楕円曲線暗号を用いた匿名認証基盤の研究開発（072108001）

Anonymous Authentications Using Elliptic Curve Cryptosystems

研究代表者
中西透　岡山大学 大学院自然科学研究科
Toru Nakanishi　Graduate School of Natural Science and Technology, Okayama University

研究分担者
野上保之†
Yasuyuki Nogami†
†岡山大学 大学院自然科学研究科
†Graduate School of Natural Science and Technology, Okayama University

研究期間　平成 19 年度～平成 21 年度

概要

本研究では、楕円曲線暗号に基づくグループ署名に対して、効率的なユーザ失効方法、高速な楕円曲線暗号・ペアリング計算実装を新たに実現した。そして、その認証システムを実装し、性能評価実験を行った。グループ署名による認証では、匿名のまま正規ユーザかどうかの確認を行なえるため、不正アクセス防止とユーザのプライバシ保護を両立できる。本研究の成果により、グループサイズ・失効数に依存しない署名生成・検証と、高速なペアリング計算処理が実現できるため、匿名認証基盤を実用的なレベルで実現できる。

Abstract

We researched and developed efficient user revocations and fast implementations of elliptic curve cryptosystems and pairing computations for pairing-based group signatures. Furthermore, we implemented the authentication system, and evaluate it from the experiments. Since group signatures allow us to confirm the validity of user while concealing user's ID, we can achieve network services with both security and privacy. We achieve the practical anonymous authentications by realizing the signing generation and verification with constant complexity w.r.t. the group size and the number of revocations, and by the fast pairing computations.

１．まえがき

インターネット・携帯電話網の急速な普及に伴い、いつでも、どこからでもサービスへのアクセスが可能となってきている。このとき、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、一般的な ID ベースの認証では、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ってしまう。こうして、誰がどこで何をしていたということを追跡することが可能となるため、 このようなプライバシの問題を解決することが急務となる。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。グループ署名による認証では、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るため、上記のプライバシ問題が解決できる。

グループ署名による匿名認証の実用化においては、実用的な認証時間の達成が最重要となる。従来、RSA 暗号をベースとしたグループ署名方式が提案されてきたが、2010 年を目処に鍵長が 2048 ビットに移りつつあり、通常の PC ですら実用的な時間での動作は困難となってきている。これに対して、鍵長の短い楕円曲線暗号および曲線上で構成されるペアリングと呼ばれる演算をベースとしたグループ署名方式が近年提案され、グループ署名による匿名認証の実現可能性が高まっている。しかし、「効率的なユーザ失効法」 、「ベースとなる楕円曲線暗号・ペアリングの高速実装」が実現できていないため、大規模なグループにおいて、実用的な認証時間（具体的には数秒以内）の達成が困難となっている。そこで本研究では、これらの 2 つの課題の解決を行い、それらに基づいた匿名認証システムの構築と実証実験を行った。

２．研究内容及び成果

本研究は 3 つのテーマに分割して推進した。テーマ毎に研究内容及び成果を以下に示す。

2.1 効率的なユーザ失効法

グループ署名よる認証では、ユーザは事前に管理サーバに対してユーザ登録を行い、所属証明書（電子証明書）を受け取る。グループ署名は所属証明書の所有を示すデータとなる。このため、ユーザ権限を失効する場合、この所属証明書を失効させる必要がある。しかし、署名データが匿名性を持つため、通常の PKI でのように ID ベースの失効確認ができない。そこで様々な失効手法が提案されていたが、ユーザやサーバが失効数に依存した回数の暗号処理を必要とするため、大規模なシステムでの運用は困難であった。

そこで本研究では、失効数（ユーザ数にも）に依存せず定数計算量でサーバでの処理およびユーザでの処理が可能な失効方法をもつグループ署名方式を構築した[1]。構築した方式では、ID 情報を秘匿したまま 2 つの ID 情報の比較を行える手法を用いて、認証しているユーザの ID が失効リスト中の全ての ID と異なるということを、計算量が失効数に依存することなく証明する。これにより、匿名性を維持したまま、定数計算量で失効確認が行える。

新たに構築した方式が、従来方式と同様の安全性を保持していることを保証する必要がある。このために、失効を考慮した署名データの偽造不能性および匿名性を定式的に定義した。そして、従来方式と同様の数学的困難性を仮定し、定義した安全性を満たすことを証明した。

さらに、本研究で実装した楕円曲線暗号・ペアリングラ

イブラリを用いて、署名生成・検証処理の実装を行い、その処理時間を測定した。その結果、RSA 暗号での 2048 ビット鍵長と同等のセキュリティを保証できる鍵長に設定した場合、通常の PC（CPU:Core2Duo 2.66GHz）において、署名生成・検証ともに失効数に依存することなく 200msec.程度で処理できることが確認できた。

2.2 ベースとなる楕円曲線暗号・ペアリングの高速実装

本開発で実現したいセキュリティレベルを考えたとき、もっとも効率のよい、実装に適したペアリング曲線は Barreto-Naehrig ペアリング曲線である。これに対して、本研究グループでは、TwistedAte ペアリングというペアリングを適用することを考えた。そしてこのペアリングが、我々がこれまでに提案してきているツイストペアリングの特長を加味することにより、高速な計算処理によって実現できることを示した。さらに、昨今使われるようになってきたマルチプロセッサ（Core2DuoTM など）による並列計算や、これに相当するマルチペアリング計算の導入を検討した。具体的には、TwistedAte ペアリングの計算式を、ツイストペアリングのアイデアを同じように用いて効率よく式変形できることを示し、これに対してマルチペアリングの計算手法や Frobenius 写像による効率のよい並列化ができるように工夫をした[2]。

工夫点を簡単に説明する。まずペアリング計算は、Miller のアルゴリズムに対する計算と、最終べきと呼ぶべき乗算により構成される。本研究の主たるターゲットは前者 Miller の計算であるが、このアルゴリズムの計算は、ループパラメータと呼ぶある整数パラメータの回数だけ一定の繰り返し計算を行うことが特徴であり、これに対し、重複する計算をまとめて行えるよう実装し、効率よくマルチペアリングの計算を行えるよう工夫した。そして、これを本研究のグループ署名に実装し、その効果を確認した。

2.3 グループ署名を用いた匿名認証システム

構築したグループ署名を匿名でのユーザ認証に適用するために、チャレンジ・レスポンス認証に基づいてグループ署名を用いた匿名認証プロトコルを設計した。構築した署名方式ではユーザは最新の失効リストを用いて署名データを作成する必要があるため、チャレンジ乱数を送信する際に失効リストもサーバから送信するようにしている。

そして本研究の評価実験として、**2.1** 及び **2.2** の成果を基に、Web ベースの匿名認証システムを実装した[3]。認証処理を Web ブラウザに直接組み込む場合、ペアリングライブラリを使用するためにブラウザなどを改編する必要があり、導入が容易ではない。そこで、ユーザ PC へプロキシソフトウエアを別に導入することを考えた。同様にサーバへの実装を容易化するために、サーバ側へもプロキシを導入した。匿名認証が必要な Web サービスを利用するとき、ブラウザからクライアントプロキシにアクセスする。次に、クライアントプロキシはサーバプロキシを経由して Web サーバへ通信を行う。そのとき、提案グループ署名方式による匿名認証を行い、認証に成功した場合、Web サーバから Web コンテンツがブラウザまで各プロキシを経由して送信される。匿名認証プロトコルは、SSL 通信路を張った後、その通信路内で行われる。実装においては、各プロキシの送信処理などは Java を用いている。一方、ペアリングライブラリは高速化のため C 言語で実装されており、署名生成・検証処理も C 言語で実装している。Java から C 言語の処理部分を呼び出す際には、JNI（Java Native Interface）を利用している。

評価実験として、サーバ PC(CPU:Core2Quad 2.83GHz) を学内 LAN へ、クライアント PC(CPU:Core2Duo 2.2GHz) を学外光回線（下り 17.7Mbps、上り 9.8Mbps)にインターネットを介して接続し、実装した匿名認証プロトコルの動作時間を測定した。その結果を図 1 に示す。

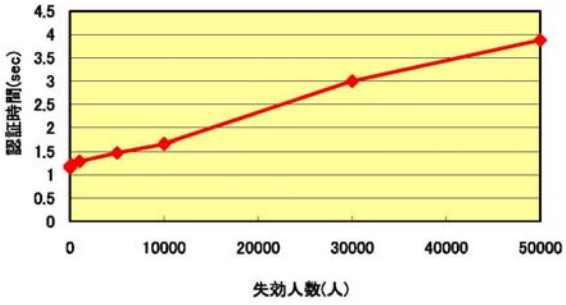

図 1 失効人数に対する認証時間の変化

上記の結果より、署名生成や検証の時間については **2.1** で述べたように失効数に依存せず数百 msec.で動作するものの、失効リストサイズの増大に伴い認証時間が増大していることがわかる。しかし、失効数が数万程度であれば数秒で認証しており十分に実用的である。

３．むすび

プライバシを保護したユーザ認証を実現するために、効率的なユーザ失効法をもつグループ署名方式及び高速な楕円曲線暗号・ペアリング実装を実現した。実証実験として、これらを用いた Web ベースの匿名認証システムを実装した結果、失効数が数万程度であっても数秒程度で認証処理が完了し、十分実用的であることが確認できた。

【誌上発表リスト】

[1]Toru Nakanishi, Hiroki Fujii, Yuta Hira and Nobuo Funabiki, “Revocable Group Signature Schemes with Constant Costs for Signing and Verifying,” Proc. PKC2009, LNCS 5443, pp. 463-480 (2009 年 3 月 20 日)

[2]Yumi Sakemi, Hidehiro Kato, Yasuyuki Nogami, Yoshitaka Morikawa, ”An Improvement of Twisted Ate Pairing with Barreto-Naehrig Curve by using Frobenius Mapping”, Proc. of ICCIT08, vol. 2, pp. 406-410 (2008 年 11 月 12 日)

[3]Toru Nakanishi, Hiroki Obayashi, Nobuo Funabiki: “An Implementation of Anonymous Authentication System for Web Services Using Proxies,” Proc. IEEE ISCE2009, pp.179-181 (2009 年 5 月 26 日)

【申請特許リスト】

[1]野上保之、酒見由美、森川良孝、スカラ倍算装置、スカラ倍算方法、及びスカラ倍算プログラム、日本、2008 年 11 月 28 日

[2]野上保之、酒見由美、森川良孝、スカラ倍算器及びスカラ倍算プログラム、全ての国、2009 年 11 月 30 日

【本研究開発課題を掲載したホームページ】

http://www.sec.cne.okayama-u.ac.jp/~nakanisi/research/SCOPE.html