電子投票におけるMixnet機関の負担軽減

2G－7

溝入 優一† 飯島 正‡ 土居 範久‡

†慶應義塾大学大学院理工学研究科 ‡慶應義塾大学理工学部

1 はじめに

電子投票とは，ネットワークを用いて電子的に選挙を行う方法である．通常の選挙では，投票時間の制限や投票所までの移動の手間などの要因により有権者が投票を行えないことが考えられ，この問題を解決するために電子投票の研究が進められている．

この電子投票を実現する際の課題の一つに，無記名投票の実現が挙げられる．これは，開票を行う機関が単に有権者と通信を行って投票内容を集めるのでは，この機関が有権者と投票内容の対応を知ることができてしまうためである．現在，この無記名投票の実現方法の一つに，Mixnet[1]という匿名通信のプロトコルを利用する方法が考えられている．しかし，この方法では，暗号に公開鍵暗号を用いる必要があるため，大規模な選挙を行う場合には，Mixnetにおいて匿名性を保つための機関(Mixnet機関)に対して大きな負担がかかると考える．

本研究では，Mixnet機関がMental Poker Protocol [2]を用いて投票者に共通鍵を配布し，その鍵をMixnetで利用することにより機関の負担を投票者に分散させる方法を提案する．そして，従来の方法と提案する方法におけるMixnet機関，投票者それぞれに必要な計算及び通信の量の比較を行った．

2 Mixnet

本章では，Chaumの提案したMixnetと呼ばれる匿名通信について述べる．Mixnetとは，図1に示すように，通信するもの同士が直接通信を行うのではなく，いくつかのMixnet機関を経由して通信を行うことによって，匿名性を保つというものである．

2.1 手順

Mixnetの手順は次に示す通りである．

1. メッセージの送り主は，自分の送りたいメッセージに対して経由するMixnet機関の公開鍵を用いて重ねて暗号化を行う．つまり，Mixnet機関の数と同じだけの暗号化が必要となる．この時，それぞれの暗号化の前に，暗号化するビット列に対してブロック長のランダムビット列を付け加える必要がある．
2. 送り主は用意した暗号文を最初のMixnet機関に送る．
3. それぞれのMixnet機関は，受け取った複数のメッセージに対して，自分の秘密鍵で復号を行い，ランダムビット列を取り除く．そして，受け取ったメッセージと復号したメッセージの対応を秘密にして次の機関に送る．
4. メッセージの受取主は最後のMixnet機関からメッセージを受け取る．

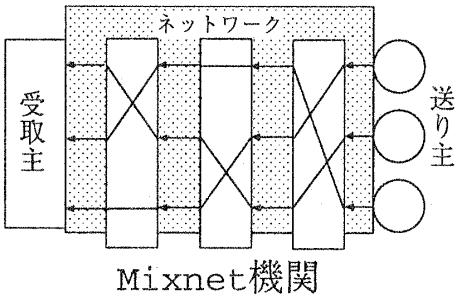

図 1: Mixnetの概要

2.2 安全性

上記のような手順をとることにより，Mixnet機関が受け取るメッセージと送り出すメッセージの対応はその機関以外は知ることができない．そのため，この方法を用いれば，すべてのMixnet機関が結託しない限り通信者の匿名性を保つことができる．

3 Mental Poker Protocol

Mental Poker Protocolとは，本物のカードを用いずに電話などのメッセージ交換だけでポーカーを行うプロトコルのことである．このプロトコルを用いてディーラーがプレイヤーに対してカードを配布すると，プレイヤー同士だけでなく，ディーラーも，どのプレイヤーがどのカードを受け取ったかを知ることはできない．

そして，このプロトコルの特徴として，プレイヤーが中心となって計算を行い，プレイヤー同士での通信が必要であるということが挙げられる．

"A Method for Lightening the Load on Mixnet Facilities in Electronic Voting", Yuichi Mizoiri, Tadashi Iijima and Norihisa Doi, Keio University

4 Mixnet機関の負担の軽減方法の提案

2章で述べたようにMixnetでは，Mixnet機関は暗号文を公開鍵を用いて復号する必要がある．そのため，大規模な電子投票では，Mixnet機関の負担が大きくなると考えられる．そこで，この負担を軽減する方法を提案する．

4.1 負担の軽減方法

我々は，Mixnetでの暗号に公開鍵暗号を使うのではなく，それぞれのMixnet機関が投票者の数だけの共通鍵をMental Poker Protocolを用いて投票者に対して事前に配布することにより，共通鍵暗号を使う方法を提案する．

通常のMixnetにおいて公開鍵を用いる必要があるのは，単に投票者がMixnet機関と事前に共有しておいた共通鍵を使って暗号化すると，Mixnet機関は復号時に投票者を特定できるためである．しかし，Mental Poker Protocolを用いて共通鍵を配布すれば，どの投票者にどの共通鍵が渡ったかを誰も知ることができないため，Mixnet機関は復号時に投票者を特定することはできない．

ただし，これだけではMixnet機関は復号時にどの共通鍵を用いればよいか分からない．そのため，機関は共通鍵に番号を付けて，共通鍵とその鍵番号の組合せを配布するものとする．そして，投票者は共通鍵で暗号化した後にその暗号文に鍵番号を付け加えておくことにより，Mixnet機関はどの共通鍵を使って復号すればよいかが分かる．ここで，Mixnetの手順では暗号化する前にブロック長のランダムビット列を加えるので，ランダムビット列の一部にその前に暗号化した共通鍵の鍵番号を用いることができるため，鍵番号を付け加えることによる暗号文の長さへの影響は少ない．

また，Mental Poker Protocolとは投票者の間で通信を行い，投票者が決まった手順で処理を行うというものであるので，共通鍵の配布に移動エージェントを利用することにより，投票者が比較的容易にこのプロトコルを採用できると考える．

4.2 提案する選挙

提案する選挙の手順は次の通りである．

1. 開票する機関はID，Mixnet機関は共通鍵と鍵番号の組を，投票者に対してMental Poker Protocolを用いて配布する．

   ここで，IDとは開票する機関が投票の正当性を確認し，投票者が自分の投票の有効性を確認するものである．

2. 投票者はIDと投票内容の組に対して，Mixnet機関の数だけの共通鍵を使って暗号化し，Mixnetを通して開票する機関に送る．
3. 開票する機関は，送られてきたメッセージのIDが自分の配布したIDの中に含まれ，同じIDが一つしかないことを確認して投票内容の集計を行い，発表する．
4. 開票する機関はすべてのIDと投票内容の組を公開し，投票者は自分の組がその中に含まれることを確認する．

4.3 負担の分散

提案する選挙では，Mixnet機関は，共通鍵を配布する手間が生じるものの，Mixnetにおける復号に共通鍵を利用するため，負担が軽減される．これに対し，投票者にとっては，Mixnetのための暗号化の処理は機関と同様に軽減されるが，Mental Poker Protocolの処理のために，必要な処理の総量が増加する．つまり，Mixnet機関の負担を投票者に分散することになる．

5 計算の処理量の比較

従来の方法と提案する方法におけるMixnet機関，投票者に必要な処理の量を試算した．

この結果，それぞれが必要な暗号化または復号するメッセージの延べビット数は，提案する方法を用いることにより機関では70%削減できるが，投票者では10倍に膨らむ．また，それぞれが必要な通信のデータの延べビット数は，提案する方法を用いることにより機関では70%削減できるが，投票者では100倍に膨らむという結果になった．ただし，ここではMixnet機関が8個以上で，投票率が60%以上としている．さらに，提案する方法では，すべての投票者に一度で共通鍵を配布すると投票者に負担がかかりすぎるため，100人毎に配布することとして計算した．

このことから，機関の負担を投票者に分散することはできるが，暗号の処理に比べ通信コストの割合が高いと投票者の負担は大きく増加してしまうことが分かる．

6 まとめ

大規模な無記名投票をMixnetを使って行う場合におけるMixnet機関の負担を投票者に分散する方法を提案した．提案する方法を用いると，どのような割合でMixnet機関の負担を分散できるかの試算を行った．

参考文献

[1] Chaum, D. L., "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms.", Communications of the ACM, Vol. 24, No.2, 84-88 (1981)

[2] Shamir, A., Rivest, R. and Adleman, L., "Mental Poker", in Mathematical Gardner, D. E. Klarner, ed., Wadsworth International, 37-43 (1981)