様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 ３０ 日現在

機関番号：１５４０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０１５３

研究課題名（和文）モバイル環境に適した匿名認証の提案とその実装

研究課題名（英文）Proposal and Implementation of Anonymous Authentications Suitable for Mobile Environment

研究代表者
中西　透（Nakanishi, Toru）

広島大学・工学（系）研究科（研究院）・教授

研究者番号：５０３０４３３２

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：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。従来の匿名認証方式では、運用上必要となる機能である、ユーザ失効、匿名不正者排除については、大規模なシステムにおいて大きなデータ量もしくは処理時間を必要とする問題があった。本研究では、モバイル環境に適した匿名認証を実現するために、効率的なユーザ失効、効率的な匿名不正者排除の方式の構築を行なった。

研究成果の概要（英文）：By anonymous authentications, a user can be anonymously authenticated, and thus the privacy of users is protected. In conventional anonymous authentication schemes, large data size and large processing time are required for user revocation and excluding anonymous dishonest users. In this study, to realize practical anonymous authentications in mobile environment, we have constructed efficient schemes for the user revocation and excluding anonymous dishonest users.

研究分野：情報セキュリティ

キーワード：プライバシ保護　認証

１．研究開始当初の背景

近年の IoT 技術の発展に伴い、どこからでもインターネットへのアクセスが可能となってきているが、その際，認証技術を用いた不正アクセス防止が必要である。しかし、一般的な ID を用いた認証では、認証サーバに、誰が、いつ、どこから、どのようなサービスを利用したかといったアクセス履歴が残ることになる。IoT 環境では、このような情報がいたるところで収集され蓄積されるため、プライバシが問題となる。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、予めサーバにグループのメンバーとして登録しておく。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、匿名認証をネットワークサービスに適用した際に運用上必要となる機能である、ユーザ失効、匿名不正者排除については、大規模なシステムにおいて大きなデータ量もしくは処理時間を必要とする。

ユーザ失効とは、ユーザをグループから離脱させることを意味し、サービスでの認証の場合、サービスから脱会する場合や秘密鍵を紛失したときなどに必要となる。認証が匿名となるため、失効ユーザかどうかの確認は容易ではない。そこで従来多数のユーザ失効方式が提案されていたが、ユーザ数 N や失効数 R が大きくなった場合に、認証処理時間や鍵サイズなどのデータ量が大きくなるという問題があった。それに対して、Libert らは Crypto2012 において、公開鍵サイズ $O(\log N)$、秘密鍵サイズ $O(1)$、認証用署名生成コストおよび検証コスト $O(1)$ となる効率的な方式を提案している。しかし、失効確認のために必要となる失効リストのサイズが、署名を各失効情報に付加するために長くなってしまうという問題がある。

匿名認証では、匿名の不正者が発生する問題があり、その不正者を排除できることが必要となる。従来、ブラックリストを用いることにより匿名不正者を排除可能な認証方式が提案されている。しかし、ブラックリストサイズや不正検出可能期間を示すウィンドウサイズに比例したべき乗演算を必要とするため、認証に時間を要する問題がある。

こうして、通信性能や処理性能が比較的貧弱であるモバイル環境では、匿名認証の実用化は容易でない。

２．研究の目的

そこで本研究では、モバイル環境に適した匿名認証を実現するために、効率的なユーザ失効、効率的な匿名不正者排除の構築・実装を目的とする。

具体的には、ユーザ失効については、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目指す。

匿名不正者排除については、べき乗演算回数がブラックリストサイズやウィンドウサイズに依存しない匿名不正者排除をもつ方式を提案する。提案する方式では、同様にアキュームレータを用いて複数のタグ情報をまとめることを考える。

３．研究の方法

(1)効率的なユーザ失効をもつ方式の構築

失効法のベースとしては、Libert らの方式(LPY12)を用いる。この失効法では、2 分木 T を考え、各ユーザを葉に割り当てる。ユーザを失効する場合、対応する葉ノードをマークする。このとき、非失効ユーザの集合は、この 2 分木 T の部分木である SD 木の集合として表現できる。SD 木 $S(i,j)$ では、2 つのノード v_i, v_j (v_i は v_j の先祖ノード)により定義され、v_j をルートとする部分木の葉ノードのユーザは全て失効されているが、それらを除いて、v_i をルートとする部分木の葉ノードのユーザは全て失効されていない。

失効数 R に対して、$O(R)$ 個の SD 木に二分木 T は分割されることが知られている。このとき、LPY12 の方式では、現在の失効状況に対して、各 SD 木にグループ管理者が署名をし、失効リストとして発行する。各ユーザは、署名する際に、自身の葉ノードが含まれる SD 木 $S(i,j)$ を選び、「自身の葉ノードのある先祖ノードが v_i であることと、ある先祖ノードが v_j でないこと」を示す。これにより、この葉ノードは $S(i,j)$ に含まれることが示され、非失効ユーザであることを示せる。この証明は、ゼロ知識証明を用いて行なうため、どの SD 木に含まれるか、どのノードが先祖ノードであるかといった情報は秘匿され、匿名性が満される。しかし問題として、失効リストでは、各 SD 木に対して署名を生成する必要があり、署名は安全性のため比較的大きな長さを取るため、1.で示したようにモバイル環境で問題となる。

本研究では、以下の着想に基づいて、失効リストの削減を行なっている。 LPY12 方式への適用において、二分木の深さ k での左へ向う辺を $(k,0)$、右へ向う辺を $(k,1)$ であらわす。ノード v_j のビット表現を $(v_{j1},\ldots,v_{jw})$ とすると、ノード v_i は v_j の先祖ノードであるため、v_i を深さ t のノードとすると、v_j のビット表現の先頭 t ビットは一致する。このとき、「自身の葉ノードのある先祖ノードが v_i であることと、ある先祖ノードが v_j でないこと」を、論理式 $(1,v_{j1})\wedge\cdots\wedge(t,v_{jt})\wedge((t+1,\neg v_{jt+1})\vee\cdots\vee(w,\neg v_{jw}))$ として表現できる。一方、本研究グループで提案しているアキュームレータの利用を考える。このアキュームレータでは、和積標準形の論理式を検証でき、そのゼロ知識証明も構成できる。その計算量は論理式の長さに依存しない。こうして、このアキュームレータを使用することにより、グループサイズや木の高さに依存

せず効率的に検証が可能となる。

（2）効率的なユーザ失効をもつ方式の改良
（1）で構成した方式では、利用しているアキュームレータの制約のため、ユーザが登録時にサーバから配布される証明書のサイズがO(1)からO(log N)に増加してしまう問題がある。そこで、アキュームレータに類似した暗号技術であるベクターコミットメントと呼ばれる手法を採用することにより、O(1)の証明書サイズを維持したまま、失効リストを圧縮する。基本的なアイデアは、複数のSD木のv_i,とv_jのID情報それぞれをベクターコミットメントで圧縮して署名を付与している。ベクターコミットメントは、元のLPY12方式で利用されているものであり、そのまま適用できるために、証明書サイズの増大を防いでいる。

（3）効率的な匿名不正者排除方式の構築
各認証セッションには、認証サーバが選んだ、ランダムな自然数をセッション番号として割り当てる。ユーザの証明書には、そのユーザの過去のセッション番号を埋め込む。べき乗演算回数がセッション数に依存しないように、アキュームレータにより一つの値に乗算を用いて変換し埋め込む。公開するリストは、不正ユーザの認証を除いた全てのセッションの番号をアキュームレータにより変換した値となる。すなわち、ホワイトリストが公開されることになる。アキュームレータの検証式により、ブラックリストサイズに依存しない処理時間で、ユーザのすべてのセッション番号がホワイトリストに載っていることを検証でき、不正者でないことを検証できる。

４．研究成果
（1）効率的なユーザ失効をもつ方式の構築
失効リストサイズを軽減した失効可能グループ署名方式を提案した。LPY12の方式との失効リストサイズ、公開鍵サイズ、証明書サイズの比較を表１に示す。

表１：各データサイズの比較

	LPY12	提案方式
失効リストサイズ	$512\cdot 7\cdot\lceil 2R-1\rceil$	$512\cdot 8\cdot\lceil (2R-1)/T\rceil$
公開鍵サイズ	$2\cdot 512\cdot\log N$	$2T\sqrt{T}\cdot 512\cdot\log N$
証明書サイズ	$9\cdot 512$	$8\cdot 512\cdot T$

ここで、Nはユーザの総数、Rは失効ユーザ数、Tは圧縮数であり、AES128 ビットと同等の安全性とするために楕円曲線暗号の各値のサイズを 512 ビットとしている。表１から分かるように、提案方式では従来方式の約$1/T$に失効リストサイズが軽減されている。一方でそのトレードオフとして、公開鍵サイズは約$T\sqrt{T}$倍に、証明書サイズは約T倍に増大している。
具体的に圧縮できるサイズとオーバヘッドが実用的にどの程度となるかを明らかにするために、具体的なパラメータを代入して考察した。$N=1{,}000{,}000$、$R=100{,}000$のときの失効リストサイズを表２に示す。

表２：具体的な失効リストサイズの比較

	LPY12	提案方式 ($T=49$)	提案方式 ($T=100$)
失効リストサイズ	$88{,}000KB$	$2{,}100KB$	$1{,}000KB$

従来方式では80MB程度であったが，$T=49$の圧縮度でも2MB、$T=100$の場合は1MB程度まで軽減できており、実用的に十分な効果があることがわかる。表３に、このときの公開鍵サイズと証明書サイズを示す。

表３：具体的な公開鍵・証明書サイズの比較

	LPY12	提案方式 ($T=49$)	提案方式 ($T=100$)
公開鍵サイズ	$2.6KB$	$860KB$	$2{,}500KB$
証明書サイズ	$0.20KB$	$25KB$	$50KB$

この表から、従来方式よりは各サイズが増大するものの深刻な問題とは成らないことが分かる。

（2）効率的なユーザ失効をもつ方式の改良
ベクターコミットメントを用いてオーバヘッドの改良を行った。(1)の方式の公開鍵サイズが$O(T\sqrt{T}\log N)$に対して、改良方式では$O(T+\log N)$となっている。また、証明書サイズは$O(T)$から$O(1)$に改善できている。この改良では、署名生成・検証時間の具体的な比較が必要であるが、その詳細な比較は今後の課題としている。

（3）効率的な匿名不正者排除方式の構築
アキュームレータを用いることにより、ブラックリストサイズに依存しない認証処理時間を実現した不正排除方式を提案した。提案方式では、ブラックリストではなくホワイトリスト(不正でないセッションIDのリスト)を利用している。提案方式の認証処理で必要となるべき乗演算(およびそれより高コストの演算)の回数は、ホワイトリストのサイズに依存していない。
提案方式の有効性を確認するため、多倍長計算ライブラリ(GMP)上で実装されているペアリングライブラリを用いて、PC上で実装し、認証処理時間の計測を行なった。計測は、CPU: Intel Core i5-4460(3.20GHz),Memory:8GB,OS:Ubuntu Linux 14.04の環境で行なっている。その測定結果を図１に示す。
図１から分かるように、従来方式では、失効数に依存して、ブラックリストサイズ(|BL|)が増大するために、認証時間も比例し

て増加しており、失効数が 500 のとき認証時間は 2 秒程度まで増加してしまう。

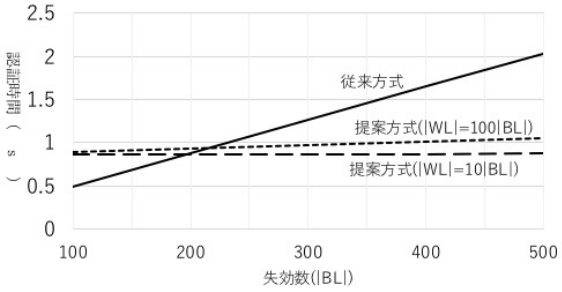

図 1:従来方式との認証時間の比較

提案方式はホワイトリストサイズ(|WL|)に依存するため、|WL|=10|BL|, |WL|=100|BL|の場合について測定を行なった。いずれの場合も失効数の増大に対して、認証時間がさほど増大しておらず、失効数 500 の場合でも 1 秒程度で収まっている。このことから、実用的なレベルで提案方式が十分に有効であることを確認できた。

匿名認証をモバイル環境で行なうシステムの開発も行なっており、その上での提案方式の評価は今後の課題である。また補助的な研究として、アキュームレータにより証明可能な論理式を CNF 式から任意のモノトーン論理式となるような方式の拡張も行なっており、これにより本方式やユーザ失効法をさらに効率化できる可能性がある。その拡張は今後の課題である。

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）

〔雑誌論文〕（計　1　件）

1. Toru Nakanishi, Nobuo Funabiki, “Revocable Group Signatures with Compact Revocation List Using Accumulators,” IEICE Trans. Fundamentals, 査読有, Vol.E98-A, No.1, pp.117-131, January 2015.

〔学会発表〕（計　１０　件）

1. Shahidatul Sadiah, Toru Nakanishi, “Revocable Group Signatures with Compact Revocation List Using Vector Commitments,” SCIS2016, 1E2-2, 2016 年 1 月 19～22 日, ANA クラウンプラザホテル熊本ニュースカイ(熊本県).
2. 愛甲悠, 中西透, “アキュームレータを用いたブラックリスト型匿名認証システムの認証時間の軽減,” 電子情報通信学会 ISEC 研究会, IEICE-ISEC2015-47, 2015 年 11 月 6～7 日, 神奈川大学(神奈川県).
3. Shahidatul Sadiah, Toru Nakanishi, Nobuo Funabiki, “Anonymous Credential System with Efficient Proofs for Monotone Formulas on Attributes,” 10th International Workshop on Security (IWSEC 2015), LNCS 9241, pp. 262-278, 2015 年 8 月 26～28 日, 東大寺総合文化センター(奈良県).
4. Nasima Begumu, Toru Nakanishi, Yasuyuki Nogami, “Reduction of Authentication Time in an Anonymous Credential System with Proofs for Monotone Formulas on Attributes,” ICCE-TW2015, 2015 年 6 月 6～8 日, National Taiwan University of Science and Technology(Taiwan).
5. Shahidatul Sadiah, Toru Nakanishi, Nobuo Funabiki, “Implementation of Anonymous Credential System with Efficient Proofs for Monotone Formulas on Attributes Excluding Restriction,” CANDAR: First International Workshop on Information and Communication Security (WICS2014), pp.531-535, 2014 年 12 月 10～12 日, グランシップ(静岡県).
6. Shahidatul Sadiah, Toru Nakanishi, Nobuo Funabiki, “Efficient Proofs for Monotone Formulas on Attributes Excluding Restriction in Anonymous Credential System,” 電子情報通信学会 ISEC 研究会, IEICE-ISEC2014-50, 2014 年 9 月 5 日, 機械振興会館(東京都).
7. Toru Mishima, Toru Nakanishi, Kan Watanabe, Nobuo Funabiki, “An implementation of mobile anonymous attribute authentication for Android devices,” 2014 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW 2014), pp. 47-48, 2014 年 5 月 26～28 日, National Taiwan Normal University(Taiwan).
8. 三嶋徹, 中西透, 渡邊寛, 舩曳信生, “Android 端末を用いたモバイル匿名属性認証システムの実装,” 情報処理学会研究報告, CSEC-64, 2014 年 3 月 6～7 日, 明治大学(東京都).
9. Toru Nakanishi, Nobuo Funabiki, “Revocable Group Signatures with Compact Revocation List Using Accumulators,” 16th Annual International Conference on Information Security and Cryptology (ICISC 2013), LNCS 8565, pp. 435-451, 2013 年 11 月 27～29 日, Konkuk university (Korea).
10. Nasima Begumu, Toru Nakanishi, Nobuo Funabiki, “Reducing public-key size in anonymous credential system for CNF formulas with constant-size proofs,” 2nd IEEE Global Conference on Consumer Electronics (GCCE2013), 2013 年 10 月 1～4 日,幕張メッセ(千葉県).

６．研究組織

(1)研究代表者

中西　透（TORU NAKANISHI）
広島大学・大学院工学研究院・教授
研究者番号：50304332

(2)研究分担者

なし

(3)連携研究者

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