-secure方式は存在していなかった。本研究では、階層型IDベース暗号における鍵更新の考え方を基にし、forward-secure方式の実現を目指す。

②複雑なアクセス制御方式への拡張

従来のグループ署名方式では、署名からある特定のグループに所属していることのみを確認する。一方で、ユーザの属性情報(性別、年齢、身分、所属チームなど)に応じて、細かなアクセス制御を行ないたい場合も多い。例えば、大学間での認証において、((A学部∨B学部)∧教員)∨事務部 のような、属性に応じた複雑なアクセス制御が考えられる。このような背景に対して、属性に基づいた論理関係(論理積や論理和)を、それ以上のプライバシ情報を明らかにすることなく保証するようなグループ署名方式の研究が現在盛んになってきている。しかし従来、短署名長を実現する効率的なペアリングベース方式が提案されていない。本研究では、効率的に属性認証可能なグループ署名方式の実現を目指す。

(3) 大学間無線LANローミングの認証基盤への応用

① 認証手順の設計

UPKIにおける大学間無線LANローミングの認証基盤として、IEEE802.1Xを用いたユーザ認証が検討されている。しかしながら、通常のIEEE802.1Xを用いたユーザ認証では、アクセスしたユーザの個人情報がローミング先の認証サーバにアクセス履歴の形で残りうることになり、プライバシ保護の観点からは望ましくない。本研究では、この問題の解決に向けて「グループ署名による匿名認証の技術」を「大学間無線LANローミングの認証基盤」へ応用するため、グループ署名を利用した無線LANの認証手順を設計する。

② 実証実験

大学間無線LANローミングのための匿名認証基盤の実現に向けて、(3)-①で設計した認証手順を実装した実証実験を行う。ここでは、実証実験を通じて実用面での課題を発見し、他の研究パートにフィードバックするとともに、最終的に本研究課題の実用性を証明する。

３．研究の方法

以下、各技術レイヤーでの具体的な研究開発内容について、それぞれ具体的に述べる。

(1) ペアリング実装

①ペアリングフレンドリ曲線の生成

本開発では、素数位数のみならず合成数位数のペアリングフレンドリ曲線も必要となる。そのため、非超特異に加えて超特異と呼ぶクラスの楕円曲線も含めて、その組織的な生成法について研究開発を行う。また、その生成には多くの計算時間を要するため、パラメータの改良を行い、生成にかかる計算処理の高速化を図る。

②ペアリング、楕円曲線暗号高速化

本研究開発では、合成数位数のペアリングに対して、ペアリングや楕円スカラー倍算な

どの計算処理の高速化が必要となる。そのため本研究開発では、数学理論に基づきながら、まずペアリング計算の高速化について研究開発を行う。続いて、合成数位数という特徴に基づいた楕円曲線暗号の高速化について研究開発を行う。そして最後に、安全性評価のための攻撃手法の検討を行う。

(2) グループ署名方式の安全性の向上と高機能化

①鍵漏洩に対して安全な方式への拡張

ペアリングを用いた階層型 ID ベース暗号が登場し、木構造においてルートの秘密鍵から子孫方向へ順々に安全に各ノードに対応した秘密鍵を生成できるようになった。この生成方法をグループ署名でのユーザの秘密鍵更新方法に適用することにより、forward-secure 方式を実現できる。このとき、階層型 ID ベース暗号と同様の秘密鍵の構造をもつグループ署名方式を利用することにより適用が可能となる。

② 複雑なアクセス制御が可能な方式への拡張

グループ署名における所属証明書に属性値を含ませ、AND 関係や OR 関係を証明可能なゼロ知識証明により、匿名属性認証が実現できる。しかしこの場合、証明効率が属性数に依存する問題がある。本研究では、ペアリングベースのアキュームレータと呼ばれる、複数情報の入力を１つのデータに圧縮しながら、その検証を入力数に依存せずに行なうことができる技術を適用した。これにより、RSA 仮定に依存せず短署名長を実現しながら、属性数に依存しない証明効率を達成できる。

(3) 大学間無線 LAN ローミングの認証基盤への応用

① 認証手順の設計

無線 LAN における IEEE802.1X 認証では、ユーザと認証サーバの間で認証情報を交換し、その有効性を検証することにより、認証を実施する。本研究パートでは、この認証過程において、(2)-②で実現する高度なグループ署名による匿名認証の技術を適用することにより、ユーザのプライバシ保護を実現する無線 LAN 認証手順を設計する。認証手順の設計に際しては、ユーザの所属先である組織とローミング先である組織の認証サーバ等が保持すべき機能や認証情報を綿密に設計し、匿名性を保ちつつも、不正アクセスが発生した場合には原因となったユーザを確実に特定できる機能を実現する必要がある。

② 実証実験

本研究パートでは、(3)-①で設計した認証手順を実装し、グループ署名による匿名認証の技術を用いた無線 LAN ローミングの実証実験を行う。ここでは、(3)-①で設計した認証手順が大学間無線 LAN ローミングの認証基盤として実用的な時間で認証を完了できるかどうかを確認するとともに、運用・管理面での課題に関しても検討する。本研究で得られた成果は逐一他の研究パートにフィードバックし、必要な場合には問題の改善を促す。

４．研究成果

以下、技術階層(1)、(2)、(3)のそれぞれについて、研究成果を報告する。

(1) ペアリング実装

本研究においては埋め込み次数3のある種のペアリング曲線に着目した。具体的に、埋め込み次数が3で2次位数の親和曲線に着目し、大きな合成数位数をもつように曲線を生成するアルゴリズムを新たに提案した。従来の1次位数の曲線の生成時間が数秒であるのに対し、提案アルゴリズムは数10分の生成時間が必要であることが明らかになった。加えて、その生成されたペアリング親和曲線を用いて、ペアリング1回の計算処理を、一般的なPCを用いても1秒をきって行えるよう改良を加えた。従来の計算手法と比べれば、こちらもおおよそ10倍の効率化が図れている結果だけ述べるが、安全性については、既存の攻撃手法およびそれを改良した手法に対し、十分な安全性をもつことを検証できている。

(2) 鍵漏洩対策および属性ベース方式

本研究では、forward-secureであるグループ署名を提案した。これにより、ある時点においてユーザの秘密鍵が漏洩したとしても、それ以前の署名についてはなりすましができず、安全性が維持される。さらに本研究では、属

性に基づいた論理関係(論理積や論理和)を、それ以上のプライバシ情報を明らかにすることなく保証するようなグループ署名方式の提案も行った。提案方式は、従来のRSAベース方式と比較して短署名長が実現されているとともに、必要なべき乗演算回数が属性数に依存せず、高速である。

(3) 大学間無線LANローミングの認証基盤への応用

本研究においては、組織間連携を考慮した匿名IEEE802.1X認証システムを提案・実装した。組織間連携を考慮した方式では、ユーザが所属する組織を事前に把握する必要があるため、ある組織への所属を証明するディジタル証明書（組織証明書）を用いてこれを実現する方式を提案した。また、実運用を考慮した検討を重ねた結果、各組織における統合認証サーバとの円滑な連携が必須と考え、大学間連携を考慮した統合認証サーバとして実績のあるShibbolethシステムとの連携を実現するシステムを提案・実装した。これらの機能を岡山大学で実際に運用中のネットワークシステムや無線LANシステムと連携させ、実環境での正常な動作および本システムの有用性を確認した。

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）

〔雑誌論文〕（計5件）

[1]A. Sudarsono, T. Nakanishi, N. Funabiki, “An Implementation of a Pairing-Based Anonymous Credential System with Constant Complexity,” Proc. IAENG ICCSA 2011, 査読有, 2011.

[2]A. Sudarsono, T. Nakanishi, N. Funabiki, “Efficient Proofs of Attributes in Pairing-Based Anonymous Credential System,” Proc. PETS 2011, 査読有, LNCS 6794, pp.246-263, 2011.

[3]T. Nakanishi, Y. Hira, N. Funabiki, “Forward-Secure Group Signatures From Pairings,” Proc. Pairing2009, 査読有, LNCS 5671, pp. 171-186, 2010.

[4]Y. Nogami, K. Nishii, Y. Sakemi, H. Kato, Y. Morikawa, “How to Generate a Secure Composite Order Ordinary Pairing-friendly Curve of Embedding Degree 3,” ITC-CSCC 2009, 査読有,2009年7月8日(韓国ソウル).

[5]T. Nakanishi, Y. Hira, N. Funabiki, “Forward-Secure Group Signatures From Pairings,” IEICE Trans. Fundamentals, 査読有, vol.E93-A, No.11, pp. 2007- 2016, 2010.

〔学会発表〕（計15件）

[6]河野, 中西, 佐藤, 濱田, 堀地, “大学ネットワークにおける匿名 IEEE802.1X 認証システムの実装,”電子情報通信学会総合大会, 2012年3月22日(岡山).

[7]濱田, 中西, 舩曳, “Web サービスにおける匿名属性認証システムの実装,”コンピュータセキュリティシンポジウム 2011 (CSS2011), 2011年10月19日(新潟).

[8]森, 角力, 野上, 松嶋, 上原, “Barreto-Naehrig 曲線上のある特殊な巡回群に対する Frobenius 写像を用いた Rho 法による攻撃の実装評価,”第34回情報理論とその応用シンポジウム, 2011年12月1日(岩手).

[9]有井, 角力, 野上, 松嶋, 上原, “BW 曲線上のある特殊なねじれ群の有理点のノルムに関する一性質,”第34回情報理論とその応用シンポジウム, 2011年12月1日(岩手).

[10]A.Sudarsono, T.Nakanishi, N. Funabiki, “An Implementation of a Pairing-Based Anonymous Credential System with Constant Complexity,”電子情報通信学会ネットワークシステム研究会(NS), 2010年12月17日(岡山).

[11]佐藤, スダルソノ, 中西, 舩曳, “組織間連携を考慮した匿名 IEEE802.1X 認証プロトコルの実装,” 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).

[12]A. Sudarsono, T. Nakanishi, N. Funabiki, “Efficient Proofs of Attributes in Anonymous Credential Systems Using a Pairing-Based Accumulator,” 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).

[13]柳, 西井, 野上, 森川,“埋め込み次数 3 または 4 かつ合成数位数をもつ非超特異ペアリングフレンドリ曲線生成法の比較,”2010 年暗号と情報セキュリティシンポジウム(SCIS2010), 2010 年 1 月 22 日(高松).

[14]出田, 野上, 森川,“2000-bit 程度の合成数位数をもつ埋め込み次数 1 の非超特異ペアリングフレンドリ曲線の生成に関する実装報告,”2010 年暗号と情報セキュリティシンポジウム(SCIS2010), 2010 年 1 月 22 日(高松).

[15]竹内, 出田, 酒見, 西井, 野上, 森川,“埋め込み次数 1 の非超特異ペアリングフレンドリ曲線上での GLV 法の適用,”電子情報通信学会情報セキュリティ研究会(ISEC), 2009 年 12 月 16 日(東京).

[16]西井, 竹内, 湯浅, 柳, 酒見, 野上, 森川,“埋め込み次数が 4 かつ合成数位数の非超特異ペアリングフレンドリ曲線の生成,”第 32 回情報理論とその応用シンポジウム(SITA2009), 2009 年 12 月 2 日(山口).

[17]藤井, 中西, 舩曳,“ペアリングを用いた効率的な属性ベースグループ署名方式の提案,”電子情報通信学会情報セキュリティ研究会(ISEC), 2009 年 11 月 12 日(岐阜).

[18]出田, 酒見, 西井, 竹内, 野上, 森川,“埋め込み次数 1 の非超特異ペアリングフレンドリ曲線を用いた Tate ペアリングの実装,”電子情報通信学会情報セキュリティ研究会(ISEC), 2009 年 9 月 25 日(東京).

[19]酒見, 西井, 出田, 湯浅, 野上, 森川,“二つの大きな素因数を含む合成数位数をもつ非超特異ペアリングフレンドリ曲線を用いたクロスツイスト Ate ペアリングの高速化,”電子情報通信学会情報セキュリティ研究会(ISEC), 2009 年 7 月 3 日(東京).

[20]西井, 酒見, 野上, 森川,“2 つの大きな素因数を含む合成数位数をもつ非超特異ペアリングフレンドリ曲線の一生成法,”電子情報通信学会情報セキュリティ研究会(ISEC), 2009 年 5 月 22 日(東京).

〔その他〕

岡山大学 PRESS RELEASE (2009.10.27)
http://www.okayama-u.net/renkei/document/pdf/pressrelease/press-091027-7.pdf

2009 イノベーションジャパン(2009.9.18)
http://www.okayama-u.net/renkei/document/pdf/InnovationJapan/2009InnovationJapan5.pdf

ホームページ等
http://www.trans.cne.okayama-u.ac.jp/~nogami/Works/Kibanb.html

６．研究組織

(1)研究代表者

森川　良孝 (MORIKAWA　YOSHITAKA)
岡山大学・大学院自然科学研究科・教授
研究者番号：30033252

(2)研究分担者

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

野上　保之 (NOGAMI　YASUYUKI)
岡山大学・大学院自然科学研究科・准教授
研究者番号：60314655

岡山　聖彦 (OKAYAMA　KIYOHIKO)
岡山大学・情報統括センター・准教授
研究者番号：20252588

河野　圭太 (KAWANO　KEITA)
岡山大学・情報統括センター・准教授
研究者番号：40397899