

準同形の一方方向性関数を用いる無記名電子投票の検討

小林 哲二

(* 日本工業大学 〒345-8501 埼玉県宮代町学園台 4-1-1 情報棟)

1. はじめに

電子投票は、投票者の名前と投票用紙記載内容に対応付けるか否かによって、記名投票と無記名投票に分類できる。ネットワークを利用する安全な無記名電子投票を実現することは、情報社会への意義が多岐であるが、現状はまだ発展段階にある。従来提案されている無記名投票方式において、ブラインド署名や Mix-net による方式の欠点は複雑な匿名通信路が必要なことなどであり、準同形性を有する暗号を使用する方式の欠点は処理が複雑なことなどである[1]。

この発表では、準同形一方方向性関数(準同形性を有する一方方向性関数)を利用して無記名投票を実現する新しい方式を提案し、ネットワーク会議用の無記名電子投票に適用する場合について、投票のプロトコル(処理手順)と簡単な数値例を示して、提案方式の有用性を考察する[2]。

2. 電子投票システムのモデル

準同形一方方向性関数を用いるネットワーク会議用の無記名電子投票のモデルを図 1 に示す。ネットワーク会議用電子投票システムは、投票管理者(議長)と投票管理端末(パソコンなど)、投票者と投票端末(パソコン又は携帯電話など)、投票サーバ(投票管理)、及び信頼サーバ(信頼できる補助のサーバ)で構成する。これらの構成要素間の通信における一般的な安全性は、通常のセキュリティ技術で保護する[3]。

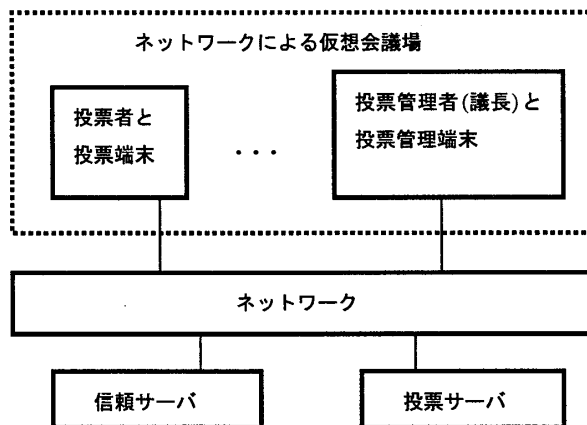


図 1 ネットワーク会議用の無記名電子投票のモデル

A Secret Voting Method by Using a Homomorphic One-way Function
Tetsuji KOBAYASHI

* Nippon Institute of Technology, 4-1-1, Joho-Building, Gakuendai,
Miyashiro-machi, Saitama-ken, 345-8501 Japan

3. 無記名電子投票方式

準同形一方方向性関数 $f(\cdot)$ は次の性質を有すると定義する。任意の数 $M, M1, M2$ について、 $f(M)$ を計算するのは容易であるが、 $f(M)$ から M を計算するのは困難又は不可能であり、かつ $f(M1) \cdot f(M2) = f(M1+M2)$ である。例えば、 $f(M) = \exp(g, M) \bmod P$, $f(M) = \exp(g, \alpha M) \bmod P$, などの関数で実現できる。ここで、 $\exp(A, B)$ は A の B 乗を表し、定数 $\{g, P, \alpha\}$ は安全性を考慮して適切に定める。

【無記名電子投票の処理手順】

無記名電子投票の処理手順概要を以下に示す。

Step 0 (初期設定) : 投票管理者は、投票者の集合を $\{\text{投票者 } 1, \text{投票者 } 2, \dots, \text{投票者 } n\}$ とし、投票者 k , $(k=1, 2, \dots, n)$ の投票メッセージ(投票内容)を V_k , $(k=1, 2, \dots, n)$ とする。投票管理者は、準同形一方方向性関数 $f(V)$, 及び投票者 k , $(k=1, 2, \dots, n)$ の投票メッセージ $\{V1, V2, \dots, Vn\}$ の取り得る数値を定め、投票サーバと投票端末に設定する。

Step 1 (信頼サーバ) : 信頼サーバは投票者 k , $(k=1, 2, \dots, n)$ に秘密の乱数 S_k , $(k=1, 2, \dots, n)$ を送信する。信頼サーバは、 $[(S1 \cdot S2 \cdot \dots \cdot Sn) \bmod P]$ を投票サーバに送信し、 $(S1, S2, \dots, Sn)$ を秘密に保持する(又は消去する)。投票サーバは、受信した $(S1, S2, \dots, Sn)$ を秘密に保持する。

Step 2 (投票者と投票サーバ) : 投票者 k , $(k=1, 2, \dots, n)$ は、 $W_k \cdot f(V_k) \bmod P$, $(k=1, 2, \dots, n)$ を個々に投票サーバに送信する。 W_k , $(k=1, 2, \dots, n)$ は秘密の乱数である。

Step 3 (投票者間の通信) : 先頭番号の投票者 1 は投票者 2 に $\{S1 \cdot W1 \bmod P\}$ を送信し、投票サーバに確認を送信する。投票者 2 は投票者 3 に $\{(S1 \cdot W1 \cdot S2 \cdot W2) \bmod P\}$ を送信し、投票サーバにその確認を送信する。投票者 3 は、投票者 4 に $\{(S1 \cdot W1 \cdot S2 \cdot W2 \cdot S3 \cdot W3) \bmod P\}$ を送信し、投票サーバにその確認を送信する。以下、同様な動作を各投票者が順次に行う。この結果、最終番号の投票者 n は $\{(S1 \cdot W1 \cdot S2 \cdot W2 \cdot \dots \cdot Sn \cdot Wn) \bmod P\}$ を受信する。

Step 4 (最終番号の投票者) : 投票者 n は投票サーバに $\{(S1 \cdot W1 \cdot S2 \cdot W2 \cdot \dots \cdot Sn \cdot Wn) \bmod P\}$ を送信する。

Step 5 (投票サーバ) : 投票サーバは、
 $A1 = [W1 \cdot f(V1)] \cdot [W2 \cdot f(V2)] \cdot \dots \cdot [Wn \cdot f(Vn)] \bmod P$
 を計算する。ここで、

$$A1 = W1 \cdot W2 \cdot \dots \cdot Wn \cdot f(V1) \cdot f(V2) \cdot \dots \cdot f(Vn) \bmod P \\ = W1 \cdot W2 \cdot \dots \cdot Wn \cdot f(V1+V2+\dots+Vn) \bmod P.$$

次に、投票サーバは、

$$C1 = [(S1 \cdot W1 \cdot S2 \cdot W2 \cdot \dots \cdot Sn \cdot Wn) \bmod P] \\ \div [(S1 \cdot S2 \cdot \dots \cdot Sn) \bmod P] (= (W1 \cdot W2 \cdot \dots \cdot Wn) \bmod P)$$

を計算し、 $(W1 \cdot W2 \cdot \dots \cdot Wn) \bmod P$ を得る。

ここで、 $\bmod P$ の除算は、 $\bmod P$ における逆数を乗じることによって計算できる。次に、投票サーバは

$A2 = A1 / [(W1 \cdot W2 \cdot \dots \cdot Wn) \bmod P] = f(V1 + V2 + \dots + Vn)$ を計算して $A2$ の数値を得る。 $f(\cdot)$ の一方向性によって、投票サーバは $f(V1 + V2 + \dots + Vn)$ から $(V1 + V2 + \dots + Vn)$ を得ることはできない。(例えば、 $f(M) = \exp(g, M) \bmod P$ の場合は、離散対数問題になる。) このことを解決するために、投票サーバは任意の時点で、 $(V1 + V2 + \dots + Vn)$ の取り得る全数値について、事前に $C1 = f(V1 + V2 + \dots + Vn)$ を計算し、計算結果の数値をテーブル $T1$ に格納する。

$T1 = \{C1 (=f(V1 + V2 + \dots + Vn)), (V1 + V2 + \dots + Vn)\}$ 。

入力値から関数 $f(\cdot)$ を計算するのは容易であり、かつ投票者集合は部分集合に分割して 1 個の部分集合ごとの投票者数を適切に設定することも可能なので、事前計算は容易に実行できる。投票サーバは $A2$ の数値を、テーブル $T1$ の各要素と照合し、 $A2 = C1$ の要素を見出した時に、その要素から投票結果の数値 $\{V1 + V2 + \dots + Vn\}$ を得る。

【備考 1】投票サーバが任意の投票者 X から確認を受信しない場合、投票サーバは、現在の投票議題の投票メンバリストから投票者 X を除去する。投票者数が多い場合には、投票者の集合を、複数の部分集合に分割可能であり、その場合は、各部分集合の投票者は、部分集合ごとに上記の無記名投票手順を実行する。

【備考 2】投票メッセージ V_k ($k=1, 2, \dots, n$) は、投票管理者が指定した条件の数値である。例えば投票メッセージに 2 つの選択肢 $\{Yes=1, No=0\}$ が存在する場合、 $(V1 + V2 + \dots + Vn)$ は、 $0 \sim n$ の整数値であるのでテーブル $T1$ には、 $(n+1)$ 個の要素がある。

【備考 3】投票メッセージ V_k ($k=1, 2, \dots, n$) の正当性を保証するために、投票端末のアプリケーションは、投票者が入力した数値の正当性を検査する必要がある。投票端末のアプリケーションは、投票サーバからダウンロードできる。投票端末のアプリケーションの正当性は、投票サーバがアプリケーションにデジタル署名を行うことによって、保証できる。投票サーバが投票端末から投票メッセージを受信時には、投票サーバが投票端末の正当性をデジタル署名によって検証する。

【簡単な数値例】

投票者が 2 人の簡単な数値例を説明のために示す(図 2)。

Step 0 (初期設定)： 準同形一方向性関数は、 $f(V) = \exp(g, V) \bmod P$, $g=2$, $P=97$, 投票メッセージは、 $V=0$ (No)又は 1 (Yes)とする。

Step 1 (信頼サーバ)： 信頼サーバは、秘密乱数 $S1=23$, $S2=53$ を生成し、投票者 1 に $S1$, 投票者 2 に $S2$ を送信し、 $S1 \cdot S2 \bmod P=55$ を投票サーバに送信する。

Step 2 (投票者と投票サーバ間)： 投票者 1 は、 $V1=0$, $W1=88$, $W1 \cdot f(V1) \bmod P=88$, $S1 \cdot W1 \bmod P=84$ を決定し、 $W1 \cdot f(V1)$ を投票サーバに送信する。投票者 2 は、 $V2=1$, $W2=77$, $W2 \cdot f(V2) \bmod P=57$, $S2 \cdot W2 \bmod P=7$ を決定し、 $W2 \cdot f(V2) \bmod P$ を投票サーバに送信する。

Step 3 (投票者間の通信)： 先頭番号の投票者 1 は投票者 2 に $S1 \cdot W1 \bmod P=84$ を送信し、投票サーバにその確認を送信する。

Step 4 (最終番号の投票者)： 最終番号の投票者 2 は、投票サーバに、 $(S1 \cdot W1) \cdot (S2 \cdot W2)=6$ を送信する。

Step 5 (投票サーバ)： 投票サーバの事前計算は $f(0+0)=1$, $f(0+1)=f(1+0)=2$, $f(1+1)=4$, $T1=\{\{1, 0\}, \{2, 1\}, \{4, 2\}\}$ である。

$$A1 = [W1 \cdot f(V1)] \cdot [W2 \cdot f(V2)] \bmod P = 69$$

$$C1 = [(S1 \cdot W1 \cdot S2 \cdot W2) \bmod P] / [(S1 \cdot S2) \bmod P] = 83$$

$$A2 = A1 / [(W1 \cdot W2) \bmod P] = f(V1 + V2) = 2$$

$A2=2$ の数値を、テーブル $T1$ の各要素と照合して、 $A2=C1 (=f(V1+V2))$ となる要素 $\{f(V1+V2), V1+V2\} = \{2, 1\}$ によって、投票集計結果として、 $V1+V2=1$ を得る。

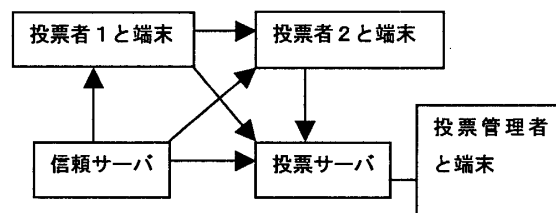


図 2 投票者が 2 人の無記名電子投票のモデル

4. 考察

- (1) 提案方式では、匿名通信路は使用しないが、準同形一方向性関数の性質によって、投票サーバ及び各投票者は、投票者と投票内容の対応付けを行えない。
- (2) 投票サーバは、投票者との通信時に、投票者 ID と投票者パスワードを検査することで多重投票を防止できる。

5. むすび

提案方式の特長は、匿名通信路を使用せずに、無記名投票を比較的容易に実現できることである。投票の安全性や性能等の考察の詳細は発表時に報告する予定である。

参考文献

- [1] 電子情報通信学会：情報セキュリティハンドブック, (2004).
- [2] T.Kobayashi: A Secret Voting Method for Network Meetings by Using a One-way Homomorphic Function, Proceedings of the 2nd Joint Workshop on Information Security (JWIS2007), IEICE, pp. 155-164, Tokyo, Japan, (Aug. 2007).
- [3] 小林哲二：オペレーティングシステム [OS] 基本技術, 日本理工出版会, (May 2006).