様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月　４日現在

研究種目：基盤研究（Ｃ）
研究期間：2007～2009
課題番号：１９５６０３６７
研究課題名（和文）高い信頼性を有する電子選挙システムの構成

研究課題名（英文）Construction of Highly Reliable Electronic Election Systems

研究代表者　満保　雅浩（MAMBO MASAHIRO）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：60251972

研究成果の概要（和文）：

民主主義的な手続きに基づく健全な電子社会を確立するために、現在必要とされる制約を可能な限り除去した、高い信頼性を有する電子選挙システムを構築することに取り組んだ。まず、公開検証型電子投票を、暗号技術の危殆化による過去の投票内容の暴露の危険性という観点から考察し､暗号の危殆化にも対応した安全な公開検証型投票方式の構成方法を示した｡そして、電子選挙における投票時刻に着目し、投票し直しを許すことによる買収や強制への耐性の向上効果について検討をおこなった。更に、投票内容が正しく処理されたことを確認するための仕組みについても考察を行った。

研究成果の概要（英文）：

For the construction of a democratic society in the highly-developed IT environment, we have examined the construction of highly reliable electronic election systems which do not contain restrictions imposed in the present systems. At first, we have reconsidered privacy problem in publicly verifiable voting schemes from the viewpoint of security degradation of cryptographic primitives and proposed a method to construct publicly verifiable voting schemes protecting user's privacy even after such security degradation. Secondly, we have paid attention to the timing of voting and discussed the effect of re-voting for decreasing the threat of vote-buying and coercion. At last, we have discussed methods for voters to check the correctness of their votes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,600,000	480,000	2,080,000
２００８年度	1,000,000	300,000	1,300,000
２００９年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,600,000	1,080,000	4,680,000

研究分野： 通信・ネットワーク工学
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：電子選挙，投票，正当性検証，匿名性，暗号危殆化

１．研究開始当初の背景

民主主義的な手続きに基づく健全な電子社会を構築していくために、不正のない電子選挙システムは欠かすことができない技術といえ、選挙の電子化により、集計処理の効率化、在宅投票の可能性などのメリットも期待される。しかし、電子選挙には、投票装置が不正なく動作していることを確認する簡易な手段がないことや、票の買収対策、脅迫対策など、現在も完全には解決仕切れていない課題が幾つも存在し、投票装置に信頼をおく、もしくは、投票所に出向くなどのある種の制約を課さなければ、誰もが安心して選挙に参加することができないという状況にあった。現在必要とされる制約を可能な限り除去した、高い信頼性を有する電子選挙システムを構築することが望まれる。

２．研究の目的

本研究では、以下の3つの項目を中心に、高い信頼性を有する電子選挙システムを構築することを目的とする。

(1) 暗号の危殆化の影響に関する研究

投票者が自己の投票内容のみならず、全ての投票内容が正しく集計されていることを確認できる（全体検証を実施する）公開検証型電子投票が現在までに考案されているが、この既存の公開検証型電子投票の多くは、利用している暗号技術の危殆化に伴う、過去の投票内容の暴露の危険性を考慮し切れていない。このため、投票の実施された時点では、プライバシーが守られていても、攻撃アルゴリズムの進展などにより、利用されていた暗号が安全でなくなり、投票行動に係わるプライバシーが保てなくなる危険性が残ってしまう。例えば、レシートフリーと呼ばれる暗号手法を用いて脅迫対策を行っても、危殆化により、レシートフリー機能が効かなくなることを恐れ、脅迫に従ってしまうことが懸念される。このように、暗号の危殆化は投票行動に少なからぬ影響を与える恐れさえ秘めており、事前に、暗号危殆化について十分に配慮のなされた電子投票方式を構成する必要性があることを示唆している。そこで、電子選挙における暗号の危殆化の影響と対策を検討する。

(2) 買収・脅迫対策の研究

選挙には票の買収や特定の投票行為の強制を防ぐ仕組みが必要であり、買収もしくは強制を行う不正者が投票内容を確認できないように、現行の選挙では、投票ブースと不正監視のための立会人により、投票者以外が投票内容に影響を与えられないという状態を作り出している。電子選挙、特に、在宅投票などのネットワーク形電子投票においては、投票ブースや不正監視のための立会人が存在しないため、不正者の影響の排除が難しくなる。このため、票の買収や特定の投票行為の強制といった不正行為への対策を欠かさずに行わなければならない。そこで、買収・脅迫対策について検討を行う。

(3) 投票内容が正しく処理されたことを確認できる仕組みの研究

投票に関係する装置を信頼せずとも、投票内容が正しく集計されていることを容易に確認できる仕組みを検討する。これは、一般には、処理内容を検証する技術の研究と捉えることができ、また、信頼性の高い電子選挙システムを様々な選挙規模において構築していくことにも関連する。

３．研究の方法

(1) 暗号の危殆化の影響に関する研究

公開検証型電子投票を幾つかの方式に分類し、暗号危殆化との関連について考察するアプローチを取った。公開検証型電子投票には、MIX-netを利用した方式と準同型性に基づいた方式が存在する。また、準同型性に基づいた方式の中には、公開鍵方式の準同型性を利用しているものがあるが、一方向性に基づかない関数の準同型性を利用している方式もあり、これらは、情報量的な安全性に基づく方式として別に分類することができる。

(2) 買収・脅迫対策の研究

佐古らは、暗号と情報セキュリティシンポジウム(SCIS)での論文賞の選出に電子投票を導入する実験(SVIS プロジェクト、 Secure Voting in Symposiums)を行っており、2008

年に実施した内容について文献[SM08]において以下のように報告している。

電子投票方式として、ミックスネットを用いた方式を採用し、ミックスネットは、文献[FMMOS02]で紹介されている有限体上のElGamal 暗号に基づく実装を、楕円 ElGamal 暗号に基づく実装に置き換えたものを用いて、安全性を損なうことなく、計算量とデータ長の低減を実現している。

そして、ミックスネットを用いた電子投票方式の特長として、以下の4点を挙げ、SCIS論文賞の投票に最初に実装する上で、ミックスネットを用いた電子投票方式が準同型暗号やブラインド署名を使った他の投票方式よりも適していると述べている。

① 選択対象の数によって方式が複雑化したり、暗号化コストが増加したりしない。
② 匿名通信路などの特別な仮定が不要である。
③ 暗号投票文を記名で送るので、送られた複数の暗号投票文のうち、最後の暗号投票文のみを有効にできる。
④ 集計結果が正しいことをだれでも確認できるという、紙ベースの投票ではなかった機能を提供することができる。

この3番目の特長は、投票者にとって、自己で投票した内容に納得できなければ、投票し直せることを意味する。実際、この内容を報告している文献[SM08]では、3.1節 概要において、提案した電子投票のメリットとして、

① 投票対象の論文を選びやすいこと
② 投票期限が来るまで何度でも投票し直すことができること
③ 投票期限が会期終了時より余裕があること
④ 分散して集計作業が可能であること

を挙げ、これらの結果、投票率が向上する効果も期待をしていたと述べている。

本研究では、この2番目のメリットを、票の買収や特定の投票行為の強制などの脅威への対策という観点から捉えられることに着目した。投票し直しが可能ならば、もし、強制を行う不正者が投票者の投票行動を監視し、特定の投票行為を強制したとしても、不正者の監視が終わった後に、投票者は投票をし直し、不正者に強制された投票内容を無効にすることができる。よって、投票期限が来るまで何度でも投票し直せるという投票形態は、票の買収や特定の投票行為の強制への耐性を向上させる効果があると考えられる。

(3) 投票内容が正しく処理されたことを確認できる仕組みの研究

電子選挙には、投票を受け付ける投票機や投票データを集計する装置、投票データを保管管理する機器及び投票データが正しく処理されたことを検証可能とするログ管理装置が存在する。電子選挙のプロトコルは、これらの装置の信頼性について何らかの仮定をおいていることが多いため、電子選挙のシステム全体としての安全性を保証するためには、これらの装置が正しく動作しないことを想定して対策を立てることが求められる。
そこで、投票者が投票内容に関する受領書を受け取ることを通して信頼性を高めようとするアプローチに着目し、受領書が正当であることを簡易に確認することができる仕組みについて検討した。

４．研究成果

(1) 暗号の危殆化の影響に関する研究

公開検証型電子投票を、暗号技術の危殆化による過去の投票内容の暴露の危険性という観点から考察し、暗号の危殆化に対応した既存の公開検証型投票方式は、通信量の増加や保有データ量の増加などが起こるため、そのようなデメリットのない準同型性に基づく方式において、匿名マルチパーティ計算の手法を組み合わせることにより、暗号の危殆化にも対応した安全な公開検証型投票方式を構成できることを示した。
投票者は、Mix-netや準同型性に基づく方式における入力を、サーバや集計者に送る前に、文献[MP03]のAMPCと呼ばれる方式を用いて、投票者と入力との対応関係をなくし、AMPCの出力をMIXサーバや集計者に渡す。AMPCは、公開鍵暗号系の技術を利用していないため、閾値以上のプレーヤが攻撃されない限り、対応関係を見つけることができない。よって、Mix-netや準同型性に基づく方式で利用される公開鍵暗号系が危殆化したとしても、投票者のプライバシーの侵害を防ぐことが可能となる。
なお、AMPCは、階層構造に配置した複数のAMPCプレーヤが、入力リストのシャッフルと、入力値の分割、および、それぞれの分割値の下部層の異なるAMPCプレーヤへの受け渡し、を順次繰り返す方式である。基礎となるAMPCでは、階層構造が逆三角形構造となっており、最終的に、入力の和を出力として計算し、かつ、その値をシャッフルしたものとして出力することができる。本研究では、AMPCのこれ

らの特性を利用していることになる。

(2) 買収・脅迫対策の研究

佐古らのミックスネットを用いた方式を参考に、投票のし直しを許すことにより、投票の参加者全員が投票を再度行わなくてはならなくなることがないように、一部の参加者のみでも投票をし直せる構成を採用した。投票が可能となる期間を複数の期間に分け、投票し直された複数の票の中から、最後に投票された票をカウントするなどの、真の票としてカウントする仕組みを取り入れている。つまり、票の中身自体は隠し、匿名性を保ちながら、票の関連性より、有効な票のみをカウントすることが可能となる。買収や脅迫への耐性が向上していることを確認するために、有効な票を投票した期間を不正者が特定することの難しさについて考察した。

また、買収・脅迫耐性の高い電子選挙システムを構成するために、集計者の秘密鍵が漏洩した際の影響とその対策としての鍵更新の効果について検討を行い、集計者の秘密鍵を更新する方が買収耐性の向上が期待できることを指摘した。

集計者の秘密鍵が投票期間を通して固定の場合、ある時間帯に漏洩した秘密鍵を入手した不正者は、集計者に送信された投票データの中で、漏洩した秘密鍵を用いて作成された投票データの内容を確認することができてしまう。このため、買収・脅迫耐性は低いと考えられる。

これに対して、集計者の秘密鍵を分割された複数の投票期間ごとに順次更新する場合、ある時間帯に漏えいした秘密鍵を入手した不正者は、その時間帯以降の集計者の秘密鍵を求めることができ、投票データの内容を確認することができてしまう。このため、秘密鍵を固定した場合と同様に、買収・脅迫につながる恐れがあるが、秘密鍵が漏洩した時間よりも前に利用された秘密鍵を求めることはできず、投票内容を特定することもできない。このため、秘密鍵が漏洩した時間よりも前の投票行動に関する買収・脅迫は起こりにくいといえ、電子選挙システムとしては、買収・脅迫耐性が上がると考えられる。

(3) 投票内容が正しく処理されたことを確認できる仕組みの研究

特殊なプリンターなどがなくとも、投票内容が正しく処理されたことを投票者が容易に確認可能な方式を、分割・選択法と呼ばれる手法や特色のある確認内容表示方法を活用しながら構成を行った。

また、選挙規模と選挙システムの関係を解明するために、大規模から小規模までの異なる規模を持つ組織向けの電子選挙を取り上げ、匿名性の侵害や不正カウントなどの不正が発生する可能性を考察した。

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）

〔学会発表〕（計 1 件）
(1) 満保 雅浩．公開検証型電子投票の安全性について．電子情報通信学会．機械振興会館，東京．2008 年 3 月 7 日．

〔その他〕
参考文献：

[FMMOS02] J. Furukawa, H. Miyauchi, K. Mori, S. Obana, K. Sako,
“An Implementation of a Universally Verifiable Electronic Voting Scheme based on Shuffling,”
Financial Cryptography 2002, Springer-Verlag, Lecture Notes in Computer Science 2357, pp.16-30 (2003).

[SM08] 佐古和恵，森健吾，
“ミックスネットを用いた SCIS 論文賞電子投票実験について，”
IEICE Fundamentals Review, Vol.2, No.1, pp.48-57 (2008).

[MP03] D. Malkhi and E. Pavlov,
“Anonymity without ‘Cryptography’,”
Financial Cryptography 2002, P. Syverson (ed.), Springer-Verlag, Lecture Notes in Computer Science 2339, pp.117-135 (2003).

６．研究組織

(1)研究代表者
満保　雅浩（MAMBO MASAHIRO）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：60251972

(2)研究分担者
なし

(3)連携研究者
なし