様式 C-19

科学研究費補助金研究成果報告書

平成　23 年　6 月　24 日現在

研究種目：若手研究（B）
研究期間：2008～2009
課題番号：20760253
研究課題名（和文）　票の買収や強要に耐性を有した電子投票に関する研究・開発
研究課題名（英文）　A study on e-voting protocols resistant to coercion and vote buying

研究代表者
中里　純二（NAKAZATO JUNJI）
独立行政法人情報通信研究機構･情報通信セキュリティ研究センター　インシデント対策グループ・有期研究員
研究者番号：60435782

研究成果の概要（和文）：
投票者が投票に参加する際に，自分の秘密鍵（秘密情報）を提示すること無く投票資格を第三者に譲渡不可能な認証方式の提案・開発を行った．提案方式では，ペアリング技術を用いる事で投票者の公開鍵を認証情報に含め，認証情を報提示するときに対となる秘密鍵情報を持っている事を証明する．そのため，秘密鍵の提示を行う事なく，第三者に認証情報の譲渡を行うことを防止した．200 人程度の候補者に対して登録から，認証完了までに約 10 秒程度で処理が完了することが確認でき，実用的であることを示した．

研究成果の概要（英文）：
I proposed and implemented anonymous authentication scheme with resistant to the coercion. The proposed scheme includes user public key into certification that is issued from administrator using pairing technique. And then, the user proves his certification with knowledge of his private key to the verifier. Therefore, the user cannot transfer his certification to a third party without disclosing his private key. It was able to perform all processes from registration to the authentication in about 10 seconds.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,400,000	420,000	1,820,000
2009 年度	1,900,000	570,000	2,470,000
年度			
年度			
年度			
総　計	3,300,000	990,000	4,290,000

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：暗号・セキュリティ

１．研究開始当初の背景

インターネットを用いた電子投票は，現在の投票とは異なり投票所へ行く必要が無く，投票期間中に投票所の設置・運営を行う必要が無くなる．また，集計処理も計算機により瞬時に行う事が可能となる

ため，非常に期待されている技術である．しかし，一方で不正な投票者や候補者により票を売買(買収)する行為や，正規の投票者が意図した票を投票できないようにする強要等の，現在では起こり難い重大な脅威が発生する可能性がある．そこで，本研究では，票の買収や強要に対して耐性を持った 電子投票方式の研究・開発を行う．

２．研究の目的

現在の投票では起こり難い重大な脅威である，票の買収や強要等に耐性を持つ電子投票へ応用可能な技術の提案･開発を行う.電子投票では，投票権（投票資格）の譲渡，コピーが容易になる．そのため，投票権を譲渡する事で票の買収，強要などが容易に行われる可能性がある．そこで，投票権の譲渡が困難な投票（投票権の確認）方式の開発が重要となる．本研究では，（1）パスワードを用いた匿名認証方式の検討を行い，匿名認証方式の問題点等を明らかにし，（2）ペアリング技術を用いた票の買収･強要に耐性を持つ匿名認証方式の開発を行う．最後に（3）実装評価を行うことで，実際に大規模なシステムとして利用した場合の運用コストを明らかにする．ペアリング技術を用いる事で，投票権の証明を行う際に利用者の秘密情報(秘密鍵)を所有している事を示す必要があるため，投票権の譲渡を抑止することが可能であると考える．さらに，投票者の数に依存せず，効率的なシステムの構築が可能になる．また，一般的にペアリング技術は計算コスト（計算時間）が高いと言われていることから，投票者等の負担や運用コストを明らかにするため試験実装を行う．運用コストを見積もる事で利用者が大規模になった場合の投票者の必要計算機性能や，集計端末の必要計算機性能を具体的に決定する事が可能となる．

３．研究の方法

（1）匿名パスワード認証方式の実装，及び認証情報の譲渡（強要）への耐性検討

電子投票において非常に重要となる認証方式について検討を行う．特に，匿名性を担保しつつ利用者（有権者）を確実に認証する必要があるため，ID（利用者を特定できる情報）を用いる事無く ID と関連付いているパスワードのみで利用者の認証が可能な，匿名パスワード認証方式の検討を行う．利用者は，管理サーバ（投票管理者)から登録されている全利用者分のパスワードを暗号化された状態で受け取り，その中から自分のパスワードを選び認証を受ける．このとき，利用者は送られてくる暗号化パスワードリストのどこに自分のパスワードが含まれているかを特定する必要がある．パスワードは暗号化されているためどれが自分のパスワードであるかがわからないため，登録時に用いた知識情報（登録画像）により特定できるようにする．そのため，管理サーバから送る暗号化されたパスワードリストは毎回ランダムな順番に生成することが可能となり，利用者のプライバシ(毎回同じ順番でリストが構成されていると，特定の利用者のパスワードを総当たりにみつけだすことが可能になる)を防ぐことができるようになる．また，認証情報の譲渡を防止する技術開発の検討を行い，大規模な利用を考慮した運用コストの見積もりを行う．

（2）認証情報の譲渡を防止する匿名認証方式の検討

（1）での検討を基に，利用者数（投票者数）に依存せず，認証情報を譲渡することが困難な匿名認証方式の開発を行う．また，利用者の検証コスト等を考えてペアリング技術を用いた新しい認証方式を導入する．認証情報（投票権）を発行する際に，利用者の公開鍵を含めることで認証時（投票権の証明時)に認証情報に含まれている公開鍵と対になる秘密鍵(利用者の秘密鍵)を持っていることを示す．そのため，利用者は自らの秘密鍵を示すこと無く，認証情報を第三者に対して譲渡することは困難になると考える．

（3）実装評価

（2）で開発した技術の実装・評価を行う．利用者数や，認証者数（有権者数），安全性などのパラメータを複数設定し，実運用可能かどうかの評価を行う．実際に利用者が許容できる最大待機時間等の設定により，提案方式がどの程度の規模のサービスとして運用可能であるかなどを見積もる．

４．研究成果

（1）匿名パスワード認証方式の実装

提案方式では，利用者（投票者）が認証サーバに登録されたパスワードを正しく知っているかを，利用者の ID を明かす事無く認証する事が可能となった．従来の方式では，利用者はサーバの保持しているデータベースと利用者との関連を示す必要があったが，提案方式ではパスワードと組となる画像（知識）によりその位置を利用者本人のみが特定可能な仕組みを取り入れた．本方式ではパスワードと画像情報を利用する事で二重の認証となり，利用者の負担を最小限にしながら安全性も向上したと考えられる．また，試験実装の結果（図１）から利用者の最大待機時間を 1 分とした場合， 3,000 人程度の利用者で

あれば，構成かのうであることが分かった．従って，大規模な選挙などに用いる場合は選挙区などにより，ある程度グループ分けを行う必要がある事がわかった．

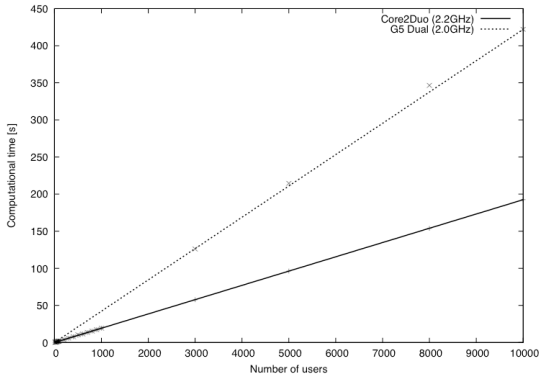

図１　利用者数と処理時間の関係

（２）認証情報の譲渡を防止する匿名認証方式

図１の結果より，匿名パスワード認証方式では，処理性能（速度）が利用者数に比例していることが示された．また，認証情報の譲渡は，パスワードの譲渡，知識の譲渡などを行うことで容易に可能であった．そこで，利用者数に依存せず，認証情報の譲渡を防止した新しい方式の提案を行った．

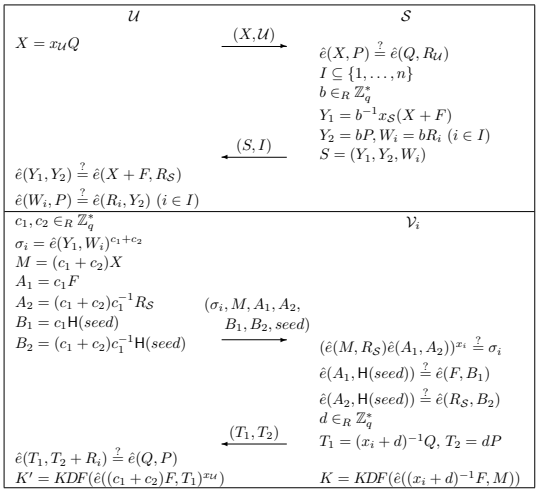

図２　提案方式プロトコル

認証情報の発行には近年多くの研究が行われているペアリング技術を利用した．ペアリング技術を利用することで，利用者の公開鍵を認証情報に含めることで，認証時に公開鍵と対となった秘密鍵を持っていることを証明することが必要となる．ここで，パスワードなどの秘密情報は，利用するシステムやサービス毎に異なるものを設定し利用することが容易にできる．そのため，あるパスワードを譲渡した場合でも特定のシステムやサービスのみ利用される様になる．しかし，秘密鍵は全てのシステムやサービスで共通のものを利用する前提のため，利用者は自分の秘密鍵を示すこと無く認証情報を第三者に譲渡することが困難になる．その結果，譲渡や買収を防止することができると考えられる．

図２に提案方式の具体的なプロトコルを示す．ここで，Q，P，Fは生成元，H(・)はハッシュ関数，x_uはユーザｕの秘密鍵，R_uはユーザｕの公開鍵を示している．提案方式では特に以下の性質を満たすことを目的とした．

認証性：利用者（有権者）が生成する投票資格要求（X）には，利用者の秘密鍵 x_u が含まれている．そのため，投票資格要求を生成可能なのは利用者本人に限定される．したがって，X を認証要求発行者（選挙管理者）が検証する事で，利用者の認証とする事が可能である．

完全性：正しくプロトコルを実行する事で，指定された資格確認者（候補者） V_j のみと，必ずセッション鍵 Key を共有する事が可能である．

検証者制限可能性：各検証者用に変換した認証情報は，提示する検証者の公開鍵 Ri が含まれているため，検証には対となる検証者の秘密鍵 xi が必要となる．また，認証情報発行者が指定した検証者意外に認証情報を提示する場合，認証情報発行者が生成した乱数 b が必要となるため，b が知られない限り正しく検証可能な認証情報の生成は困難である．したがって，指定された検証者以外が検証可能な人相情報を生成することは困難である．

再利用不可能性：検証者に提示する認証情報を検証するためには，検証者の秘密鍵が必要となる．そのため，他の検証者および認証情報発行者は認証情報の正当性を検証できない．したがって，検証者が提示された認証情報を利用することで利用者に成り済まし，他の検証者に正しく認証情報を提示することは困難である．

追跡不可能性：検証者に示す認証情報を生成する際，c1，c2 により毎回ランダマイズ化する事で検証者には利用タイミングごとに異なった認証情報を生成できる．従って，検証者同士が結託しても，同じ利用者が生成した認証情報であるか特定する事は困難である．また，たとえ認証情報発行者と検証者が結託した場合でも，利用者により生成され

た c1, c2 を知る事無く認証情報発行者が自らが発行した認証情報と各検証者向けに変換された認証情報を関連づける事は困難である.

譲渡不可能性：認証情報を譲渡された利用者は,正規の利用者に対する正しい認証情報を生成することはできる.しかし,最終的に行われる鍵共有では,認証情報の発行を受けた正規の利用者の秘密鍵が必要となり,鍵共有が成功しない.そのため,正規の利用者は自分の秘密鍵を提示すること無く認証情報を譲渡することは困難である.

以上の条件により，利用者の数に依存せず,認証情報の譲渡を防止した効率の良い方式の提案を行った.

（3）実装評価

（2）で提案を行った匿名認証方式の実装・評価を行った．ここでは，各パラメータを変化させた場合のパフォーマンス評価を行った．特に,安全性の指標となる鍵サイズの違いによるシステムパラメータの生成パフォーマンスや，検証者数（候補者数）によって影響する認証情報の生成・発行コスト，及びその検証コストを明らかにした．開発には Java を用いたペアリングベースの暗号ライブラリである jPBC を利用し，CPU: Quad-Core Xeon (2.26GHz × 2)，メモリ: 32GB のコンピュータを利用した．また，本実装では，最も一般的な楕円曲線である $y^2=x^3+x$ をペアリングの構成に用いた.

図 3 より，安全性の指標となる鍵サイズにより,システムパラメータの生成時間は累乗関数的に増加し,鍵生成の時間は線形関数的に増加することが分かった.また,一般的な安全性を担保した場合(鍵サイズは 512 ビット程度と言われている)，鍵生成までには 1 秒程度と現実的な性能であることが分かった.

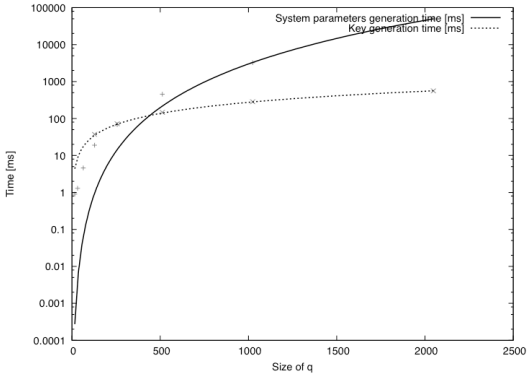

図３鍵サイズとシステムパラメータ生成時間

提案方式では，提示先の数（候補者数）に応じて利用者の処理時間が異なってくることから，利用者の最大待機時間（処理時間)を 10 秒とした場合の評価を行った.このとき,安全性のパラメータとなる鍵サイズを 512bit とし，一般的な安全性を確保することを考慮した.図４より，利用者の待機時間（処理時間）は提示先の数に比例することが分かった.また，最大待機時間を 10 秒とした場合,提示先の数は約 200 個程度となった.

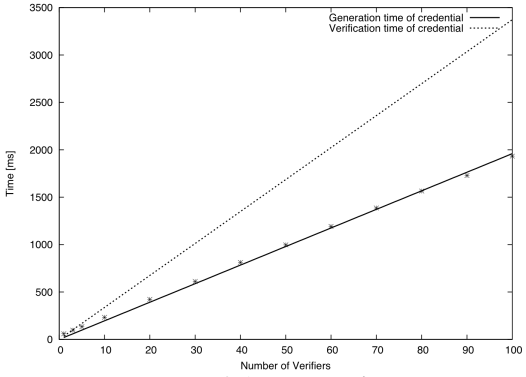

図４　提示先数と処理時間

以上の結果より，提案方式は投票者数に依存しない方式であり,実際に国政選挙などに利用した場合でも,各候補者数の最大は 200 人以上とはならないため,十分実用的な方式であることが示された．また，

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）

〔学会発表〕（計　2 件）

１）中里　純二 他，プライバシを考慮した資格証明システムの実装，コンピュータセキュリティシンポジウム（CSS 2010），2010 年 10 月 20 日，岡山コンベンションセンター（岡山）

２）中里　純二 他，匿名パスワード認証を用いた匿名告発システムの提案，コンピュータセキュリティシンポジウム（CSS 2008），2008 年 10 月 8 日，沖縄コンベンションセンター（沖縄）

６．研究組織

(1)研究代表者

中里　純二（NAKAZATO JUNJI）

独立行政法人情報通信研究機構・情報通信セキュリティ研究センター　インシデント対策グループ・有期研究員

研究者番号：60435782

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：