電子投票と電子入札

佐古　和恵

1. はじめに

暗号技術は単なる情報の秘匿や認証機能に留まらず，紙ベースでの情報交換と同様の安全性を電子社会で実現し，さらに紙ベースでは困難であった新機能を実現するメカニズムを提供してくれる有望な技術である．複雑な機能は，暗号化，署名といった単一の機能を応用した処理や手続きを，規定された方法で多者間で情報をやりとりすることによって実現できる．これらの手続きを暗号プロトコルと呼ぶ．本稿では，電子投票，電子入札において電子化に伴うデメリットを解消し，さらに現行の方式では実現が困難な機能を提供する暗号プロトコルを紹介する．

2. 投票の要件

無記名投票に求められる要件として

- 非有権者の投票や二重投票などの不正投票防止
- 誰が何に投票したのかを秘匿するプライバシー保護

の2点がある．

例えば，紙ベースの選挙では，人手で投票者を認証している．すなわち投票受付で投票者がまだ投票していない有権者であることを確認し，確認されたら紙の投票用紙を渡している．これによって確認された人のみが投票でき，不正投票が防止できる．また，各投票者に同じ投票用紙が渡されるので，集計箱に集まった投票用紙を見てもどの投票者が投函したものか知ることができない．したがって投票の秘密が守られる．

ICカードなどを使って電子的に投票者を認証する手段はあると仮定して，上記の方式をそのまま電子化したらどうなるであろうか．共通の投票用紙であれば投票者に個別に渡す必要はなく，投票者は投票内容を電子的な投票データとして送付することになる．では，投票者確認を行なった投票者の投票データを受理すればよいのだろうか？　このようにすると，この投票データがどの投票者のものかわかってしまい，投票の秘密が守られない．かといって，投票者確認と投票データ受付を独立に行なうと，不正投票への対策が施せない．そこで，この不正投票防止とプライバシー保護を実現するために，暗号技術を用いた投票プロトコルが有効となる．

暗号技術を用いると，さらに**集計結果の検証**が可能になる．紙ベースの投票では，自分の投票内容が集計結果に確実に反映されていることを直接確認することは困難である．電子投票ではこれも可能になる．

ところで，投票の秘密を知っている当の投票者が，正しく集計されているのを検証できるという機能は，コンピュータの検索機能があればそれほど難しいことではない．そしてこの機能には限界もある．すなわち，自分の投票が正しく集計されていることが確認できても集計結果全体の正当性は保証できない．そこで，暗号プロトコルを用いると，当事者でなくても，第三者が投票の秘密を保証しつつ集計結果全体の正当性を確認できるようにすることができる．

さて，このように誰が何に投票したかわからないが，不正投票や不正集計のない結果であることを保証するプロトコルはどのように実現できるのであろうか．本稿では例として3つの方式を紹介する．第一の方式はブラインド署名という技術を用いて，単一のセンタにより実現できる投票方式である．これは実用的な方式であるが，匿名通信路がいること，投票者が自分の投票しか検証できないというデメリットがある．第二，第三の方式は共に複数のセンタで権限を分散して運営する投票方式である．処理はやや複雑になるが，第三者が全集計が正しく計算されたことを確認できる方式になっている．

以下では，各方式について紹介する．

さこ　かずえ
NECインターネットシステム研究所
〒216-8555 川崎市宮前区宮崎4-1-1

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

3. ブラインド署名を用いた単一センタ方式

3.1 概要

この方式はブラインド署名[1]という特別な技術を用いる．通常の署名では，あるメッセージに対して本人が本人の秘密鍵を用いて署名処理を行なう．ブラインド署名でも本人が本人の秘密鍵を用いて署名処理を行なうのであるが，このとき，本人はどのメッセージに署名しているのか，メッセージがブラインド（目隠し）されていてわからない，という性質を持つ．通常の使い方では，自分の知らない文章に対して署名を付与することは考えにくい．しかし，電子投票のようにプライバシーを保護する必要のあるとき，このような性質の署名が有効に作用するのである[2]．

投票プロトコルを説明する．便宜上，認証センタと集計センタにわけて話をすすめるが，後述のようにこれらは同一のセンタが兼ねることができる．まず，投票者を認証する認証センタが電子的に投票者確認を行なう．次に，確認できた投票者の投票データを上述のブラインド署名という技術によって，投票者は投票データの内容を見せずに認証センタの署名を付与してもらう．次に，投票者はこの認証センタの署名付きの投票データを投票箱代わりの集計センタに提出する．集計センタは，投票者を確認する必要はなく，投票者の提示した投票データに認証センタの正しい署名が付与されているかどうかを確認して，投票データを受理する．

このようにすれば，認証センタによって確認された投票者のみの投票データを受理することができる．認証センタは投票者名は見られるが，投票データの中身はわからず，集計センタは投票データは見られるが投票者は誰かわからないので投票の秘密を守ることができる．

しかし，これだけでは，有権者が二重投票をすることを防ぐことができない．すなわち，認証センタの署名つきの投票データを何度も集計センタに送りつけることにより，複数票分の投票ができてしまうのである．そこで，投票データの一部分にランダムな文字パターンを入れることにする．これにより，同一の有権者が同じ投票データを送付しても1票分としてのみ数えることができる．また，投票者がこの文字パターンを書き留めておけば，公開された受理投票データの一覧を検索して自分の投票データが確実に集計されていることを確かめることができる．なお，二人の投票者が偶然同一の文字パターンを選択してしまう確率を低くするために，このパターンは十分長くとる必要がある．

3.2 具体的なプロトコル

ここでは，RSA署名に基づくブラインド署名プロトコルを紹介する．RSA署名[19]は，公開鍵(e, n)に対して，$d\cdot e=1 \bmod lcm(p-1, q-1)$となる$d$が秘密鍵になる．ここで$p, q$は$p\cdot q=n$となる大きな素数であり，$lcm(a, b)$は$a$と$b$の最小公倍数を意味する．あるメッセージ$m$に対しての署名文は，$s=m^d \bmod n$となる．署名文の正当性を確認するためには，$s^e \bmod n=m$が成立することを検証すればよい．この式が成り立つのは，任意のαに対して

$$\alpha^{e\cdot d} \bmod n=\alpha \tag{1}$$

が成り立つからである．

さて，投票者は投票データmに対する認証センタの署名文$s=m^d \bmod n$を入手したいのだが，投票データmは認証センタに見せたくない．そこで，投票者は投票データにある細工をして認証センタに渡す．その細工とは，ランダムな数rを選んでmの代わりに

$$m'=m\cdot r^e \bmod n$$

を渡すのである．この結果，mがrによって隠されてしまい，認証センタはmを知り得ない．認証センタは投票者を認証できれば，m'に対して

$$s'=(m')^d \bmod n$$

を計算して返す．このとき，$s'=(m\cdot r^e)^d=m^d\cdot r^{e\cdot d} \bmod n$であり，式(1)より，投票者は

$$s'/r=m^d \bmod n$$

を入手できる．

このブラインド署名を使う場合に，いくつか気をつける点がある．たとえば，不正投票者がm'として，ランダムな数r_1, r_2を使って

$$m'=m\cdot r_1^e\cdot r_2^e \bmod n$$

と計算するかもしれない．この結果得られた$s'=(m')^d \bmod n$を用いて，それぞれ$m, m\cdot r_1^e, m\cdot r_2^e$に対する署名文を$s'/r_1\cdot r_2, s'/r_2, s'/r_1$から生成できてしまう．この結果，1回の登録で$m, m\cdot r_1^e, m\cdot r_2^e$という3つの正しい署名付きの投票文を生成でき，すべてを投票センタに送れば3票分の投票ができてしまうという不正が成り立ってしまう．そこで，有効な投票データのフォーマットに冗長性を付与し，$m, m\cdot r_1^e$がともに有効な投票データにならないようにする配慮が必要になる．

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

たとえば，投票データフォーマットをM＝投票内容を示すデータ，R＝ランダムな文字パターンとし，

$$M\|R\|h(M\|R)$$

を投票データとすることができる．ここで‖は文字の連結であり，hはハッシュ関数である．このRは前述の通り，多重投票を防ぐための識別子としての役割を果たす．

3.3 メリットデメリット

ブラインド署名を用いた本方式は，認証センタと集計センタが結託しても，認証と投票データを送付するタイミングが独立であり，誰が投票データを送付したかを類推できなければ，投票の秘密が洩れない．したがって，単一のセンタが両センタの機能を兼ねることができる．ただ，投票者が投票データを送付するときに，投票者に関する情報がもれないような匿名通信路で送付する必要がある．ここでIPアドレスなどにより投票者が特定できてしまうと，投票の秘密は守れない．このような匿名通信路を実際にどう構築できるかは，大きな問題である．

4. 権限分散による複数センタ方式

本章で紹介する2方式は，匿名通信路の存在に安全性の根拠をおくのではなく，「複数のセンタが結託しない」という前提に根拠をおく安全な方式になっている．これらの方式では，認証センタに投票者認証をしてもらった時に直接暗号化した投票データを提出する．この暗号投票データの復号権限を認証センタ以外の複数のセンタに分散させることにより，投票の秘密を守るのである．各センタが協力すれば，最終的に投票データが復号され，集計結果を得ることができる．

この場合でも，最終的に復号結果を公表し，投票者がユニークに埋め込んだランダム文字列を検索することによって，各投票者が集計されていることを確認することができる．しかし，より望ましい方式，すなわち，投票の秘密を知らない第三者であっても集計結果全体の正当性を確認できるようにすることができる．

集計結果の正当性を示すためには，復号プロセスが正しいことを示す必要がある．受け取った暗号投票データをそのまま復号してみせてしまうと復号プロセスの正しさは証明できても，明らかに投票の秘密が守られない．そこで，受け取った暗号投票データになんらかの処理を施して，公開してもいい復号対象の暗号データを生成する必要がある．具体的には

(1) 暗号データをシャッフルする処理を挿入[3]～[5]

(2) 暗号データを統合する処理を挿入[6]～[9]

という二つの方針が知られている．まず，これらに共通に用いられる確率暗号およびゼロ知識証明について触れたあと，各方針の代表的な方式について簡単に説明する．

4.1 確率暗号について

暗号時にランダム成分を利用する暗号方式を確率暗号[10]といい，例としてElGamal暗号[11]があげられる．ElGamal暗号では，素数p，生成元gに対して秘密鍵xと公開鍵(y, p, g)の関係は

$$y=g^x \bmod p$$

で与えられる．この公開鍵(y, p, g)でメッセージmを暗号化する場合，乱数rを発生させ，

$$(g^r \bmod p,\ m\cdot y^r \bmod p)$$

が暗号文となる．

暗号文(G, M)に対して復号は，秘密鍵xを用いて

$$M/G^x \bmod p$$

によりmが求められる．同じメッセージmでも，乱数rの取り方により暗号文が異なってくること，乱数成分を知らなくても復号ができることがElGamal方式の特徴となっている．

また，この方式では，暗号文の集合と復号結果の集合を公開しても，それらの対応が秘匿できるという特徴がある．たとえばRSA暗号のように決定的な暗号アルゴリズムの場合は復号結果を公開鍵を用いて暗号化してみてどの暗号文と等しくなるかにより，暗号文と復号結果の対応が容易にわかる．しかし，ElGamalのような確率暗号の場合，乱数成分rがあるため，このような対応が秘匿される．

4.2 ゼロ知識証明について

ゼロ知識証明とは，洩れる知識をゼロにして命題を証明することである．ここではそのしくみについて詳細には述べないが，NP命題であれば，ゼロ知識証明プロトコルを構成することができること[12]を紹介しておく．

たとえば，上述のElGamal暗号文(G, M)を復号した結果がmになったことを，秘密鍵xに関する情報を一切漏らすことなく証明することができる．これは，$(y, p, g), (G, M), m$が与えられて

$$\exists x \text{ s.t. } y=g^x \bmod p \text{ AND } M/m=G^x \bmod p$$

というNP命題を証明すればよい．証明の過程でxを用いるけれども，証明文には秘密鍵xの情報は洩れないのである．

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

同様に，ElGamal暗号文(G, M)はm_1，あるいはm_2を暗号化した結果であることを，どちらであるかを漏らすことなく証明することができる．これは，$(y, p, g), (G, M), m_1, m_2$が与えられて

$\exists r$ s.t.

$(G, M)=(g^r, m_1 \cdot y^r)OR(G, M)=(g^r, m_2 \cdot y^r)$

ということをrに関する情報を漏らさずに証明するのである．

4.3 シャッフル処理を用いる方式

この投票方式では，受け取った暗号データの順番を入れ替え（シャッフル）して，過不足なくシャッフルしたことと，シャッフル後の個々の暗号データを正しく復号したことの証明を付与することにより，集計結果の正当性を保証するものである．

では，どのようにシャッフルをすればよいのであろうか．シャッフル前とシャッフル後のデータを公開するという前提では，単なるデータの並び変えでは対応を秘匿することができない．そこで，暗号データを，復号結果を変えずに別の暗号データに変換するという処理が必要になる．この処理は「再暗号化」と呼ばれる．

前節で紹介したElGamal暗号の例をとってみよう．ElGamalの暗号文(G, M)に対して，乱数r'を発生させ，公開鍵(y, p, g)を用いて

$(G', M')=(G \cdot g^{r'} \bmod p, M \cdot y^{r'} \bmod p)$

により再暗号文(G', M')を得る．この再暗号文の復号結果はもともとの暗号文の復号結果に等しくなるが，(G', M')と(G, M)をみてもその関係はわからない．この結果，暗号データの表面を変えて対応がわからないようにシャッフルすることができる．また，正しくシャッフルしたかどうかはNP問題であるので，ゼロ知識証明を用いればその対応を秘匿してシャッフルの正しさを証明できる．

4.4 暗号データ統合処理を用いる方式

この方式では，個々の暗号投票データを復号するのではなく，あらかじめ暗号データを「統合」し，その結果を復号することにより投票結果を得るのである．簡単のために，賛成/反対の二値の投票を考える．賛成票を1，反対票を0で表現すると，これらの値を加算した結果が賛成票の総数になる．そこで，暗号文のまま暗号投票データを加算し，その結果の暗号データを復号すれば，投票の結果を得ることができる．それぞれの暗号投票データを直接復号しないので，投票の秘密を守りつつ，復号処理の正当性を示すことができる．

暗号データを統合するためには，準同型性のある暗号関数が有用である．前述のElGamal暗号はこの性質を持つ．すなわち，$(g^{r_1}, m_1 \cdot y^{r_1})$と$(g^{r_2}, m_2 \cdot y^{r_2})$をかけあわせると，$m_1 \cdot m_2$の暗号文が得られる．そこで，賛成票のメッセージをある定数V，反対票のメッセージを1として，投票者はいずれかの値を暗号化する．全暗号データを乗算した結果を復号し，その底Vの離散対数を求めれば，これが賛成票の総数になる．暗号データの乗算を誰でもできるので，乗算結果の復号処理のみ正しいことを確認すれば，集計結果が正しいことが保証できる．

ただし，不正な投票者がV^2の暗号文を暗号投票データとして提出すると，これは2票の賛成投票と同値になる．したがって，各投票者が自分の暗号投票データはVあるいは1の投票データであること，そしてそのどちらであるかを知られないようにゼロ知識証明で証明する必要がある．

なお，この方式は統合できる投票メッセージに制限があるため，自由記述形式の投票を集計するには向かない．

5. 電子入札プロトコル

5.1 封印メカニズムとは

紙ベースの入札では，入札値を記入した入札書を封じて期日までに開札者に届け，開札日に開札者がすべての入札書を開封し，その中で最小（あるいは最大）の入札値を申請していた人が落札者となる．これを電子的に行なうにはどうしたらよいであろうか．入札値を他人に知られないように封印する機能と，封印されたものが改変されることなくそのままの形で開封できる機能が必要になる．

通常の暗号化では入札値を秘匿できても，それが後日意図的に異なるように復号することを防止する機能はない．たとえば，ある鍵Kで入札値を暗号化すれば，Kが漏洩しない限り入札値は秘匿される．しかし，開封する時点でKではなく，K'を提示すれば，復号結果はもともとの入札値と異なるものとなってしまい，封印時点での入札値を保証できない．

そこで，暗号技術を応用してこのような封印機能を実現することが研究されている[13]．これを用いれば公平に電子入札を実現することができる．さまざまな封印メカニズムが知られているが，次節ではハッシュ関数を用いたものを紹介する．

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

5.2 ハッシュ関数を用いた封印メカニズム

暗号研究の中で，ハッシュ関数はデジタル署名を効率よく実現する技術として研究がすすめられてきた[14]．すなわち，長いメッセージ全体に対して署名処理を行なう代わりに，ハッシュ化した値に署名しても安全性が失われないハッシュ化方法が模索されてきた．この結果，

(1) 任意長のデータを入力として一定長のハッシュ値を出力する

(2) 同じハッシュ値になる2つのデータを探すことは困難

という性質を満たすハッシュ関数が実用化されている[15]．

性質(1)から明らかなように，本関数は多対1の写像になっている．そして(2)の性質から，ハッシュ値から逆像を求めるのが難しい，一方向関数になっていることが多い．このような一方向ハッシュ関数を利用すれば封印メカニズムが実現できる．封印したい値をハッシュ化して，その結果を公表する．ハッシュ関数が一方向なので，ハッシュ値からもとの値を求めることが困難になっている．開封するときは，封印していた値そのものを提示する．この値が封印した値であることを確認するためには，ハッシュ値を比較してみればよい．異なる値を提示しても性質(2)から同じハッシュ値になる可能性はほとんどないので，不正開封が検出される．

6. 入札値を秘匿する入札プロトコル

5章で紹介した封印メカニズムを用いれば，紙ベースの入札と同様に公平な電子入札が実現できる．

ところで，紙ベースの入札では，すべての入札値を開封しないと落札値が決定できない．このことは，開札者に対して入札値を秘匿できないということである．さらに，開札者が最大の値を落札値をして決定したことを保証するためには，全入札値を公開する必要が生じる．

入札プロトコルを工夫すれば，すべての入札値を開封しなくても，封印した状態にある処理を加えることで最大値である落札値を求めることができる．さらに，この落札値が最大であることを，他の入札値を封印したまま証明することができる．

具体的には誰が処理を行なうかによって二通りの方法が知られている．

(1) 開封権限が分散された複数のセンタが行なう[16]

(2) 各入札者が常に関与して行なう[17]，[18]

以下ではそれぞれの方法について紹介する．

6.1 開封権限を複数のセンタに分散させる方法

この方式では封印メカニズムとして公開鍵のインデックスを用いる[16]．まず，入札可能な値の集合$\{v_1, v_2, \cdots, v_{N-1}, v_N\}$に対してElGamal公開鍵$\{P_{v_1}, P_{v_2}, \cdots, P_{v_{N-1}}, P_{v_N}\}$と対応する秘密鍵$\{s_{v_1}, s_{v_2}, \cdots, s_{v_{N-1}}, s_{v_N}\}$が作成され，秘密鍵は複数の開札センタに分散される．入札者が値v_bを入札したいとき，公開されている公開鍵の集合とある決められた定数Mを用いてこの入札値を

$$P_{v_b}(M)$$

により暗号化する．Mを知っていても，$P_{v_b}(M)$からどのP_{v_b}が使用されたかがわからないので，これはv_bを秘匿する暗号文となっている．

開札は全センタが協力して行なう．まず，全部の暗号入札値を，入札可能な最大値v_Nに対応するx_{v_N}で復号を試みる．この結果Mに復号される暗号入札値があれば，これはP_{v_N}を用いて暗号化されたものであるから，最大値のv_Nを入札したものであることがわかる．もし，どの暗号入札値もMに復号されない場合には，次に$x_{v_{N-1}}$により復号を試す．このようにして，最初にMに復号される暗号入札値が見つかった時のv_tが落札値であり，落札者はx_{v_t}でMに復号される暗号入札値を入れた入札者である．落札者が見つかった時点でそれ以上の復号処理を試行しなければ，他の入札者の入札値は開札者にも秘匿される．

6.2 入札者が開封に関与する方法

上記の方式では複数のセンタに開封権限を委ねているので，入札者が何も関与しなくてもいいメリットがあるが，少なくとも1つのセンタを信頼する必要がある．ここでは，入札者自身が関与することによりセンタを信頼しなくても入札値を秘匿できる方法を紹介する[18]．

入札可能な値の集合$\{v_1, v_2, \cdots, v_{N-1}, v_N\}$に対して，入札値を$v_b$にすることは，$v_b$には入札するが，$\{v_{b+1}, v_{b+2}, \cdots, v_{N-1}, v_N\}$には入札しないということである．そこで，乱数$L_{b-1}$を発生させ，

$$L_b = hash(yes \| L_{b-1})$$

$$L_i = hash(no \| L_{i-1}) (i = b+1, \cdots, N)$$

によりL_Nを計算し，L_Nを公開する．

開札時にはすべての入札者が同席する必要がある．まず，v_Nが落札値であるかどうかを確かめるため，

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

全入札者はL_{N-1}の提示を求められる．このとき$L_N = hash(yes \| L_{N-1})$となる人がいればその人が落札値$v_{L_N}$で落札したことになる．全員が$L_N = hash(no \| L_{N-1})$の場合，次に全入札者は$L_{N-2}$を提示し，落札値が決まるまで続けられる．

7. まとめ

暗号技術を用いて，紙ベースでの情報交換では困難であった複雑な機能が実現できることを電子投票，電子入札を例にとって紹介した．これからも電子化に伴うデメリットを解消し，さらにより望ましい機能を提供する技術として，暗号研究への期待は大きい．

参考文献

[1] Chaum: "Security without identification: transaction systems to make big brother obsolete", Communications of the ACM, pp. 1030-1044 (1985).

[2] 太田:「単一の選挙管理者を用いた電子投票方式」, 電子情報通信学会春季全国大会 A-294 (1988).

[3] Chaum: "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, pp. 84-88 (1981).

[4] Sako, Kilian: "Receipt-free mix-type voting scheme-A practical solution to the implementation of a voting booth", Advances in Cryptology—EUROCRYPT '95, pp. 393-403 (1995).

[5] Abe: "Mix-networks on permutation networks", Advances in Cryptology—ASIACRYPT '99, pp. 258-273 (1999).

[6] Cohen (Benaloh) Yung: "Distributing the power of a government to enhance the privacy of voters", Annual Symposium on Principles of Distributed Computing, pp. 52-62 (1985).

[7] Sako, Kilian: "Secure voting using partially compatible homomorphisms", Advances in Cryptology—Crypto '94, pp. 411-424 (1994).

[8] Cramer, Franklin, Schoenmakers, Yung: "Multi-authority secret-ballot elections with linear work", Advances in Cryptology—EUROCRYP '96, pp. 72-83 (1996).

[9] Cramer, Gennaro, Schoenmakers: "A secure and optimally efficient multi-authority election scheme", Advances in Cryptology—EUROCRYPT '97, pp. 103-118 (1997).

[10] Goldwasser, Micali: "Probabilistic encryption", J. of Comp. and Syst. Sci., pp. 270-299 (1984).

[11] ElGamal: "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. on Information Theory, pp. 469-472 (1985).

[12] Goldwasser, Micali, Wigderson: "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems", Journal of the ACM, pp. 691-729 (1991).

[13] Blum: "Coin flipping by telephone", Proc. of COMPCON, IEEE, pp. 133-137 (1982).

[14] 岡本, 山本:「現代暗号」, 産業図書 (1997).

[15] Menezes, van Oorschot, Vanstone: "Handbook of applied cryptography", CRC Press (1996).

[16] Sako: "An auction protocol which hides bids of losers", Public Key Cryptography 2000, pp. 422-432 (2000).

[17] Sakurai, Miyazaki: "A bulletin-board based digital auction scheme with bidding down strategy", International Workshop on Cryptographic Techniques and E-Commerce, pp. 180-187 (1999).

[18] 鈴木:「逐次開示可能なコミットメントによる効率的な入札方式」, 信学技報 ISEC99-67 (1999).

[19] Rivest, Shamir, Adleman: "A method for obtaining digital signature and public-key cryptosystems", Communications of the ACM, pp. 120-126 (1978).

© 日本オペレーションズ・リサーチ学会. 無断複写・複製・転載を禁ず.