3M−4

シャッフリングによる高速な大規模電子投票システムの実現

古川 潤 † 佐古 和恵† 森 健吾 † 尾花 賢 † 瀧澤 政明†† 笹村 直樹†† 宮内 宏 †
†NEC インターネットシステム研究所 ††NEC 情報システムズ

1 はじめに

近年, 低い運用費や正確な集計が見込まれるため, 電子投票に期待が集まっている. 電子投票の核となる技術は, 有権者確認のなされた投票者と投票内容との対応を, 不正な集計を許さずに隠す方法である. このような性質を満たす暗号プロトコルは幾つか [4, 1, 5, 2] 知られており, 我々は [3] で [4] の実装を報告した.

今回我々は, シャッフルと部分復号を証明する新しい方式を提案し, これを実装することにより, [3] で提案したシステムを高速化した. 提案方法は, [2] のシャッフルの証明方法と, 部分復号の証明方法を融合した方法で, 単純に両方法を独立に行うよりも高速である.

その結果, 10万票の集計, 正当性証明と正当性検証を PC を用いて 3 時間 44 分で実行できた. また, 証明文と復号文を合わせたデータの量である通信データ量は 200Mbyte となった. 本結果では [3] の結果に比べ, 計算時間がおよそ 1/22 に, 通信データ量がおよそ 1/44 に削減された.

2 シャッフリングに基づく投票システム

2.1 ElGamal シャッフル

有権者確認がなされた投票者と投票内容の対応を, シャッフリングにより隠す方法を述べる. シャッフルとは, n 個の暗号文 $E_1, \ldots, E_n$ から $E'_1, \ldots, E'_n$ への変換で, 次の 2 条件を満たすものである.

条件 1. 復号関数を D としたとき, $D(E'_i) = D(E_{\pi(i)})$ が全ての i に関して成り立つ置換 π が存在する.

条件 2. D を知らなければ, E_i と E'_i からは π に関する情報は漏れない.

条件 1 により, 集計結果の正当性が保証される. 条件 2 により, 投票者と投票内容との対応を隠すことができる。

Realization of Fast and Large Scale Electronic Voting System using Shuffles
† FURUKAWA Jun, Kazue Sako, Kengo Mori, Satoshi Obana
†† Masaaki Takizawa, Naoki Sasamura
† Hiroshi Miyauchi
NEC Internet System Research Laboratories (†)
NEC Informatec Systems (††)

ElGamal 暗号文を用いてシャッフルを行うことを考える. p, q を, $q|p-1$ である二つの素数とし, 位数 q の $(\mathbf{Z}/p\mathbf{Z})^*$ の部分群を $\mathbf{G_q}$ とする. g を $\mathbf{G_q}$ の元とする. $p, q, g, \bar{y}$ を公開鍵とし, $\bar{y} = g^{\bar{x}} \bmod p$ なる $\bar{x} \in \mathbf{Z}/q\mathbf{Z}$ を秘密鍵とする. ここで ElGamal シャッフルは, 暗号文の組 $(G_i, M_i)_{(i=1,\ldots,n)}$ を入力とし, 暗号文の組 $(\bar{G}_i, \bar{M}_i)_{(i=1,\ldots,n)}$ を出力する. 各暗号文の要素は $\mathbf{G_q}$ の元であり, 出力 $(\bar{G}_i, \bar{M}_i)_{(i=1,\ldots,n)}$ は, 無作為に選ばれた π と $\{s_i\}_{(i=1,\ldots,n)} \in_U \mathbf{Z}/q\mathbf{Z}$ を用いて,

$$(\bar{G}_i, \bar{M}_i) = (g^{s_i} G_{\pi(i)}, \bar{y}^{s_i} M_{\pi(i)}) \bmod p$$

により計算される.

2.2 電子投票システム

実装した電子投票システムでは, 前述したシャッフルと復号を複数のセンタで行うことにより, 誰に対しても投票者と投票内容との対応を隠した. また, 各シャッフルおよび復号の正当性を零知識証明を用いて示すことにより, 集計の正当性も保証している.

この零知識証明に, 次節で提案する新しい方法を使うことにより, [3] と比べ大幅な高速化を達成した. 本システムのその他の構成は, [3] と同じであるためここでは説明を省略する.

3 シャッフルと復号の正当性証明方法の提案

以下において, 関数 $\mathcal{H}$ 及び関数 $\tilde{\mathcal{H}}$ をそれぞれ $\mathbf{Z}/q\mathbf{Z}$ 及び $\mathbf{G_q}$ の元を出力する汎用一方向性ハッシュ関数とする. $p, q, g, \bar{y}, G_i, M_i, \bar{G}_i, \bar{M}_i, \pi$ の定義は第 2 節と同じである. 復号用の秘密鍵を x, y を $y = g^x \bmod p$, シャッフルと復号後の暗号文を $\{(G'_i, M'_i)\}_{(i=1,\ldots,n)}$ とする.

証明者 (シャッフルと復号を行うセンタ) は無作為に選んだ置換 π と $s_i \in_U \mathbf{Z}/q\mathbf{Z}$ と復号の秘密鍵 x を使ってシャッフルと復号を次のようにする $(i = 1, \ldots, n)$:

$$(G'_i, M'_i) = \left(g^{s_i} G_{\pi(i)}, \bar{y}^{s_i} M_{\pi(i)} / G_i'^{x}\right) \bmod p$$

$i = 1, \ldots, n$ に関して, 証明者は無作為に, $z, z_i, \rho, \sigma, \tau, \lambda, \lambda_i, z' \in_U \mathbf{Z}/q\mathbf{Z}$ を選び, 次の計算をする.

$$\tilde{g} = \tilde{\mathcal{H}}(p, q, y, 0), \quad \tilde{g}_i = \tilde{\mathcal{H}}(p, q, y, i)$$

$$
\begin{aligned}
v &= g^{\rho}, w = g^{\sigma}, t = g^{\tau}, u = g^{\lambda}, u_i = g^{\lambda_i} \bmod p \\
\tilde{g}_i' &= \tilde{g}^{s_i}\tilde{g}_{\pi(i)}, \quad \tilde{g}' = \tilde{g}^{z}\prod_{j=1}^{n}\tilde{g}_j^{z_j} \bmod p \\
g' &= g^{z}\prod_{j=1}^{n}G_j^{z_j}, \quad m' = \bar{y}^{z}\prod_{j=1}^{n}M_j^{z_j} \bmod p \\
\dot{t}_i &= g^{3z_{\pi(i)}+\tau\lambda_i}, \quad \dot{v}_i = g^{3z_{\pi(i)}^2+\rho s_i} \bmod p \\
\dot{v} &= g^{\sum_{j=1}^{n} z_j^3+\tau\lambda+\rho z} \bmod p \\
\dot{w}_i &= g^{2z_{\pi(i)}+\sigma s_i}, \quad \dot{w} = g^{\sum_{j=1}^{n} z_j^2+\sigma z} \bmod p \\
c_i &= \mathcal{H}(p,q,g,\bar{y},\tilde{g},\{\tilde{g}_j\},\{(G_j,M_j)\},\{(G_j',M_j')\}, \\
&\quad \tilde{g}',\{\tilde{g}_j'\},g',m',v,w,t,u,\{u_j\}, \\
&\quad \{\dot{t}_j\},\dot{v},\{\dot{v}_j\},\dot{w},\{\dot{w}_j\},i:(j=1,\ldots,n)) \\
r_i &= c_{\pi^{-1}(i)} + z_i, \quad r = \sum_{j=1}^{n} s_j c_j + z \bmod q \\
\lambda' &= \sum_{j=1}^{n}\lambda_j {c_j}^2 + \lambda \bmod q \\
\zeta &= \prod_{j=1}^{n} {G_j'}^{c_j}, \quad \eta = \zeta^{x} \bmod p \\
\eta' &= \zeta^{z'}, \quad y' = g^{z'} \bmod p \\
c' &= \mathcal{H}(p,q,g,y,y',\zeta,\eta,\eta') \\
r' &= c'x + z' \bmod q
\end{aligned}
$$

そして, $g', m', \tilde{g}', \tilde{g}_i', v, w, t, u, u_i, \dot{t}_i, \dot{v}_i, \dot{v}, \dot{w}_i, \dot{w}, r, r_i, \lambda', \eta, \eta', y', r' (i = 1, \ldots, n)$ を証明文とする. 証明文と,$\{(G_i', M_i')\}$ を検証者 (シャッフルセンタの出力結果を検証するセンタ) に送る.

検証者は証明者と同様に $(c_i)_{(i=1,\ldots,n)}$ を生成する. 次に,

$$\zeta = \prod_{j=1}^{n} {G_j'}^{c_j} \bmod p$$

を計算し, 証明者と同様に c' を生成する. 検証者は, 以下の式が成り立てばシャッフル復号を正当と見なす:

$$
\begin{aligned}
g^{r}\prod_{j=1}^{n}G_j^{r_j} &= g'\zeta \bmod p \\
\bar{y}^{r}\prod_{j=1}^{n}M_j^{r_j} &= \eta\, m'\prod_{j=1}^{n}M_j'^{c_j} \bmod p \\
\tilde{g}^{r}\prod_{j=1}^{n}\tilde{g}_j^{r_j} &= \tilde{g}'\prod_{j=1}^{n}\tilde{g}_j'^{c_j} \bmod p \\
g^{\lambda'} &= u\prod_{j=1}^{n}u_j^{c_j^2} \bmod p \\
t^{\lambda'}v^{r}g^{\sum_{j=1}^{n}({r_j}^3-{c_j}^3)} &= \dot{v}\prod_{j=1}^{n}\dot{t}_j^{{c_j}^2}\prod_{j=1}^{n}\dot{v}_j^{c_j} \bmod p \\
w^{r}g^{\sum_{j=1}^{n}({r_j}^2-{c_j}^2)} &= \dot{w}\prod_{j=1}^{n}\dot{w}_j^{c_j} \bmod p
\end{aligned}
$$

$$g^{r'} = y^{c'}y' \quad , \quad \zeta^{r'} = \eta^{c'}\eta' \bmod p.$$

4 実装結果

本章では, 実装システムの実行速度及び通信データ量について述べる. 実装システムにおいては, 3 個の機関によるシャッフルと復号, 1 個の機関による検証に要する合計時間と, この時の通信データ量を測定した. 各機関にはそれぞれ 1 台の Athlon 1GHz PC を用い, $|p| = 1024, |q| = 160$ としている. 表 1 に暗号文数が 1 万と 10 万の場合の結果を [3] の結果と比較して示す. また, 集計のみにかかった時間も実測した. これらの値により, 提案方式の実用性が確認された.

項目 / 手法	所要時間		通信データ量 (byte)	
投票者数	1 万人	10 万人	1 万人	10 万人
提案方式	20 分	3 時間 44 分	20M	200M
[3] 方式	8 時間	80 時間	870 M	8.7G
集計のみ	8 分	1 時間 10 分	5 M	50M

表 1: 実測結果

5 まとめ

シャッフリングを用いて高速かつ安全な電子投票システムを設計し、実装した。その結果、3 個の機関でシャッフルと復号を行い 1 個の機関で検証した場合, 10 万票の集計, 正当性証明, 正当性確認を 3 時間 44 分で実行することができた. 集計のみならば 1 時間 10 分で実行できた. この時の通信データ量は 200Mbyte であった. 今後は楕円曲線暗号を用いるなどして、さらに効率を挙げていきたい.

参考文献

[1] M. Abe: "Mix-networks on permutation networks," *Advances in Cryptology - ASIACRYPT '99*, 258-273, Springer-Verlag, 1999.

[2] Furukawa J., K. Sako: "An Efficient Scheme for Proving a Shuffle," *Advances in Cryptology - CRYPTO 2001*, Springer-Verlag, 2001.

[3] 佐古, 古川, 森, 尾花, 瀧澤, 笹村, 宮内: "シャッフリングによる大規模電子投票システムの実現," 情報処理学第 62 回全国大会 6G-1, 3-117, 2001.

[4] K. Sako, J. Kilian: "Receipt-Free Mix-Type Voting Scheme," *Advances in Cryptology - Eurocrypto'95*, 393-403, Springer-Verlag, 1995.

[5] 古川 潤: "効率の良い全体検証可能なシャッフル" SCIS 2001, 15B-2