社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38（６）
2007／7／19

小規模投票の匿名性を維持する得票数秘匿型電子投票方式

遠藤 つかさ† 越前 功‡ 吉浦 裕§

†電気通信大学大学院電気通信学研究科 〒182-8585 東京都調布市調布ヶ丘 1-5-1
‡国立情報学研究所コンテンツ科学研究系 〒101-8430 東京都千代田区一ツ橋 2-1-2
§電気通信大学電気通信学部 〒182-8585 東京都調布市調布ヶ丘 1-5-1

E-mail: †endo@edu.hc.uec.ac.jp, ‡iechizen@nii.ac.jp, §yoshiura@hc.uec.ac.jp

あらまし 小規模投票では,匿名性の喪失や買収・強制が大きな問題となる.本論文では,小規模投票における得票数の公開が匿名性の低下につながることを,エントロピーを用いて示す.この分析に基づき,匿名性を二つに分けて厳密化した上で,得票数秘匿型電子投票方式を提案する.提案方式の安全性はマルチパーティプロトコルの安全性に帰着する.

キーワード 電子投票, 匿名性, マルチパーティプロトコル

Electronic Voting Scheme to Maintain Anonymity in Small Scale Election by Hiding the Number of Votes

Tsukasa ENDO† Isao ECHIZEN‡ and Hiroshi YOSHIURA§

†The University of Electro-Communications 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan
‡National Institute of Informatics 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan
§The University of Electro-Communications 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan
E-mail: †endo@edu.hc.uec.ac.jp, ‡iechizen@nii.ac.jp, §yoshiura@hc.uec.ac.jp

Abstract Loss of anonymity, bribery, and coercion are more serious in small-scale voting than in large-scale one. This paper shows that the entropy of each vote can be decreased, i.e., the anonymity of voting can be compromised, by opening the number of votes that each candidate had. The paper gives two strict definitions of anonymity instead of the previous definition and, based on the new definitions, it proposes a new e-voting scheme that keeps the number of votes secret. The security of the propose scheme is equivalent to that of an existing multi-party protocol.

Keyword Electronic Voting,Anonymity,Multi Party Protocol

1. はじめに

近年,インターネットの普及とともにセキュリティ技術や暗号技術の実用化が進んでいる.その中のひとつとして電子投票が期待されている.従来は市長選などの大規模電子投票を対象とした研究が主に進められてきた.しかし小規模電子投票には,大規模電子投票とは違った問題がある.

たとえば,アリスはある委員会の委員である(図 1).この委員会は次期委員長を決定する選挙を行うことになった.立候補するのは現委員長と現副委員長である.現委員長派と現副委員長派はそれぞれ票の囲い込みに躍起になっている.アリスは中立派なので,絶対に自分の投票内容を秘密にし,どちらの派閥とも波風を立てることなく選挙を終えたい.もし投票内容が漏れたら自分の将来に影響するかもしれないからである.しかし中立派の委員は少数なので,2 人の候補の得票数から中立派の委員の投票の傾向が判明してしまう.

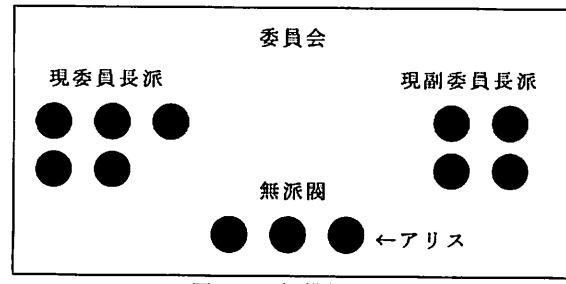

図 1 小規模投票の例

このように小規模投票の場合，少数の投票者内の派閥の分布や利害関係が，ある程度正確に判ってしまう．そのため得票数が公開されると中立派の投票行動や派閥内の裏切りが推定できる．いったん傾向が判明すると投票者個人に対しての問い合わせや観察も可能になり，投票の匿名性が失われる．また実際に匿名性が維持されている場合でも，投票者が匿名性の低下を不安に感じ自由に投票できなくなるおそれがある．匿名性の低下は自由な投票行動を阻害する．

そこで本論文では，小規模投票における得票数公開と匿名性の関係について分析した．この分析に基づいて，候補者の得票数を秘匿しながら当選者を示す得票数秘匿型電子投票方式を提案する．

2 章では小規模電子投票の特性を分析し，要件を定義する．3 章では従来の電子投票方式と関連研究について述べる．4 章では投票のモデルを作り，投票の規模と匿名性の関係を分析する．5 章ではマルチパーティプロトコルに基づいた得票数秘匿型電子投票方式を提案する．6 章では提案方式を評価する．

2. 小規模電子投票の問題点と特性

2.1. 小規模投票の問題点

小規模投票では，有権者内の派閥の分布や利害関係がある程度正確に判ってしまう．そのため，ある候補に予想された得票数と実際の得票数との差を比較することで，中立派の投票行動や派閥内の裏切りが推定できる．また，以下の要因により匿名性は更に低下する．

(1) 管理者や集計者が信頼できる第三者とは限らない

小規模投票の場合，手間やコストを省くため，投票の管理や集計を第三者機関に依頼することは少ない．このとき投票者の代表や投票を行う組織の事務職員などが管理者や集計者となり，管理者や集計者から投票内容が漏えいする可能性がある．

(2) 筆跡による推定の可能性が大きい

小規模投票では投票用紙に候補者の氏名を記入することが多い．日頃からお互いの筆跡を知っていると，投票用紙の筆跡から投票者と投票内容の関係が推定できる．

(3) 観察による推定の可能性が大きい

互選など同じ室内で投票を行う場合，手の動きや表情を観察することで投票内容の推定が可能である．

実際に匿名性が低下しない場合でも，上記の理由により投票者が匿名性低下の可能性を感じているときは，自由に投票することができない．

また小規模投票では関与者間の利害関係がある場合が多いので，買収や強制が行われやすい．大規模投票に比べ少数の票を操作するだけで結果に影響を与えることができる．少数の候補者に対して買収や強制を行っても露見しにくい．

2.2. 電子投票規模の大小比較

電子投票の課題は応用により異なるが，大まかに言うと大規模電子投票では，物理的な投票と同程度の安全性を保ちつつ効率や利便性を向上させる必要がある．それに対し小規模電子投票では，物理的な投票と同程度の効率を保ちつつ，匿名性や買収耐性を向上させる必要がある．

2.3. 得票数秘匿型電子投票の要件

本論文では小規模電子投票の課題のうち匿名性の維持を目的とし，得票数の秘匿により匿名性を維持する方式を提案する．そのためにまず投票の結果を二つに分けて考える．

結果①：得票数(各候補者の得票数や，信任/不信任の得票数，議案の賛成/反対の得票数)．

結果②：結論(当選者，信任/不信任，議案の可否)．

この分類に基づき匿名性を以下の二つに分けて考える．

匿名性①：得票数の公開により得られた情報から推定される以上の，投票者と投票内容を関係づけるのに必要な情報が得られないこと．

匿名性②：当選者，信任/不信任，議案の可否などの公開により得られた情報から推定される以上の，投票者と投票内容を関係づけるのに必要な情報が得られないこと．

従来の電子投票で扱っていた匿名性は基本的に匿名性①に相当する．本研究では匿名性②を要件とする．なお，匿名性②は匿名性①を包含しており，より強い要件である．

匿名性②を要件としたことにより公開検証可能性を以下のように定義する

公開検証可能性：全投票者が当選者，信任/不信任，議案の可否などの投票の結論に対し，その妥当性を検証できること．

そのほかの用件は従来と同様である．

有権者確認可能性：有権者のみが投票者になれること．

公平性：投票締め切り以前に投票の途中経過を知ることができないこと．

頑健性：不正者が存在しても選挙を遂行できること．

二重投票不能性：有権者が決められた票数のみ投票できること．

3. 従来の電子投票

3.1. 電子投票の主な方式

従来の電子投票の主な方式を述べる.

準同型性暗号利用方式:投票者以外に複数の集計者を必要とする.各投票内容を暗号化したまま集計を行うことができる.投票は信任投票に限られるため,複数の候補がいる投票では信任投票を平行して行う.投票内容の正当性を示すためゼロ知識証明を用いるため大規模投票には向かない.

Mix-net 方式:Mix サーバと呼ばれる管理者を必要とする.暗号化された投票のリストを複数の Mix サーバが協力して復号化し,その順番を入れ替え再暗号化して出力する.出力された結果から集計を行う.Mix サーバが 1 つでも正しく動作すれば投票者と投票内容が結びつかない.投票内容に制限はない.Mix サーバの動作を保証するためにゼロ知識証明が必要であり,大規模投票には向かない.

ブラインド署名利用方式:選挙管理者,集計者,匿名通信路で構成される.投票者は投票内容に対するブラインド署名を選挙管理者から得る.投票者は署名付きの投票を匿名通信路で集計者に送信する.集計者は署名のついた投票を公開し集計する.投票内容に制限はない.大規模投票に最も向いている.

マルチパーティプロトコル利用方式:投票者のみで構成され,管理者や集計者を必要としない.投票内容を入力として,それを集計する関数を計算するマルチパーティプロトコルを利用する.投票者間の通信量や計算量が大きく,大規模投票には不向きである.投票内容は投票ごとに定められた形式に従う必要がある.

各方式の特性を表 1 にまとめる.

表 1:各電子投票方式の比較

方式	集計者	信任投票以外	自由記述	規模
準同型性暗号利用	必要	不可	不可	小,中
Mix-net 利用	必要	可	可	小,中
ブラインド署名利用	必要	可	可	大,中,小
マルチパーティプロトコル利用	不要	可	不可	小

3.2. 従来の得票数秘匿型電子投票方式

文献[6]では,株主総会などの 1 人が複数投票可能な投票を提案している.議案の可否を決めるとき,賛成総数と反対総数を集計するが,投票者の持つ票数が公開されている場合匿名性低下の可能性がある.たとえば 1 人が奇数票,他が偶数票を持っている場合,賛成総数が奇数で反対総数が偶数であれば,奇数票を持つ投票者が賛成に投票したことが判明してしまう.そこで匿名性維持のために賛成総数と反対総数を公開せずに議案の可否だけを公開する方式を提案している.これは閾値型 ElGamal 暗号を基にしており,集計者を複数にし,Boudot の手法を用いることで賛成票数と反対票数を秘匿している.

この方式は小規模投票への適用を目的としたものではなく,複数の集計者を必要とする.また投票内容が議案の可否および信任/不信任であるとき以外に,そのまま用いることはできない.

4. 得票数と匿名性の関係

得票数の公開が匿名性に及ぼす影響を分析する.得票数を公開した場合と秘匿した場合で,投票内容のあいまい性にどれだけ差があるか,2 人の候補者を想定した以下の投票モデルを用いて比較した.引き分けの場合には各候補者の得票数は投票者総数の 1/2 であることが判明し,得票数を秘匿することはできない.そのためここでは引き分けの場合を除外して考える.

＜モデル＞

候補者：C_1, C_2

投票者総数：I

候補者 C_1 の得票数：D_1,候補者 C_2 の得票数：D_2

候補者 C_1 の支持者数：E_1,候補者 C_2 の支持者数：E_2

中立派の人数：N

条件：

- 投票者は候補者 C_1, C_2 のどちらかに必ず投票する.
- 支持者数 E_1, E_2 の値は既知とし,候補者 C_1 の支持者は必ず候補者 C_1 に投票し,候補者 C_2 の支持者は必ず候補者 C_2 に投票する.すなわち,
  $D_1 + D_2 = E_1 + E_2 + N = I$ を満たす.
- 候補者 C_1, C_2 の支持者数 E_1, E_2 は半数未満であるすなわち, $E_1 < \lfloor (I+1)/2 \rfloor (i = 1,2)$ が成立する.
- 当選者は C_1 であり,これは既知とする.

＜考え方＞

(a)得票数を公開したケース,および(b)得票数を秘匿したケースのそれぞれにおいて,中立派の一人が特定の候補者に投票するあいまいさを表すエントロピーを求め,両者を比較する.

＜手順＞

(1) 事象の定義：以下の 2 つの事象 $\tilde{X}, \tilde{Y} \in F$ （F は事象全体の集合）を定義する.

$$\tilde{X} = \{n, n+1, \cdots, N\},\ \tilde{Y} = \{C_1, C_2\}$$

ただし, $n = \lfloor I/2 \rfloor + 1 - E_1$

ここで事象 $\tilde{X}$ は N 人の中立派のうち，C_1 に投票した人数として考えられる全ての結果であり，事象 $\tilde{Y}$ は N 人の中立派から無作為抽出した 1 人が投票した候補者として考えられる全ての結果である．

(2) 事象 $\tilde{X},\tilde{Y}$ に対応する確率変数をそれぞれ X,Y とする．ここで $\tilde{X}$ の要素は X の値にそのまま対応しており，$\tilde{Y}$ の要素は要素 C_1,C_2 をそれぞれ 0, 1 に変換したものを Y の値として用いる．上記より，P_X は次式で与えられると仮定する．

$$P_X(X=x)=1/(N-n+1)$$

(3) 得票数を公開したときの，N 人の中立派から無作為抽出した 1 人が $C_1(C_2)$ に投票する確率は，条件付き確率となり以下のようになる．

$$P_{Y|X}(Y=0\mid X=x)=x/N$$

$$P_{Y|X}(Y=1\mid X=x)=(N-x)/N$$

(4) (a)得票数 $D_1(D_2)$ を公開したケースは，条件付きエントロピー $H(Y\mid X)$ となる．(2)(3)より，(a)投票数を公開したケースのエントロピー $H(Y\mid X)$ は次式となる．

$$\begin{aligned}&H(Y\mid X)\\&=-\sum_{x\in X}\sum_{y\in Y}P_X(X=x)P_{Y|X}(Y=y\mid X=x)\\&\quad\log P_{Y|X}(Y=y\mid X=x)\\&=-(1/N)\sum_{x\in X}\{P_X(X=x)\\&\quad(x\log(x/N)+(N-x)\log((N-x)/N))\}\end{aligned}$$

(5) N 人の中立派から無作為抽出した 1 人が $C_1(C_2)$ に投票する確率は，

$$P_Y(Y=y)=\sum_{x\in X}P_X(X=x)P_{Y|X}(Y=y\mid X=x)$$

より

$$P_Y(Y=0)=1/(N-n+1)\sum_{x\in X}x/N$$

$$P_Y(Y=1)=1/(N-n+1)\sum_{x\in X}(N-x)/N$$

となる．

(6) (5)より (b)得票数を秘匿したケースのエントロピー $H(Y)$ は次式となる．

$$\begin{aligned}&H(Y)\\&=-\sum_{y\in Y}P_Y(Y=y)\log P_Y(Y=y)\\&=-1/(N(N-n+1))\left\{\left(\sum_{x\in X}x\right)\log\left(1/(N(N-n+1))\sum_{x\in X}x\right)\right.\\&\left.+\left(\sum_{x\in X}(N-x)\right)\log\left(1/(N(N-n+1))\sum_{x\in X}(N-x)\right)\right\}\end{aligned}$$

E_1,E_2,N の比を固定し，投票者総数 I を横軸，エントロピーの値を縦軸としたとき，(a)得票数 $D_1(D_2)$ を公開したケースと (b)得票数を秘匿したケースのグラフを以下に示す．

図 2 では $E_1:E_2:N=1:1:1$ である．ここで，◆の系列は得票数を公開したケースのエントロピーを示す．中立派の人数が奇数の場合と偶数の場合でエントロピーが大きく異なる（奇数の場合が大きい）．そのため◆の系列が 2 つ存在するように見えるが実際には 1 系列である．同様に□の系列は得票数を秘匿したケースのエントロピーであり，これも実際には 1 系列である．この図から，得票数を公開したときのエントロピーのほうが小さいことがわかる．

図 3 では $E_1:E_2:N=5:5:1$，図 4 では $E_1:E_2:N=5:4:3$ とした．

また $E_1:E_2:N=1:1:1$ としたときの (a)得票数を公開したケースおよび (b)得票数を秘匿したケースのエントロピーの差，すなわち相互情報量 $I(Y;X)=H(Y)-H(Y\mid X)$ のグラフを図 5 に示す．この場合の相互情報量は，得票数を公開することで，中立派が特定の候補者に投票するあいまいさがどれだけ減少したかを表している．

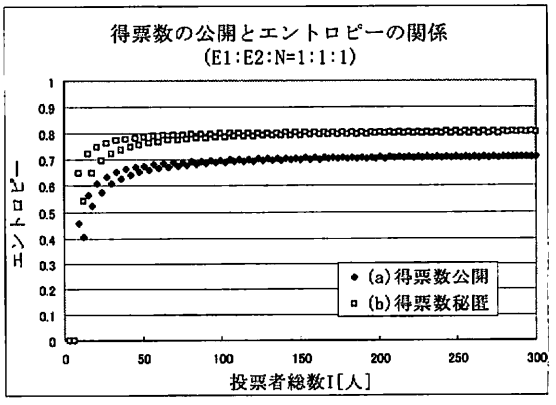

図 2：得票数の公開とエントロピーの関係

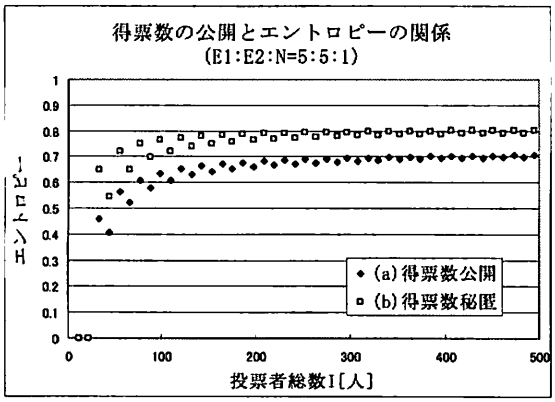

図 3：得票数の公開とエントロピーの関係

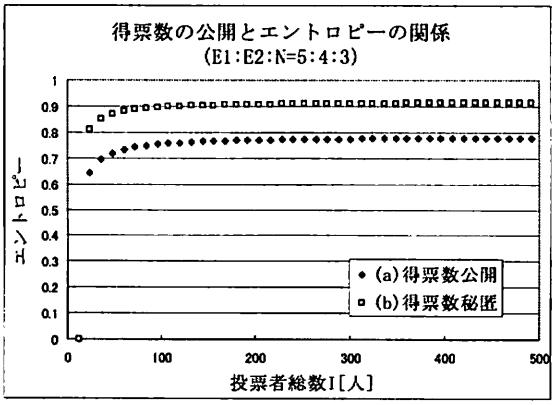

図 4：得票数の公開とエントロピーの関係

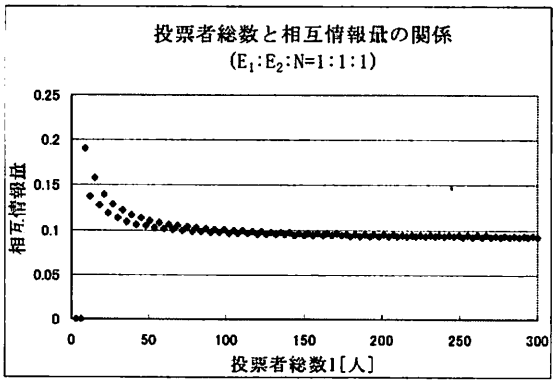

図 5：投票者総数と相互情報量の関係

これらのグラフから，
$P_X(X = x) = 1/(N - n + 1)$ と仮定したとき，以下のことが言える．

・全ての場合について投票者公開時のエントロピーは，投票者秘匿時のエントロピーよりも小さい．

・全ての場合について投票者総数が減少するほどエントロピーは減少する．

・投票者総数が減少するほど投票者秘匿時と公開時のエントロピーの差，すなわち相互情報量が大きくなる．

・支持者数 E_1, E_2 が同数の場合，中立派の人数 N が奇数の方がエントロピーは大きい．

得票数を公開すると中立派の 1 人がどちらの候補に投票したかの不確定度が低下し，低下の度合いは投票者総数が少ないほど大きいことを確認した．

5. 提案方式

5.1. 方針

(1)マルチパーティプロトコルの利用

小規模電子投票では，投票の管理や集計を信頼できる第三者に依頼することは少ない．たとえば大学の教授会や企業内委員会の場合，集計者は大学の事務職員や企業の総務課職員であることが多い．そのため集計者が集計結果をどの候補者，投票者にも話さないという仮定を設けることは適切でない．そこで，集計者を置かずに当選者を求めるマルチパーティプロトコル利用方式に基づいて得票数秘匿型電子投票を提案する．

マルチパーティプロトコルとは，複数の参加者 $A_1, A_2, \cdots$ がそれぞれ秘密情報 $x_1, x_2, \cdots$ を持つ状況下で，秘密情報を秘匿したまま，秘密情報の関数値 $f(x_1, x_2, \cdots)$ を計算する方法である．提案方式では，ブール回路と検証可能な秘密分散によって構成されるマルチパーティプロトコルを用いる．

マルチパーティプロトコルを用いた方式では計算量や通信量が大きくなってしまうが，提案方式は小規模電子投票を想定しているため，現実的な時間で処理可能であると考えられる．

(2)オークションプロトコルの利用

第一価格秘密オークションでは，各入札者は他の入札者の入札値を知らされずに入札し，最高値の入札者がその値で落札する．このとき落札値以外の入札値は秘匿される．入札値を得票数，落札者を当選者と対応づけると得票数秘匿型電子投票方式に類似していることがわかる．第一価格オークションを参考にして，マルチパーティプロトコルを用いた電子投票を拡張することにより，得票数秘匿型電子投票方式を提案する．

5.2. 前提とする第一価格秘密オークション

文献[5]ではマルチパーティプロトコルを用いた第一価格秘密オークションの効率的な方法を提案している．本研究ではこれを採用する．

第一価格秘密オークションプロトコルは，以下の関数をマルチパーティプロトコルにより計算する．

(1) I 人の入札者 $A_i(i=1,...,I)$ がそれぞれ J ビットの入札値 $Bi=(b_i^{(1)},...,b_i^{(J)})$ $(i=1,...,I)$ を入札する．このとき，落札値と落札者だけを公開し，他の入札値を秘匿する．

(2) I 個の入札値 $B_1,...,B_I$ があるとき，入札値の上位 j ビット目を並べた値を V_j $(j=1,...,J)$ とし，以下のように定義する．

$$V_j=(b_1^{(j)},...,b_I^{(j)})$$

(3) W を落札者候補のリストとし，$W=(w_1,...,w_I)$ と定義する．A_i が落札者の候補に残っている場合 $w_i=1$ とし，そうでない場合は $w_i=0$ とする．W の初期値を $(1,...,1)$ とする．

(4) 2つのベクトル $X=(x_1,...,x_I),Y=(y_1,...,y_I)$ があるとき，$X\wedge Y$ を以下のように定義する．

$$X\wedge Y=(x_1\wedge y_1),...,(x_I\wedge y_I)$$

$j=1$ から J まで Step1 から Step2 を繰り返す．

Step1. $S_j=W\wedge V_j$

$$=(w_1\wedge b_1^{(j)},..,w_I\wedge b_I^{(j)})$$

$$b_{\max}^{(j)}=(w_1\wedge b_1^{(j)})\vee\cdots\vee(w_I\wedge b_I^{(j)})$$

Step2. $b_{\max}^{(j)}=1$ のとき，W の値を S_j の値と置き換える．

(5) $W=(w_1,...,w_I)$ において $w_i=1$ のとき，A_i が落札者である．落札値は $B_{\max}=(b_{\max}^{(1)},...,b_{\max}^{(J)})$ である．

5.3. 実現方式

I 人の投票者と，J 人の立候補者がいる．各立候補者の得票数を秘匿しながら，最多得票者を示す．ここで $J=2$ とすると，信任票の数を秘匿しながら信任/不信任の結論を示す信任投票となる．

全体の流れは以下のようになる．投票者が自らの投票内容を秘密分散し各投票者に部分情報を送信する．その後各投票者は他の投票者から送信された部分情報をもとに計算を行う．計算が終了したら各投票者は計算結果を公開する．各候補者の計算結果は，最終結果の部分情報になっているため，すべての候補者の計算結果を統合すると当選者のみが示される．得票数や当選者候補リストから外れた候補者などの計算途中の情報は，投票者全員が結託しないかぎり秘匿できる．

以下の関数をマルチパーティプロトコルにより計算する．

(1) I 人の投票者 $A_i(i=1,...,I)$ が J 人の候補者 $C_j(j=1,...,J)$ のなかから1人を選び，J ビットの投票 $B_1,...,B_I$ $(B_i=(b_i^{(1)},...,b_i^{(J)}))$ をする．候補者 C_j に投票するとき $b_i^{(j)}=1$，投票しないとき $b_i^{(j)}=0$ とする．ただし B_i のなかに1はひとつだけとする．

(2) 得票数 Dj は，関数 g を

$g(x_1,...,x_m)=x_1+\cdots+x_m$ とすると

$D_j=g(b_1^{(j)}+\cdots+b_I^{(j)})$ となる．

ここで，$Dj=(d_j^{(1)},...,d_j^{(L)})$ と表す．D_j のビット数 L は，$L=\lceil\log_2 I+1\rceil$ となる．

(3) V_l を $V_l=(d_1^{(l)},...,d_J^{(l)})$ $(l=1,...,L)$ と定義する．

(4) W を当選者候補のリストとし，$W=(w_1,...,w_J)$ と定義する．C_j が当選者の候補に残っている場合 $w_j=1$ とし，そうでない場合は $w_j=0$ とする．W の初期値を $(1,...,1)$ とする．

(5) 2つのベクトル $X=(x_1,...,x_I),Y=(y_1,...,y_I)$ があるとき，$X\wedge Y$ を以下のように定義する．

$$X\wedge Y=(x_1\wedge y_1),...,(x_I\wedge y_I)$$

$l=1$ から L まで以下の Step1 から Step2 までを繰り返す．

Step 1. $S_l=W\wedge V_l$

$$=(w_1\wedge d_1^{(l)},...,w_J\wedge d_J^{(l)})$$

$$d_{\max}^{(l)}=(w_1\wedge d_1^{(l)})\vee\cdots\vee(w_J\wedge d_J^{(l)})$$

Step 2. $d_{\max}^{(l)}=1$ のとき，W の値を S_l の値に置き換える．

(6) $W=(w_1,...,w_J)$ において $w_j=1$ のとき，C_j が当選者である．

例として，4人の投票者 A_1，A_2，A_3，A_4 が3人の候補者 C_1，C_2，C_3 の中から1人を選ぶ場合を示す．このとき，I=4，J=3 である．

(1) 投票者 A_1，A_2，A_3，A_4 がそれぞれ候補者 C_3，C_1，C_2，C_2 へ投票したとすると，投票 B_1，B_2，B_3，B_4 は $B_1=(0,0,1)$，$B_2=(1,0,0)$，$B_3=(0,1,0)$，$B_4=(0,1,0)$ となる．

(2) 得票数 D は，$L=\lceil\log_2 4+1\rceil=3$ より3ビットの値となる．

候補者 C_1 の得票数は $D_1=g(0,1,0,0)=(0,0,1)$

候補者 C_2 の得票数は $D_2=g(0,0,1,1)=(0,1,0)$

候補者 C_3 の得票数は $D_3=g(1,0,0,0)=(0,0,1)$

(3) D_1，D_2，D_3 より V_1，V_2，V_3 は以下のようになる．

$V_1=(0,0,0)$，$V_2=(0,1,0)$，$V_3=(1,0,1)$

(4) $W=(1,1,1)$とする.

(5) $S_1=W\wedge V_1=(0,0,0),\quad d_{\max}^{(1)}=0,$

$S_2=W\wedge V_2=(0,1,0),\quad d_{\max}^{(2)}=1,\quad W:=S_3=(0,1,0)$

$S_3=W\wedge V_3=(0,0,0),\quad d_{\max}^{(3)}=0,$

(6) $W=(0,1,0)$より候補者C_2が当選者となる.

6. 評価

6.1. 安全性

匿名性1:提案方式では,投票の結論である当選者しか出力しない.得票数など結論を導くのに必要な計算過程の情報は,マルチパーティプロトコルの性質により,投票者全員が結託しない限り秘匿される.情報の秘匿に関する安全性はマルチパーティプロトコルの安全性に帰着する.

匿名性2:投票者は投票内容を秘密分散し,その部分情報を全ての投票者に分配する.投票者全員が結託しない限り投票内容は復元できない.この安全性もマルチパーティプロトコルの安全性に帰着する.

有権者確認可能性:部分情報を分配する際に投票者の電子署名を付ければ,投票権を持たない者が投票しようとして他の投票者に部分情報を送っても,不正な投票だと判明する.

頑健性:マルチパーティプロトコルの頑健性に帰着する.

二重投票不能性:有権者確認可能性により,同じ投票者が2回投票することを防ぐことができる.5.3節の投票形式より,1回の投票で同じ候補者に複数票投票することはできない.1回の投票で複数の候補に1票ずつ投票することを防ぐのは今後の課題である.

公平性:すべての投票が終わってから計算を始めるので,投票の前に投票結果の一部を知ることはない.

公開検証可能性:有権者確認可能性,頑健性,二重投票不能性が満たされている場合には,投票結果の正当性はプロトコルの正当性により保証されると考えられるが,今後更に検討が必要である.

6.2. 効率

マルチパーティプロトコルではブール回路のANDゲートとNOTゲートに対して定められた手続きを行う.ANDゲートは投票者間での通信が必要なので,全体の処理効率はANDゲート数に影響される.そのためマルチパーティプロトコルの効率はANDゲートの数によって評価されることが多い.本研究ではそれにならい,候補者の得票数を集計する回路と提案方式の回路のANDゲート数を比較した.

投票者数$I(I\geq 2)$,候補者数Jとする.得票数を集計する回路に必要なANDゲートの数は,得票数の表現に必要なビット数Lとすると,

$$4JL(I-1)$$

である.

提案方式の回路に必要なANDゲートの数は,

$$4JL(I-1)+L(2J-1)$$

である.

比をとると

$$\frac{4JL(I-1)+L(2J-1)}{4JL(I-1)}<1+\frac{1}{2(I-1)}$$

となる.

$I\geq 2$より

$$1+\frac{1}{2(I-1)}\leq 1.5$$

となる.

提案方式に必要なANDゲートの数は,候補者の得票数を集計するだけの電子投票に必要なANDゲート数に比べ,高々1.5倍である.

7. まとめ

小規模電子投票では,物理的な投票と同程度の効率を保ちつつ,匿名性や買収耐性を向上させる必要があることを示した.得票数の公開が匿名性の低下につながることを定量的に示した.匿名性を二つに分けて厳密化し,その定義を元に得票数秘匿型電子投票方式を提案した.

小規模投票では投票者や候補者と集計者が既知の関係であることが想定される.そこで集計者を必要としないマルチパーティプロトコルを用いた電子投票方式に基づき,電子オークションプロトコルを参考にして,得票数を秘匿した.

提案方式の安全性を評価し,新たに定義した匿名性および有権者確認可能性,公平性,頑健性はマルチパーティプロトコルの安全性に帰着することを示した.

今後の課題は二重投票不能性および公開検証可能性のより厳密な検証である.

謝辞

電気通信大学情報通信工学科の太田和夫教授には,オークションプロトコルについて御教授いただきました.ここにお礼を申し上げます.

文　献

[1] 岡本龍明, 山本博資, 現代暗号, 産業図書, 東京, 1997

[2] 岡本龍明, 太田和夫, 暗号・ゼロ知識証明・数論, 情報処理学会監修, 共立出版, 東京, 1995

[3] 黒沢薫, 尾形わかは, 電子情報通信レクチャーシリーズ～現代暗号の基礎数理, コロナ社, 東京,

2004
[4] 甘利俊一, 情報理論, ダイヤモンド社, 東京, 1970
[5] K. Kurosawa, W. Ogata," Bit-Slice Auction Circuit," In Proceedings of ESORICS2002, volume2502, pp.24- 38, 2002.
[6] 税所哲朗, 齊藤泰一, 土井洋, 辻井重男," 重み付き投票の電子化とその安全性に関する考察," 情報処理学会論文誌, Vol.44, No.8, pp.1913-1923, 2003
[7] 税所哲郎, 齊藤泰一, 土井洋, 辻井重男," 1人複数投票可能な電子投票に関する一考察 一株主総会における議決権行使プロトコルの実現—," 情報処理学会研究報告. CSEC, 17, 2002
[8] 情報理論とその応用学会, 暗号と認証, 培風館, 東京, 1996
[9] 山口浩, 大久保美也子, 北沢敦, 辻井重男," 電子投票・アンケート諸方式に対する比較考察," 情報処理学会研究報告. CSEC, 17, 2002
[10] 境隆一, 笠原正雄," 電子投票方式に関する考察," Proc. of SCIS 2006, 2006