同報環境に適した無記名投票プロトコルの一例

5T－4

紙田　剛　武藤　康史　高木　和幸　岡田　謙一　松下　温
慶応義塾大学

1　はじめに

昨今、ＬＡＮ等の同報通信機能を備えた通信網が注目されている。同報環境においては、通信情報の秘密保持が重要な課題となる。我々は、遠隔地間での会議という環境を設定し、ＵＮＩＸシステム上に、暗号通信を基本とする会議システムを実装した。

本件では、その一機能として、我々の考案した同報暗号通信鍵管理方式（ＭＣＫ）を利用した、電子無記名投票プロトコルを提案する。従来は、基本的に、投票者以外に選挙管理委員と集計者が必要で、これらに不正がないことが大前提とされているが、ＭＣＫの利用により、委員の権限を軽減し、集計者を排除することで、より簡素で効率的な無記名投票を行うことができる。

2　無記名投票成立の条件

無記名投票の満たす条件として、以下の五つが考えられる。

(1)　投票者と投票の対応は、他人にわからない。
(2)　二重三重の投票は認めない。
(3)　非有権者が投票できない。
(4)　有権者、非有権者にかかわらず、他人の投票、集計結果を改ざんできない。
(5)　投票が公平である。つまり、他人の投票内容を知ってから投票できない。

3　同報暗号鍵管理方式（ＭＣＫ）

本件で用いる、同報環境に適した、暗号通信のための鍵管理方式について説明する。

3.1　暗号法

現在の暗号法は、大きく分けて、秘密鍵暗号系と公開鍵暗号系の二つに分類される。

秘密鍵暗号系では、暗号化鍵と復号化鍵が共通で、通信者間で秘密にされる。公開鍵暗号では、暗号化鍵が公開され、復号化鍵が秘密にされる。通信する側は、公開されている通信相手の暗号化鍵で暗号化し、通信を受ける側は、自分の復号化鍵で復号化する。

3.2　鍵管理システム

秘密鍵暗号系における通信は、一対一であり、通信相手が増加するとそれにともなって、管理する鍵も増加していった。最近ではグループ化が進み、グループ用の鍵も必要になってきた。しかし、それぞれ個別の鍵で暗号化しようとすると、管理する鍵の数が多すぎて、管理しきれなくなってしまう。

3.2.1　鍵管理

そこで我々は、こういった状況を考慮し、秘密鍵暗号系に対し、グループ化に対応できる鍵管理システムを考案した。それぞれのユーザーは、図一のように共通鍵Ｋ0と、鍵を生成するために使われる補助情報（以後これをピースと呼ぶ）を持つ。各ユーザーは、それぞれある一つのピース以外を持つことになるのだが、ここでは便宜的にユーザーＵｉはピースＰｉを持たないことにする。

	P1	P2	P3	P4	P5	K0
U1	×	○	○	○	○	○
U2	○	×	○	○	○	○
U3	○	○	×	○	○	○
U4	○	○	○	×	○	○
U5	○	○	○	○	×	○

図1．各ユーザーが持つピース

3.2.2　鍵の生成

実際に通信に用いる鍵の生成法を説明する。例えば、ピースＰｉを使って鍵を生成したい場合は、

$$G = f(K0、Pi)$$

という一方向関数ｆ（）によってＧを生成する。複数のピースによって鍵を生成する場合は、

$$G = f(\ldots f(f(K0, P1), P2), \ldots, Pi)$$

とする。

ユーザーＵ１とＵ４が通信する場合、それぞれの共通鍵Ｋ0とピースＰ2，Ｐ3，Ｐ5を持っているので、これらより鍵Ｇを生成する。Ｕ1とＵ4以外に、このＫ0、Ｐ2，Ｐ3，Ｐ5を全て所有するユーザーはいないので、他のユーザーは、この鍵Ｇを生成することはできない。また、ユーザーＵ2、Ｕ3、Ｕ5がグループを形成したい場合には、Ｋ0とピースＰ1，Ｐ4より鍵Ｇを生成する。さらに、全員で通信をしたい場合は、共通鍵Ｋ0を用いればよい。

3.2.3　管理する鍵の数

ユーザーがｎ人いる場合、この方式では、各ユーザーが管理する鍵の数は、グループの数にかかわらず、共通鍵１個とピースｎ－１この和ｎ個である。これに対し従来の方式では、ｍ個のグループに属していれば、自分を除いたｎ－１人のとの鍵と、ｍ個のグループ用鍵を合わせてｎ＋ｍ－１個となる。従って、我々の方式の方が少ないことがわかる。

4　提案方式

従来の電子無記名投票プロトコルでは、投票者以外に、有権者を定め、投票参加権を与える選挙管理委員と、投

An Exanple of Secret Vote Protocol Suitable for Broadcast environment

Takeshi Kamita　Yasushi Mutoh　Kazuyuki Takagi　Kenichi Okada　Yutaka Matushita
Keio University

票の集計者が必要とされる。本件では、遠隔地間での電子通信会議という環境を設定している。会議のメンバーのうち一人が無記名投票を発起し、それ以外の選挙に必要なメンバーが投票者となる。この発起人が、選挙管理委員の役割を果たし、投票参加権を発行する。集計は、全投票が、各投票者に同報され、各々で行う。

4.1 プロトコル

1. 投票参加権の発行
   (1) 発起人Pは、乱数xを発生させる。
   (2) Pは、xを会議メンバーのうち、選挙に必要なメンバー（Pを含む）を含むグループ鍵G0を生成し、これでxを暗号化したもの
   $$GID = f(x, G0)$$
   を同報する。xを所持することが、投票権を持つことになる。xは、後に投票内容を暗号化する鍵となるが、その復号化鍵yを、ここでPが生成する。（図2. phase① ）
2. 投票
   (3) 投票者iは、GIDよりxを求め、自分のピース全てと共通鍵K0より、
   $$ID = f(\ldots f(f(x, P1), P2), \ldots, Pn), K0)$$
   を生成する。IDは、個人固有の情報で、後に二重投票を発見するのに用いられる。
   (4) 投票内容Vを、xで暗号化する。
   $$Vx = f(V, x)$$
   (5) グループ鍵G1（発起人Pを含まない）を生成し、これでx，ID、Vxを暗号化し、同報する。（図2. phase② ）
3. 集計
   (6) 各メンバーに、投票が順次集められ、G1によって復号化される。xより、投票が投票資格のあるメンバーのものかどうかが、また、IDより二重投票があるかないかが判明する。
   (7) 締切時間に、Pはyを同報する。各メンバーのシステムで、Vxがyによって復号化され、投票内容が集計される。
   （図2. phase③ ）

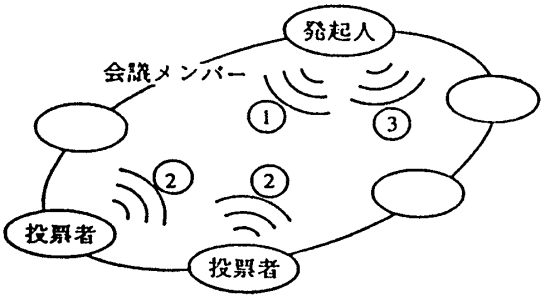

図2.通信の順番

5 検討

MCKを用いることで、グループ鍵を扱えるという時点で、あらかじめ投票者が正当な有権者であることが認められる。それゆえ、発起人は投票参加権を発行するが、整理券程度の意味しか持たず、従来の選挙管理委員のように、有権者自体を設定する権限はない。また、集計者を省くことができ、集計を各自が行うので、責任が分散され、システムがより安全で、簡素かつ効率的になる。

では、以下で、本方式が、2で述べた無記名投票成立の条件を満たすかどうか、順に検討する。

(1) 無記名性

投票者は、投票内容（xで暗号化したもの）と、IDをいっしょに伝送する。IDは個人固有のものであるが、誰のものであるかは分からないので、投票者と投票の対応は、他人にはわからない。さらに通信内容全体をG1で暗号化しているので、発起人もわからない。

(2) 二重投票の発見

IDは個人固有であるので、二重投票がなされても、IDを比較すれば発見できる。

(3) 非有権者による投票

非有権者は、有権者グループに対応するグループ鍵の生成が不可能であるために、投票は不可能である。

(4) 投票及び集計結果の改ざん

投票内容Vは、xで暗号化され、さらに発起人を含まないグループ鍵G1で暗号化されて伝送される。従って、外部のものは、伝送中及び開票前の投票内容を操作することはできない。発起人も、(1)で述べた理由で操作できない。集計は各自が行い、集計結果は、開票と同時にわかるので、集計結果を操作することはできない。

(5) 公平性

投票内容は、xによって暗号化されており、各投票者のシステムで蓄積されていくが、締切時間に発起人がyを発送しない限り、投票者は内容を見ることができない。したがって、他人の投票内容を見てから、投票することはできない。

6 おわりに

本研では、暗号通信による電子通信会議システムの一機能として、我々の考案したMCKを利用した、無記名投票の一方式を提案した。この方式の利点は、MCKの利用により、従来の方式より

- 通信回数を大幅に削減した。
- 役割分担を減らし、簡素化した。
- 集計を各投票者が行うことで、責任を分散し、より安全にした。

等の点である。

7 参考文献

[1] 吉倉、林、”電子無記名投票の一方式の提案”、ISEC90−46
[2] 浅野、松本他、”公平な電子無記名投票の一方式”、ISEC90−35
[3] 武藤、中村他、”グループに適した暗号化鍵の管理と配送システム”、
情報処理学会第42回（平成3年前期）全国大会