強制耐性電子投票方式に対する1つの反証 物理的投票ブースの効果

櫻井幸一 [1,*]　上繁義史 [2]

概要:2003 年に混合ネットを利用した電子投票プロトコル[Providing Receipt-freeness in Mixnet-based Voting Protocols, ICISC2003]は、無証拠性を主張している：投票者は、第三者に対して、自分の投票事実を証明できない。このため、強制投票への対策にもなっているとも考えられる。しかし、本稿では、具体的に如何にして、強制投票の可能性があるのか、投票ブースの役割と限界に注意しての解析を行う。

キーワード：電子投票，無証拠性、強制耐性、投票ブース

Disproving coercion resistance in some e-voting scheme, or power of physical voting booth

Kouichi SAKURAI[1,*]　Yoshifumi Ueshige[2]

Abstract: Lee et al. designed an electronic voting protocol [Providing Receipt-freeness in Mixnet-based Voting Protocols, ICISC2023], which claims to achieve receipt free: voters cannot prove the fact of their vote to a third party. Therefore, this could be seen as a countermeasure against coerced voting. In this paper, however, we analyze how exactly the possibility of coerced voting exists inside thee-voting scheme of Lee et al.

Keywords: e-voting, coerforce, receipt-free, voting booth

1. はじめに

研究開発史-1990 年代:現在の選挙の多くは匿名形式で，投票者は投票所へ出向き、本人確認を行い、仕切られた投票ブースで無記名票に選択候補名を書き込み、最後に投票箱へ入れる。この物理的な選挙を電子化・オンライン化する試みは、1990 年代は海外の暗号学者が先駆けた。国内でも企業の研究らが中心となり盛んに研究した。

この時期は，中央集権型システムを前提とし，公開暗号技術で信頼性とプライバシーの問題を解決してきた。

電子投票の理想的安全性:1990 年代の中央管理型電子投票では、公開型電子掲示板を仮定し、投票者自らが 集計結果を確認できる検証可能性を重視し、応用暗号技術により、これを実現した。この検証可能性は，投票者が自分の投票事実を他人にも証明できるため、票売買という新たな，しかし現実の深刻な問題を生み出すことになる[1]。

以降、無証拠性を満たす電子選挙方式の研究が活発となるが，未だに実用レベルでの解決には至ってはいない状況にある。

2. 混合ネット型[ICISC2003]vs 絶対当選系

混合ネットに基づく電子投票方式では、無証拠性を実現することは難しいと考えられてきた。その理由は、ユーザは投票用紙をどのように暗号化したかを購入者に証明することができるからである。この課題に対して、Lee ら[2]は、再暗号化技法と指定検証者再暗号化証明（DVRP）を用いることで、混合ネット型電子投票方式を無証拠化する方法を提案した。この方式では、投票者は、耐タンパランダマイザ(TRR)が提供する乱数化サービスを通じて、暗号化された投票用紙を準備する必要がある。また、Lee らは、無証拠性を実現するための提案技法は、ほとんどのミックスネット型の電子投票方式に適用できると主張している。特に、論文[2]では、投票ブースが不要であることが強調されている。

その一方で文献[4]では、投票所における現行の無記名選挙制度でも、強制が可能な事例を具体的に紹介している。巧妙ではあるが、不正(被強制)投票者は、他人が記名した投票用紙を、自ら投票箱に投函するという手法である。

本研究では、Lee らの提案で主張している、投票ブースの不要性を再考する。我々は、青木[4]が紹介している絶対当選システムにおける強制投票手法を手本に、投票ブースの役割と限界を解析する。

1 九州大学 大学院システム情報学研究院
Graduate School of Information Science and Electrical Engineering, Kyushu University.
2 長崎大学　ICT 基盤センター
Center for Information and Communication Technology, Nagasaki University.
* sakurai@inf.kyushu-u.ac.jp

© 2023 Information Processing Society of Japan

絶対当選系[4]は電子投票に関する文献ではないが，耐強制性が無効化される投票の攻撃モデルと考えられる。仮に当選者が 1 名の場合には必ず強制者が支持する候補が当選する。

候補者をX，Xの支持者をY，Yによって投票行動を強制される投票者を$\{Z_i|1 \leq i \leq N\}$とする。こちらの投票者を含めた投票者数をMとする。Z_1はYの自宅から投票所に行き，投票を行うふりをして白票をYの自宅に持ち帰る。Z_1から白票を受け取ったZ_2はYの監視の下でXの氏名を記入し，その票を持って投票所に行く。Z_2は白票を受け取るが，持参した票により投票する。Z_2は白票をYの自宅に持ち帰り，Z_3が同様の投票行動を行う。これをZ_Nまで繰り返すことによって，Xは少なくとも$N-1$票を得ることができる。総投票数Mに対して，$N-1 > M/2$であればXは当選となる。

この方法において，投票用紙への記名を強制者の前で行うため耐強制性が成立しない。投票ブースで別の氏名に書き換えることができるため無証拠性の成立についても議論の余地がある。

本研究では，この手法の電子投票への適用までは到達していないが，電子投票が投票ブースに設置された固定端末ではなく，投票者のもつスマートデバイスを用いる場合には，この攻撃が成功する可能性がある。

3. さいごに

本研究での指摘は、文献[3]で河辺らが与えている定理証明による無証拠性の結果を否定するものではない。しかし、文献[3] では、“すべての候補者は、攻撃者以外から最低一票は獲得する”という条件下での議論になっていることに注意する。

またLeeらの方式[2]では、投票者が利用する耐タンパランダマイザ(TRR)が提供する乱数化サービスを導入している。独立した関心としては、最近の分散環境下でのこうした乱数提供サービスの実現と応用がある[5]。

文献[6]では、検証性実現を実現する公開掲示板が、ブロックチェーンの登場により、もはや物理的な仮定と呼ばない時代になったことを論じた。しかし、投票所と投票ブースまでも必要としない、理想的な電子投票システムの設計は、未解決問題と言える。

謝辞

本研究は科研費 J-22K12029 の支援を受けている。また、本研究のきっかけは、ICISC2003 での Li らの投票方式[2]を事例に形式的手法による無証拠性解析を行った河辺らの研究[3]を、NTT 櫻田英樹研究員から紹介されたことがきっかけとなった、ここに謝意を表す。

参考文献

[1] J. Benaloh and D. Tuinstra, Receipt-free secret-ballot elections (extended abstract) Proc.the twenty-sixth ACM symposium on Theory of Computing (STOC) Pages 544-553 (1994)

[2] B. Lee, C.Boyd, Ed. Dawson, KJ Kim, Yang, J. Yang, & S. Yoo, (2004) Providing Receipt-Freeness In Mixnet-Based Voting Protocols. In Lim, J I & Lee, D H (Eds.) Proc. 6th International Conference on Information Security and Cryptology - ICISC 2003. pp. 245-258. (2004)

[3] 河辺 真野, 櫻田, 塚田 電子投票プロトコルに対する無証拠性の定理証明 情報処理学会論文誌 52(9) 2549-2561 2011 年

[4] 青木雄二 ナニワ資本論 朝日新聞社 pp. 156-159 絶対当選システム 1999 年

[5] 櫻井幸一 乱数ビーコンサービスの現状と課題 第 102 回コンピュータセキュリティ・第 52 回セキュリティ心理学とトラスト合同研究発表会 (2023.7 月)

[6] Misni, Dutta, and 櫻井 2E1-3 ブロックチェーンを利用した電子投票システムの安全性 SCIS2020, 2E1-3 (2020.Jan)

© 2023 Information Processing Society of Japan