L-001

準同形の一方向性関数による無記名の電子投票方式の機能拡張

The Functional Extension of the Secret Voting Method Using a One-way Homomorphic Function

小林 哲二 *

Tetsuji KOBAYASHI

１．はじめに

無記名の電子投票は投票者自身の名前を投票用紙に記載しない形態の電子投票である．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通信量が多いことなどである[1]．この発表では，著者が提案した準同形性を有する一方向性関数による無記名電子投票の実現方式について[2], [3]，機能拡張を行い，ネットワーク会議(ネットワークを利用する室内会議やネットワーク仮想会議)への適用をモデルとして有用性を考察する．

２．無記名電子投票のモデル

準同形の一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．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(信頼できる補助的サーバ)で構成し，投票端末同士も通信可能とする．構成要素間の通信の安全性は通常のセキュリティ技術で保護する[4].

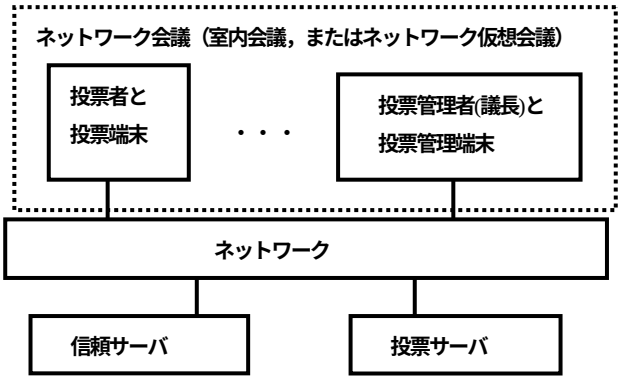

図１　ネットワーク会議用の無記名電子投票のモデル

３．ネットワーク会議用の無記名電子投票

（1）概要： 投票者と信頼サーバの通信，投票者間の通信，及び投票者と投票サーバの通信によって，投票者の投票内容を準同形性の一方向性関数に入力した値を投票サーバに送信する．投票の集計は準同形性一方向性関数によって自動的に計算し，集計値の値を事前計算したテーブルを参照して求める．

* 日本工業大学工学部情報工学科，埼玉県宮代町学園台 4-1-1
Nippon Institute of Technology, Dept. of Computer and Information Engineering, 4-1-1, Gakuendai, Miyashiro-machi, Saitama-ken, 345-8501 Japan.

準同形の一方向性関数 f(・)は次の性質を有する．

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)･f(M2) = f(M1+M2) である．例えば，f(M) = exp(g, M) mod P, f(M)=exp(g, αM) mod 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, α}は安全性を考慮して適切に定める．

（2）無記名電子投票の通信プロトコル

Step 0 (**初期設定**)： 投票管理者は，n 人の投票者の集合を{投票者 1，投票者 2，…，投票者 n}とし，投票者 k, (k=1,2,…,n)の投票内容を Vk, (k=1,2,…,n)とする．各投票者はそれぞれ投票者 ID と投票者パスワードを所有する．投票管理者は準同形の一方向性関数 f(V)を定め，投票の選択肢を投票内容の数値 Vk, (k=1,2,…,n)に対応付けてその取り得る数値を定め，投票サーバと投票端末にアプリケーションを用いて設定する．

f(･)の一方向性によって，f(V1+V2+…+Vn)から (V1+V2+…+Vn) を得ることはできないので，事前に(V1+V2+…+Vn)の取り得る全数値について，C1 = f(V1+V2+…+Vn) を計算し，数値をテーブル T1 に格納する(表１参照).

T1 ={C1 (= f(V1+V2+…+Vn)) , (V1+V2+…+Vn) }

表１　事前計算テーブル T1

f(V1＋V2＋・・・＋Vn)	(V1＋V2＋・・・＋Vn)
f ((V1＋V2＋･･＋Vn) **の最小値**)	(V1＋V2＋・・＋Vn) **の最小値**
・・・	・・・
f ((V1＋V2＋･･＋Vn) **の最大値**)	(V1＋V2＋・・＋Vn) **の最大値**

図２に，投票の選択肢ごとの集計が可能な投票内容 Vk, （k=1,2,・・・,n）のビット列の設定例を示す．各選択肢の集計値は次の条件を満たす．

各選択肢の集計値 ＞ (投票者総数)・(投票の各選択肢の数値)

m 番目 選択肢の 集計値	・・・	２番目 選択肢の 集計値	１番目 選択肢の 集計値

図２　投票の選択肢ごとの集計が可能な投票内容のビット列

投票内容 Vk, (k=1,2,…,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による入力値の正当性を検査する．投票端末はアプリケーションを投票サーバからダウンロードし，

その正当性は，投票サーバがアプリケーションにディジタル署名を行うことによって保証する．投票サーバが投票端末から投票内容を受信時には，投票サーバが投票端末の正当性を投票端末によるディジタル署名によって検証する．

Step 1 (投票者と信頼サーバの通信)： 信頼サーバは，秘密通信によって投票者 k と秘密データ Sk, (k=1,2,…,n)を共有する．

Step 2 (信頼サーバと投票サーバの通信)：信頼サーバは，[(S1･S2･…･Sn) mod P] を投票サーバに送信し，送信完了を確認後に Sk, (k=1,2,…,n)を消去する．投票サーバは，受信した[(S1･S2･…･Sn) mod P]を保持する．

Step 3 (投票者と投票サーバの通信)：投票者 k,(k=1,2,…,n)は，秘密乱数 Wk, (k=1,2,…,n)をそれぞれ生成し，投票者 ID と投票者パスワードによって投票サーバにログインし，
Wk･f(Vk) mod P, (k=1,2,…,n) を投票サーバに送信する．

Step 4 (投票者間の通信)： 先頭番号の投票者 1 は投票者 2 に {S1･W1 mod P}を送信する． 投票者 2 は投票者 3 に {(S1･W1･S2･W2) mod P} を送信する． 投票者 3 は，投票者 4 に{(S1･W1･S2･W2･S3･W3) mod P} を送信する．以下，同様な処理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･W1･S2･W2･…･S_{n-1}･W_{n-1}) mod P}を受信する．

Step 5 (最終番号の投票者 n と投票サーバの通信)：
最終番号の投票者 n は，投票サーバに
{(S1･W1･S2･W2･…･Sn･Wn) mod P}を送信する．

Step 6 (投票サーバによる集計)： 投票サーバは，各投票者および信頼サーバから得たデータによって，次の計算を行う．

A1 = [W1･f(V1)]･[W2･f(V2)]･…･[Wn･f(Vn)] mod P
(= W1･W2･…･Wn･f(V1)･f(V2)･…･f(Vn) mod P
= W1･W2･…･Wn･f(V1+V2+…+Vn) mod P)
B1 = [(S1･W1･S2･W2･…･Sn･Wn) mod P]
／ [(S1･S2･…･Sn) mod P] (= (W1･W2･…･Wn) mod P)
A2 = A1／B1 (= f(V1+V2+…+Vn))

投票サーバは A2 の数値を, 事前計算テーブル T1 のエントリ(行)の要素と照合し，A2 = f(V1+V2+…+Vn) の要素を見出してそのエントリ(行)の要素から投票集計の数値{V1+V2+…+Vn}を得る．

４．考察

(1) 無記名性： 無記名性は準同形性の一方向性関数とそれを利用する通信プロトコルによって確保されており，投票サーバは投票者名と投票内容を対応付けできない(匿名通信路は不要)．

(2) サーバによる投票者の検証： 投票者が投票サーバや信頼サーバへログイン時に，各サーバは，投票者 ID および投票者 ID パスワードによって，各投票者の正当性を検証できる．

(3) 投票内容の正当性： 投票サーバは，送信元のディジタル署名が有効なメッセージだけを用いることによって，投票内容の正当性を保証できる．

(4) １人の投票者による多重投票の検出： 投票者は，投票サーバへのログイン時に投票者 ID を入力するので，同じ投票者が投票を 2 回以上行う場合はその重複によって検出できる．

(5) 各投票者による投票内容の検証： 投票サーバは，投票サーバの処理とデータを公開できるので，投票者はそれぞれ自己の投票が投票集計に含まれていることを，投票サーバからの公開情報で検証できる．投票結果検証者(投票者または部外者)は，投票サーバの公開情報によって投票結果を検証できる．

(6) 結託による不正対策： 信頼サーバは秘密データ Sk, (k=1,2,…,n)だけを知ることができ, かつ投票者間は秘密通信なので，信頼サーバと投票サーバが結託しても，投票サーバは秘密データ Wk, (k=1,2,…,n)を知ることができないから，無記名性を保持できる．信頼サーバと各投票者で秘密データ Sk, (k=1,2,…,n)を共有していることによって，一部分の投票者と投票サーバが結託しても投票サーバは秘密データ Wk, (k=1,2,…,n)を知ることができないから，無記名性を保持できる．

(7) 無記名投票における通信メッセージ総数：

システム全体の通信メッセージ総数 =
信頼サーバと n **人の投票者のメッセージ(合計** n **個)**
＋ 信頼サーバから投票サーバへのメッセージ(合計 1 **個)**
＋ n **人の投票者から投票サーバへのメッセージ(合計** n **個)**
＋ n **人の投票者間のループ状メッセージ(合計(**n−1**)個)**
＋ 最終番号の投票者から投票サーバへのメッセージ(合計 1 **個)**
= n + 1 +n + (n - 1) + 1 = 3n + 1

投票者１人当りの通信メッセージ総数 = (3n + 1) / n = 3 + 1/n.

(8) 事前計算の計算量： １つの投票内容 Vk, (k=1,2,…,n)の選択肢の総数を m とすると，

事前計算テーブルのエントリ総数
＝投票者総数・(選択肢の総数 − 1) ＋1 ＝ n･(m−1)＋1

であるので，事前計算は準同形の一方向性関数 f(・)の計算を，(n･(m−1)＋1）回，行うことで完了する．

(9) 投票者間で通信が不可の場合： 通信方法を変更することによって無記名投票を実現できる．

５．むすび

準同形性の一方向性関数によって無記名電子投票を実現する方式について，機能拡張と有用性を考察した．提案方式の特長は，匿名通信路や準同形暗号を使用せずに，基本的な関数だけで安全な無記名投票を比較的容易に実現できることである．

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： 特願 2008- 56974, 特許出願, (Feb. 2008).
[4] 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).