SCIS 2003 The 2003 Symposium on Cryptography and Information Security
Hamamatsu,Japan, Jan.26-29,2003
The Institute of Electronics, Information and Communication Engineers

準同型暗号系に基づいた分割可能な複数票電子投票方式
Divisible Voting Scheme Based on Homomorphic Cryptosystem

石田 夏樹* 尾形 わかは*
Natsuki Ishida Wakaha Ogata

あらまし 分割可能な複数票投票とは, 各投票者の持ち票が複数であり, 複数の候補者に持ち票を分割して投票できる投票形式である. このような投票形式が用いられる具体的な例としては, 株主総会における投票がある. 本稿では, ある特殊な性質を持つ自然数の多重集合として *Divisible Multiset* を定義し, これを準同型性に基づく電子投票方式と組み合わせることによって, 安全な分割可能な複数票電子投票方式を提案する. 提案方式では, 各投票者が複数の候補者に持ち票を分割して投票する際, 暗号化及びゼロ知識証明を持ち票数に対して log オーダ回行なえばよく, 単純に既存の単票電子投票方式を各投票者の持ち票数回繰り返す場合に比べ, 効率的である.

キーワード 電子投票, 多候補者選挙, 複数票投票, 準同型性, *Divisible Multiset*

1 はじめに

今までに提案された電子投票方式には, Yes か No のいずれかを選択する信任投票, 複数の候補者のいずれかを選択する多候補者選挙, 任意の投票内容を投票可能な投票などがある. これらの電子投票方式の多くは, 各投票者の持ち票が一票である, 単票投票形式である. これに対して, 各投票者の持ち票が複数票である, 複数票投票形式がある. 複数票投票形式が用いられる具体的な例としては, 株主総会における投票がある. 複数票投票形式には, 各投票者が, 選択した一候補者に持ち票をすべて投票する形式 [11] と, 複数の候補者に持ち票を分割して投票できる形式 [12] がある. 本稿では, 後者の分割可能な複数票投票形式を扱う.

分割可能な複数票投票形式は, 既存の電子投票方式（例えば, 準同型性に基づく電子投票方式 [1]〜[5],[7],[8],[10]）を用いて実現できるが, 各投票者の持ち票の分割を秘匿にするには, 単純な方法だと, 単票投票を各投票者の持ち票数回繰り返すこととなり, 効率的ではない.

本稿では, まず最初に, 各投票者が複数の候補者に持ち票を分割する際に用いる, ある特殊な性質を持つ自然数の多重集合 *Divisible Multiset* を定義し, *Divisible Multiset* の要素数を持ち票数に対して log オーダにできることを示す. 次に, 準同型暗号系に基づいた分割可能な複数票電子投票方式を提案する. 提案方式では, *Divisible Multiset* の要素数回の投票で済むので, 効率的である.

* 東京工業大学, 〒 152-8550 東京都目黒区大岡山 2-12-1, Tokyo Institute of Technology, 2-12-1, O-okayama, Meguro-ku, Tokyo, 152-8550, Japan, { ishida, wakaha } @crypt.ss.titech.ac.jp

2 準備

2.1 準同型暗号系

$E(\cdot)$ を確率的公開鍵暗号系の暗号化アルゴリズムとする. $E(\cdot)$ が準同型な性質を持つとは, 任意の平文 m_1, m_2 に対して $E(m_1 + m_2) = E(m_1) \times E(m_2)$ となる演算子 $(+, \times)$ が存在することである. 準同型な性質を持つ確率的公開鍵暗号系の例としては Paillier 暗号 [9] がある.

Paillier 暗号に対しては, 暗号文が特定の複数の平文のいずれかを暗号化したものであることをゼロ知識証明で示すことが可能であり, 秘密鍵を分散共有することで復号に閾値法を用いることが可能である. [6]

2.2 分割可能な複数票電子投票方式

分割可能な複数票電子投票方式は, 松尾ら [12] によって提案された. 松尾らは, 分割可能な複数票電子投票方式として Divisible Voting Scheme（以後 DVS と記す）を以下のように定義した.

DVS は, 投票サーバと, n 人の投票者 $\mathcal{V}_1, \ldots, \mathcal{V}_n$ によって構成されるマルチパーティープロトコルである. 投票者 $\mathcal{V}_i$ は $N^{(i)}$ 票を持っているとする. 投票者は持ち票を分割して M 通りの選択肢 $A_1, \ldots, A_M$ に投票する. ここで, $A_1, \ldots, A_M$ に対する票数をそれぞれ $v_1^{(i)}(\geq 0), \ldots, v_M^{(i)}(\geq 0)$ と記述する. すると, すべての i に対して $\sum_{j=1}^{M} v_j^{(i)} = N^{(i)}$ が成り立つ必要がある. 投票サーバは, すべての j に対して $\sum_i v_j^{(i)}$ を求める.

ここで, 以下の条件を満たすとき, DVS はセキュアであると言う.

健全性: いかなる投票者 $\mathcal{V}_i$ も, 自分の持ち票数 $N^{(i)}$ を超える投票はできない. すなわち,

$$0 \leq v_j^{(i)} \leq N^{(i)} \ (1 \leq i \leq n, 1 \leq j \leq M)$$

$$\sum_{j=1}^{M} v_j^{(i)} = N^{(i)} \ (1 \leq i \leq n)$$

完全性: 健全性を満たすすべての投票に対して, 投票サーバはすべての j に対して集計結果 $\sum_i v_j^{(i)}$ を正しく出力する.

プライバシ: 投票サーバと投票者は集計結果 $\sum_i v_j^{(i)}$ $(1 \leq j \leq M)$ 以外のいかなる情報も得ない. ただし, 各投票者 $\mathcal{V}_i$ の持ち票数 $N^{(i)}$ と, 各 $\mathcal{V}_i$ が投票に参加したかどうかは公開でもよい.

3 Divisible Multiset

本章では, 次章で提案する DVS において, 各投票者が複数の選択肢に持ち票を分割する際に用いる *Divisible Multiset* を定義し, *Divisible Multiset* の要素数を持ち票数に対して log オーダにできることを示す.

定義 3.1 自然数 M,N に対して, 次式を満たす自然数の多重集合 X を (M,N)-*Divisible Multiset* と定義する.

$$\forall n_1 \in \mathbb{N} \cup \{0\} \ \cdots \ \forall n_M \in \mathbb{N} \cup \{0\} \left(\sum_{i=1}^{M} n_i = N \rightarrow \right.$$
$$\exists X_1 \subseteq X \ \cdots \ \exists X_M \subseteq X \left(\bigcup_{1 \leq i \leq M} X_i = X \wedge \right.$$
$$\left. \left. \forall i \in \{1, \ldots, M\} \left(\sum_{n \in X_i} n = n_i \right) \right) \right)$$

□

例 3.2 任意の自然数 M,N に対して, N 個の 1 からなる自然数の多重集合 X は (M,N)-*Divisible Multiset* である. このとき, $\sum_{i=1}^{M} n_i = N$ を満たす任意の非負の整数 $n_1, \ldots, n_M$ に対して, n_i 個の 1 からなる自然数の多重集合を X_i とすると,

$$\bigcup_{1 \leq i \leq M} X_i = X \ , \ \forall i \in \{1, \ldots, M\} \left(\sum_{n \in X_i} n = n_i \right) \quad (1)$$

を満たす. □

上記の例で分かるように, 要素数が N である (M,N)-*Divisible Multiset* を構成することは容易である. 次の定理では, $M = 2$ のとき, 要素数が $O(\log N)$ である (M,N)-*Divisible Multiset* を構成できることを示す.

定理 3.3 任意の自然数 N に対して, 要素数が $\lfloor \log_2 N \rfloor + 1$ である $(2,N)$-*Divisible Multiset* が存在する. □

(証明)

$N = 1$ のとき, 自然数の多重集合 $X = \{1\}$ は明らかに $(2,1)$-*Divisible Multiset* である. 以下では, $N \geq 2$ のときについて証明する. 任意の自然数 N に対して, 次式が成り立つ.

$$\begin{aligned} N &= \left(2^{\lfloor \log_2 N \rfloor} - 1\right) + \left(N - 2^{\lfloor \log_2 N \rfloor} + 1\right) \\ &= \left(\sum_{i=0}^{\lfloor \log_2 N \rfloor - 1} 2^i \right) + \left(N - 2^{\lfloor \log_2 N \rfloor} + 1\right). \end{aligned}$$

$2^{\lfloor \log_2 N \rfloor} \leq N$ より $N - 2^{\lfloor \log_2 N \rfloor} + 1 \geq 1$. 自然数の多重集合 X を

$$X = \left\{2^i \mid 0 \leq i \leq \lfloor \log_2 N \rfloor - 1\right\} \cup \left\{N - 2^{\lfloor \log_2 N \rfloor} + 1\right\}$$

とする. 以下では, X が $(2,N)$-*Divisible Multiset* であることを証明する. n_1, n_2 を $n_1 + n_2 = N$ を満たす非負の整数とする. $0 \leq n_1 \leq n_2 \leq N$ としても一般性を失わない. $2^{\lfloor \log_2 N \rfloor} \leq n_1$ と仮定すると $N < 2^{\lfloor \log_2 N \rfloor + 1} \leq n_1 + n_2$ より $n_1 + n_2 \neq N$ となるので,

$$n_1 \leq 2^{\lfloor \log_2 N \rfloor} - 1 \quad (2)$$

である. $n_1 = 0$ のとき, $n_2 = N$ となるので,

$$X_1 = \phi \ , \ X_2 = X$$

とすると, 式 (1) を満たす. $n_1 \geq 1$ のとき, n_1 の 2 進数表現を $\left(\beta_{\lfloor \log_2 n_1 \rfloor}, \ldots, \beta_0\right)$ とし,

$$\begin{aligned} X_1 &= \left\{2^i \mid 0 \leq i \leq \lfloor \log_2 n_1 \rfloor, \beta_i = 1\right\} \\ X_2 &= X - X_1 \end{aligned}$$

とする. 式 (2) より $\lfloor \log_2 n_1 \rfloor \leq \lfloor \log_2 N \rfloor - 1$ となるので,

$$X_1 \subseteq \left\{2^i \mid 0 \leq i \leq \lfloor \log_2 N \rfloor - 1\right\} \subset X$$

である.

$$\sum_{n \in X_1} n = \sum_{i=0}^{\lfloor \log_2 n_1 \rfloor} \beta_i 2^i = n_1$$

及び

$$\sum_{n \in X_2} n = \sum_{n \in X} n - \sum_{n \in X_1} n = N - n_1 = n_2$$

より, 式 (1) を満たす. □

例 3.4 $N = 100$ のとき,

$$X = \{1, 2, 4, 8, 16, 32, 37\}$$

は $(2,100)$-*Divisible Multiset* である. 例えば, $n_1 = 45$, $n_2 = 55$ に対して,

$$X_1 = \{1, 4, 8, 32\} \ , \ X_2 = \{2, 16, 37\}$$

とすると, 式 (1) を満たす. □

次の定理では, $M \geq 3$ のとき, 要素数が $O(M\log N)$ である (M,N)-*Divisible Multiset* を構成できることを示す.

定理 3.5 3 以上の整数 M, 任意の自然数 N に対して, 要素数が $(M-1)\left(\left\lfloor \log_2 \left\lceil \frac{N}{M} \right\rceil \right\rfloor + 1\right)+1$ 以下である (M,N)-*Divisible Multiset* が存在する. □

(証明)

任意の自然数 N に対して, 次式が成り立つ.

$$N = \sum_{i=1}^{M} \left(\left\lfloor i\frac{N}{M} \right\rfloor - \left\lfloor (i-1)\frac{N}{M} \right\rfloor \right).$$

N_i $(1 \leq i \leq M)$ を

$$N_i = \left\lfloor i\frac{N}{M} \right\rfloor - \left\lfloor (i-1)\frac{N}{M} \right\rfloor$$

とする. N_i は明らかに非負の整数である. $N_i \leq \left\lfloor \frac{N}{M} \right\rfloor - 1$ と仮定すると $\left\lfloor i\frac{N}{M} \right\rfloor \leq \left\lfloor (i-1)\frac{N}{M} \right\rfloor + \left\lfloor \frac{N}{M} \right\rfloor - 1$ となり $\left\lfloor i\frac{N}{M} \right\rfloor > i\frac{N}{M} - 1$ 及び $\left\lfloor (i-1)\frac{N}{M} \right\rfloor + \left\lfloor \frac{N}{M} \right\rfloor - 1 \leq (i-1)\frac{N}{M} + \frac{N}{M} - 1 = i\frac{N}{M} - 1$ より矛盾となるので,

$$\left\lfloor \frac{N}{M} \right\rfloor \leq N_i \tag{3}$$

である. $\left\lceil \frac{N}{M} \right\rceil + 1 \leq N_i$ と仮定すると $\left\lfloor (i-1)\frac{N}{M} \right\rfloor + \left\lceil \frac{N}{M} \right\rceil + 1 \leq \left\lfloor i\frac{N}{M} \right\rfloor$ となり $\left\lfloor (i-1)\frac{N}{M} \right\rfloor + \left\lceil \frac{N}{M} \right\rceil + 1 > \left((i-1)\frac{N}{M} - 1\right) + \frac{N}{M} + 1 = i\frac{N}{M}$ 及び $\left\lfloor i\frac{N}{M} \right\rfloor \leq i\frac{N}{M}$ より矛盾となるので,

$$N_i \leq \left\lceil \frac{N}{M} \right\rceil \tag{4}$$

である. 式 (3) 及び式 (4) より

$$\left\lceil \frac{N}{M} \right\rceil - 1 \leq \left\lfloor \frac{N}{M} \right\rfloor \leq N_i \leq \left\lceil \frac{N}{M} \right\rceil \tag{5}$$

である. また,

$$N_M = N - \left\lfloor (M-1)\frac{N}{M} \right\rfloor \geq N - (M-1)\frac{N}{M} = \frac{N}{M} > 0$$

より N_M は自然数である.

$N_i = 0$ $(1 \leq i \leq M-1)$ のとき, $Y_i = \phi$ とする. $N_i \geq 1$ $(1 \leq i \leq M-1)$ のとき, $(2, N_i)$-*Divisible Multiset* を Y_i とする. $Y_M = \{N_M\}$ とする. 自然数の多重集合 X を

$$X = \bigcup_{1 \leq i \leq M} Y_i$$

とする. 式 (4) 及び定理 **3.3** より

$$|X| = \sum_{i=1}^{M-1} |Y_i| + |Y_M| \leq (M-1)\left(\left\lfloor \log_2 \left\lceil \frac{N}{M} \right\rceil \right\rfloor + 1 \right) + 1$$

である.

以下では, X が (M,N)-*Divisible Multiset* であることを証明する. n_i $(1 \leq i \leq M)$ を $\sum_{i=1}^{M} n_i = N$ を満たす非負の整数とする. $0 \leq n_1 \leq n_2 \leq \cdots \leq n_M \leq N$ としても一般性を失わない. 次式が $j = M-1$ のとき成立することを数学的帰納法で示す.

$$\exists X_1 \subseteq X \ \cdots \ \exists X_j \subseteq X \left(\bigcup_{1 \leq i \leq j} X_i \subseteq \bigcup_{1 \leq i \leq j} Y_i \wedge \forall i \in \{1, \ldots, j\} \left(\sum_{n \in X_i} n = n_i \right) \right) \tag{6}$$

最初に, $j = 1$ のとき式 (6) が成立することを示す. $N_1 + 1 \leq n_1$ と仮定すると $N = M\frac{N}{M} < M\left(\left\lfloor \frac{N}{M} \right\rfloor + 1\right) = M(N_1 + 1) \leq \sum_{i=1}^{M} n_i$ より $\sum_{i=1}^{M} n_i \neq N$ となるので, $n_1 \leq N_1$ である.

$N_1 = 0$ のとき, $n_1 = 0$ より $X_1 = \phi = Y_1$ とすると, 式 (6) は成立する. $N_1 \geq 1$ のとき, Y_1 は $(2, N_1)$-*Divisible Multiset* より, 任意の n_1 $(0 \leq n_1 \leq N_1)$ に対して $\sum_{n \in X_1} n = n_1$ となる自然数の多重集合 $X_1 \subseteq Y_1$ が存在するので, 式 (6) は成立する.

次に, $j = k$ のとき式 (6) が成立するならば, $j = k+1$ のとき式 (6) が成立することを示す. ただし, $1 \leq k \leq M-2$ とする. $\sum_{i=1}^{k+1} N_i + 1 \leq \sum_{i=1}^{k+1} n_i$ と仮定すると

$$\left(\sum_{i=1}^{k+1} N_i + 1\right) + \frac{M-(k+1)}{k+1}\left(\sum_{i=1}^{k+1} N_i + 1\right) \leq \sum_{i=1}^{k+1} n_i + \sum_{i=k+2}^{M} n_i = \sum_{i=1}^{M} n_i$$

及び

$$\left(\sum_{i=1}^{k+1} N_i + 1\right) + \frac{M-(k+1)}{k+1}\left(\sum_{i=1}^{k+1} N_i + 1\right) = \frac{M}{k+1}\left(\sum_{i=1}^{k+1} N_i + 1\right) = \frac{M}{k+1}\left(\left\lfloor (k+1)\frac{N}{M} \right\rfloor + 1\right) > \frac{M}{k+1}\left((k+1)\frac{N}{M}\right) = N$$

より $\sum_{i=1}^{M} n_i \neq N$ となるので, $\sum_{i=1}^{k+1} n_i \leq \sum_{i=1}^{k+1} N_i$ である. 帰納法の仮定より, $j = k$ のとき式 (6) を満たす $X_1, \ldots, X_k$ が存在する. したがって, 任意の n_{k+1} $(0 \leq n_{k+1} \leq \sum_{i=1}^{k+1} N_i - \sum_{i=1}^{k} n_i)$ に対して $\sum_{n \in X_{k+1}} n = n_{k+1}$ となる自然数の多重集合

$$X_{k+1} \subseteq \bigcup_{1 \leq i \leq k+1} Y_i - \bigcup_{1 \leq i \leq k} X_i = \left(\bigcup_{1 \leq i \leq k} Z_i \right) \cup Y_{k+1}$$

が存在することを示せば十分である. ただし, 自然数の多重集合 Z_i $(1 \leq i \leq k)$ を

$$Z_i = Y_i \setminus \bigcup_{1 \leq l \leq k} X_l$$

とする. また, $Z_0 = \phi, Z_{k+1} = Y_{k+1}$ とする.

$n_{k+1} = \sum_{i=1}^{k+1} N_i - \sum_{i=1}^{k} n_i$ のとき,

$$X_{k+1} = \bigcup_{1\le i\le k+1} Y_i - \bigcup_{1\le i\le k} X_i$$

とすると

$$\begin{aligned}\sum_{n\in X_{k+1}} n &= \sum_{i=1}^{k+1}\sum_{n\in Y_i} n - \sum_{i=1}^{k}\sum_{n\in X_i} n \\ &= \sum_{i=1}^{k+1} N_i - \sum_{i=1}^{k} n_i \;=\; n_{k+1}\end{aligned}$$

及び

$$\bigcup_{1\le i\le k+1} X_i = \bigcup_{1\le i\le k+1} Y_i$$

より, 式 (6) は成立する.

$n_{k+1} < \sum_{i=1}^{k+1} N_i - \sum_{i=1}^{k} n_i$ のとき,

$$\begin{aligned}\sum_{i=0}^{m}\sum_{n\in Z_i} n \;\le\; n_{k+1} \;&\le\; \sum_{i=0}^{m+1}\sum_{n\in Z_i} n - 1 \\ &= \sum_{i=0}^{m}\sum_{n\in Z_i} n + \sum_{n\in Z_{m+1}} n - 1\end{aligned}$$

を満たす m $(0 \le m \le k)$ が存在し,

$$0 \le \left(n_{k+1} - \sum_{i=0}^{m}\sum_{n\in Z_i} n\right) \le \sum_{n\in Z_{m+1}} n - 1 \qquad (7)$$

となる. 一方, $Z_{m+1} \subseteq Y_{m+1}$ より,

$$\sum_{n\in Z_{m+1}} n - 1 \le \sum_{n\in Y_{m+1}} n - 1 = N_{m+1} - 1 \qquad (8)$$

である. 式 (5) より

$$N_{m+1} - 1 \le \left\lceil \frac{N}{M} \right\rceil - 1 \le N_{k+1} \qquad (9)$$

である. 式 (7) 及び式 (8) 及び式 (9) より

$$0 \le \left(n_{k+1} - \sum_{i=0}^{m}\sum_{n\in Z_i} n\right) \le N_{k+1}$$

である. Y_{k+1} は $(2, N_{k+1})$-*Divisible Multiset* より,

$$\sum_{n\in Y'_{k+1}} n = \left(n_{k+1} - \sum_{i=0}^{m}\sum_{n\in Z_i} n\right)$$

を満たす $Y'_{k+1} \subseteq Y_{k+1}$ が存在する. ここで,

$$X_{k+1} = \left(\bigcup_{0\le i\le m} Z_i\right) \cup Y'_{k+1}$$

とすると

$$\begin{aligned}\sum_{n\in X_{k+1}} n &= \sum_{i=0}^{m}\sum_{n\in Z_i} n + \sum_{n\in Y'_{k+1}} n \\ &= \sum_{i=0}^{m}\sum_{n\in Z_i} n + \left(n_{k+1} - \sum_{i=0}^{m}\sum_{n\in Z_i} n\right) \\ &= n_{k+1}\end{aligned}$$

及び

$$\begin{aligned}X_{k+1} &= \left(\bigcup_{0\le i\le m} Z_i\right) \cup Y'_{k+1} \\ &\subseteq \left(\bigcup_{1\le i\le k} Z_i\right) \cup Y_{k+1} \\ &= \left(\bigcup_{1\le i\le k} Y_i - \bigcup_{1\le i\le k} X_i\right) \cup Y_{k+1},\end{aligned}$$

$$\bigcup_{1\le i\le k+1} X_i \subseteq \bigcup_{1\le i\le k+1} Y_i$$

より, 式 (6) は成立する.

したがって, $j = M-1$ のとき式 (6) を満たす $X_1, \ldots, X_{M-1}$ が存在する. ここで,

$$X_M = X - \bigcup_{1\le i\le M-1} X_i$$

とすると

$$\sum_{n\in X_M} n = \sum_{n\in X} n - \sum_{i=1}^{M-1}\sum_{n\in X_i} n = N - \sum_{i=1}^{M-1} n_i = n_M$$

より, 式 (1) を満たす. □

例 3.6 $M = 3, N = 1000$ のとき,

$$\begin{aligned}X \;=\; \{&1, 2, 4, 8, 16, 32, 64, 128, 78, \\ &1, 2, 4, 8, 16, 32, 64, 128, 78, 334\}\end{aligned}$$

は $(3, 1000)$-*Divisible Multiset* である. 例えば, $n_1 = 133$, $n_2 = 267, n_3 = 600$ に対して,

$$\begin{aligned}X_1 &= \{1, 4, 128\} \\ X_2 &= \{2, 8, 16, 32, 64, 78, 1, 2, 64\} \\ X_3 &= \{4, 8, 16, 32, 128, 78, 334\}\end{aligned}$$

とすると, 式 (1) を満たす. □

4 提案する分割可能な複数票電子投票方式

本章では, 準同型暗号系に基づいた DVS の投開票の手順を提案し, 提案方式の安全性と性能の評価を行なう.

4.1 投開票の手順

投票者 $\mathcal{V}_i$ の持ち票数を $N^{(i)}$, 投票者 $\mathcal{V}_i$ の選択肢 A_j $(1 \le j \le M)$ への投票数を $v_j^{(i)}$, $(M, N^{(i)})$-*Divisible Multiset* を $X^{(i)}$ とする. 総票数 w は $w = \sum_i N^{(i)}$ となる. 準同型な性質を持つ確率的公開鍵暗号系の暗号化アルゴリズムを $E(\cdot)$ とし, 平文空間を $(w+1)^M$ 以上とする.

［投票］　投票者 $\mathcal{V}_i$ は, 次式を満たす自然数の多重集合 $X_j^{(i)}$ $(1 \le j \le M)$ を得る.

$$\bigcup_{1\le j\le M} X_j^{(i)} = X^{(i)}, \forall j \in \{1,\ldots,M\} \left(\sum_{n\in X_j^{(i)}} n = v_j^{(i)} \right) \tag{10}$$

投票者 $\mathcal{V}_i$ は, 自然数の多重集合 $X^{(i)}$ のすべての要素 $x_k^{(i)}$ $\left(1 \le k \le \#X^{(i)}\right)$ に対して, $x_k^{(i)} \in X_j^{(i)}$ となる j を $j_k^{(i)}$ とし, 暗号文 $E\left((w+1)^{j_k^{(i)}-1}\right)$ を投票する. 投票の際に, 暗号文が平文 $(w+1)^{j-1}$ $(1 \le j \le M)$ のいずれかを暗号化したものであることをゼロ知識証明で投票サーバに示す. 投票者 $\mathcal{V}_i$ が投票したすべての暗号文の正当性が証明されたならば, 投票サーバは自然数と暗号文の組 $\left(x_k^{(i)}, E\left((w+1)^{j_k^{(i)}-1}\right)\right)$ $\left(1 \le k \le \#X^{(i)}\right)$ を有効にする.

［開票］　すべての有効な自然数と暗号文の組から, 準同型な性質を用いて暗号文

$$\begin{aligned} & E\left(\sum_i \left(\sum_{1\le k\le \#X^{(i)}} x_k^{(i)}(w+1)^{j_k^{(i)}-1}\right)\right) \\ = \;& E\left(\sum_i \left(\sum_{j=1}^{M}\sum_{n\in X_j^{(i)}} n(w+1)^{j-1}\right)\right) \\ = \;& E\left(\sum_i \left(\sum_{j=1}^{M} v_j^{(i)}(w+1)^{j-1}\right)\right) \\ = \;& E\left(\sum_{j=1}^{M}\left(\left(\sum_i v_j^{(i)}\right)(w+1)^{j-1}\right)\right) \end{aligned} \tag{11}$$

を得る. 秘密鍵を分散共有している複数の投票サーバによって閾値法を用いて復号を行ない

$$S = \sum_{j=1}^{M}\left(\left(\sum_i v_j^{(i)}\right)(w+1)^{j-1}\right)$$

を得る. 選択肢 A_j $(1 \le j \le M)$ の集計結果 $S_j = \sum_i v_j^{(i)}$ を次式より得る.

$$\begin{aligned} S_1 &= S \bmod (w+1) \\ S_2 &= (S - S_1)(w+1)^{-1} \bmod (w+1) \\ S_3 &= (S - S_1 - S_2(w+1))(w+1)^{-2} \bmod (w+1) \\ &\vdots \\ S_M &= \left(S - \sum_{l=1}^{M-1} S_l(w+1)^{l-1}\right)(w+1)^{-(M-1)} \end{aligned}$$

4.2　安全性の評価

提案方式がセキュアな DVS であることを示す. ただし, 秘密鍵を分散共有している複数の投票サーバのうち, 不正を行なう投票サーバの数は閾値法により定まる閾値以下であると仮定する.

完全性:　すべての投票が健全性を満たすならば,

$$\sum_i v_j^{(i)} \le \sum_i N^{(i)} = w \;(1 \le j \le M)$$

より

$$\begin{aligned} S_1 &= \sum_{j=1}^{M}\left(\left(\sum_i v_j^{(i)}\right)(w+1)^{j-1}\right) \bmod (w+1) \\ &= \sum_i v_1^{(i)} \end{aligned}$$

である. 同様に, $S_j = \sum_i v_j^{(i)}$ $(2 \le j \le M)$ である. 暗号文の復号は, 秘密鍵を分散共有している複数の投票サーバによって閾値法を用いて行なわれるので, 仮定より正しく行なわれる. 暗号文の復号以外の開票の手順は, 公開掲示板上で行なわれるので, 投票サーバによる不正は考えなくてよい. したがって, 提案方式は完全性を満たす.

健全性:　投票者 $\mathcal{V}_i$ が投票したすべての暗号文の正当性が証明された場合についてのみ考える. 有効となる自然数と暗号文の組を $\left(x_k^{(i)}, E\left((w+1)^{J_k^{(i)}-1}\right)\right)$（ただし, $1 \le k \le \#X^{(i)}$, $1 \le J_k^{(i)} \le M$ である）とする. 準同型な性質を用いて暗号文

$$\begin{aligned} & E\left(\sum_{1\le k\le \#X^{(i)}} x_k^{(i)}(w+1)^{J_k^{(i)}-1}\right) \\ & \quad = E\left(\sum_{j=1}^{M}\sum_{1\le k\le \#X^{(i)}, J_k^{(i)}=j} x_k^{(i)}(w+1)^{j-1}\right) \end{aligned}$$

を得る. ここで,

$$V_j^{(i)} = \sum_{1\le k\le \#X^{(i)}, J_k^{(i)}=j} x_k^{(i)} \quad (1 \le j \le M) \tag{12}$$

とすると, 式 (11) 以降の開票の手順より, 選択肢 A_j $(1 \le j \le M)$ の集計結果 S_j に $V_j^{(i)}$ 票が加算されていることが分かる. $x_k^{(i)}$ は $(M, N^{(i)})$-*Divisible Multiset* $X^{(i)}$ の要素であるので,

$$0 < x_k^{(i)} \le N^{(i)}\ ,\ \sum_{k=1}^{\#X^{(i)}} x_k^{(i)} = \sum_{n\in X^{(i)}} n = N^{(i)} \tag{13}$$

を満たす. 式 (12) 及び式 (13) より,

$$0 \le V_j^{(i)} = \sum_{1\le k\le \#X^{(i)}, J_k^{(i)}=j} x_k^{(i)} \le \sum_{k=1}^{\#X^{(i)}} x_k^{(i)} = N^{(i)}$$

及び

$$\sum_{j=1}^{M} V_j^{(i)} = \sum_{j=1}^{M}\sum_{1\le k\le \#X^{(i)}, J_k^{(i)}=j} x_k^{(i)} = \sum_{k=1}^{\#X^{(i)}} x_k^{(i)} = N^{(i)}$$

となるので, 提案方式は健全性を満たす.

プライバシ: 健全性を満たすすべての $v_j^{(i)}$ $(1 \leq j \leq M)$ の組み合わせに対して, *Divisible Multiset* の定義より式 (10) を満たす $X_j^{(i)}$ $(1 \leq j \leq M)$ が存在する. よって, $v_j^{(i)}$ に関する情報を得るためには, 投票者 $\mathcal{V}_i$ が投票した暗号文が平文 $(w+1)^{j-1}$ $(1 \leq j \leq M)$ のいずれを暗号化したものであるかを区別できなければならない. しかし, そのような不正を実行できるのは, 閾値を超える投票サーバが結託した場合だけであり, 仮定より実行不可能である. したがって, 提案方式はプライバシを満たす.

以上より, 提案方式はセキュアな DVS である. 松尾らの方式 [12] では, 特定のサーバに対して, 他のサーバや投票者と結託しないと仮定している. 提案方式では, 特定のサーバに対して特別な仮定を設けることなく, セキュアな DVS を実現している.

4.3 性能の評価

選択肢の数を M, 投票者 $\mathcal{V}$ の持ち票数を N とする. 提案方式において, 投票者 $\mathcal{V}$ が投票の際に行なう暗号化及びゼロ知識証明の回数は, (M,N)-*Divisible Multiset* の要素数と等しいので, $M=2$ のとき $O(\log N)$, $M \geq 3$ のとき $O(M \log N)$ である. 一方, 松尾らの方式 [12] において, 投票用紙管理サーバが投票以前の準備段階で投票者 $\mathcal{V}$ に送信するシェアの数は, $M=2$ のとき $O(N)$, $M \geq 3$ のとき $O\left(M(M-1)^N\right)$ である. したがって, $N \gg 1$ または $M \geq 3$ のとき, 提案方式はより実用的である.

5 まとめ

本稿では, まず最初に, 各投票者が複数の選択肢に持ち票を分割する際に用いる, ある特殊な性質を持つ自然数の多重集合 *Divisible Multiset* を定義し, *Divisible Multiset* の要素数を持ち票数に対して log オーダにできることを示した. 次に, 準同型暗号系に基づいた DVS を提案した. 提案方式はセキュアな DVS であり, *Divisible Multiset* の要素数回の投票で済むので効率的であることを示した.

参考文献

[1] J.Benaloh and D.Tuinstra. “Receipt-Free Secret-Ballot Elections” STOC94, pp.544-553.

[2] J.Benaloh and M.Yung. “Distributing the Power of a Government to Enhance the Privacy of Voters” Proc. of PDOC86, pp.52-62.

[3] J.Cohen and M.Fischer. “A Robust and Verifiable Cryptographically Secure Election Scheme” FOCS85, pp.372-382.

[4] R.Cramer, M.Franklin, B.Schoenmakers and M.Yung. “Multi-Authority Secret-Ballot Elections with Linear Work” In Proc. of EUROCRYPT’96, pp.72-82.

[5] R.Cramer, R.Gennaro and B.Schoenmakers. “A Secure and Optimally Efficient Multi-Authority Elections” In Proc. of EUROCRYPT’97, pp.103-118.

[6] I.Damgård and M.Jurik. “A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-Key System” PKC2001, pp.119-136.

[7] K.R. Iversen. “A Cryptographic Scheme for Computerized General Elections” In Proc. of CRYPTO’91, pp.405-419.

[8] H.Kikuchi, J.Nakazato and S.Nakanishi. “Oblivious Ciphertext Demultiplexer and Multi-way Election” In Proc. of SCIS2002.

[9] P.Paillier. “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes” EUROCRYPT’99, pp.223-238.

[10] K.Sako and J.Kilian. “Secure Voting Using Partially Compatible Homomorphisms” In Proc. of CRYPTO’94. pp.411-424.

[11] 税所, 齋藤, 鈴木, 土井, 辻井. “準同型性暗号を利用した 1 人複数投票可能な電子投票方式” コンピュータセキュリティシンポジウム 2002 論文集, IPSJ Symposium Series, Vol.2002, No.16, pp.467-472.

[12] 松尾, 尾形. “分割可能な複数票電子投票方式” 信学技報, ISEC2002-96.