Design of E-voting with an Absentee Voter Which Enables Ballot-Cancellation and Receipt-Free

許, 容碩
九州大学大学院システム情報科学府

櫻井, 幸一
九州大学大学院システム情報科学研究院

出版情報：Proc. of the 2003 Symposium on Cryptography and Information Security. 1, pp.185-190, 2003-01. 2003 Symposium on Cryptography and Information Security
バージョン：
権利関係：

票-取消と無証拠性が可能な不在者投票を含んだ電子投票の設計
Design of E-voting with an Absentee Voter Which Enables Ballot-Cancellation and Receipt-Free

許 容碩 *　　櫻井 幸一†
Yong-Sork HER　　Kouichi SAKURAI

あらまし 最近, 電子投票に関する研究が活発に進行している．電子投票は, 現行の投票制度の問題点を解決して, 投票率の増加と速い投票, 開票の進行が可能となる．しかし, 電子投票では現行の投票制度では発生しない, 無証拠性問題が発生する．無証拠性の手法は特定党と特定候補への投票行為の販売を防止する手法である．電子投票におけるこの手法は, 投票者が特定政党と特定候補に自身の投票方法や投票内容について証明出来ないことが必要となる．本論文では投票の販売を防止するために, 独立的な二つの機関を利用して, 投票内容を二つの機関の公開鍵で暗号化する手法を提案する．また, 本論文では, 不在者と一緒に電子投票をするために, 票-取消手法を導入する．本論文の票-取消手法は機密性を維持しながら, 投票を取消すことができる．

キーワード 電子投票, 暗号学, 二重暗号, 票-取消, 無証拠性

1　はじめに

1.1　動機

暗号技術を利用したさまざまな電子投票システムが提案されている [3, 4, 5, 6, 7]．この中でもいくつかは, すでに実験システムなどで施行されている．しかし, 実際の選挙では, 一般有権者と不在者が一緒に投票を進行しているにもかかわらず, 大部分の電子投票システムでは不在者投票に関しては考慮されていない．日本の現行の選挙法では, 不在者が投票後, 開票するまでの間に死亡したり選挙権を喪失した場合には, 無効票とみなして対応する必要がある [18]．したがって, 目標とする電子投票システムでも, プライバシーを侵害することなく, 如何にして不在者投票を投票後に無効化する票-取消手法を実現するかが鍵となる．また, 本論文では電子投票の様々な必須条件の中で無証拠性に重点をおく．票の売買防止を実現するために, 必要な性質として無証拠性がある．この性質は, 投票者が特定政党と特定候補に自身の投票方法や投票内容について証明出来ないことが必要となる．最近, 様々な無証拠性を実現する方式が提案されているが, これらの手法は複数のネットワーク 通信路や複数のセンターを利用することが多い [5, 6, 14]．複数のネットワーク通信路や複数のセンターの利用は, 電子投票システムの実現を困難にする．本論文では二つの独立的な機関を利用した二重暗号をベースとし無証拠性を実現した方式を提案する．提案する手法は単純で, 効率的な電子投票システムを実現することができる．

1.2　無証拠性を実現する既存の方式

この章では, 既存の無証拠性手法を提案して, この手法の長所と短所を分析する．Benaloh と Tuinstra は電子投票システムで最初の無証拠性手法を紹介した [5]．彼らの手法はいくつかのセンターと各投票者間に物理的な安全な通信路 (voting booth と呼ばれる．) を必要とする．彼らは homomorphic 暗号化を利用した二つの投票プロトコルを提案した．しかし, センターは各投票者がどのように投票をしたかを知っているため無証拠性ではないことが知られている．

Sako と Kilian は mix-net 通信路を基盤とする無証拠性を提案した [6]．彼らは盗聴防止可能な通信路として, 安全な一方向の通信路を仮定した．彼らの手法の短所は mix-net を用いた手法ゆえに集計で多くの負荷が生まれることができる．

Hirt と Sako は homomorphic 暗号化を基盤とする効率的な無証拠性を提案した [14]．無証拠性を実現するために, 彼らは複数センターと投票者間の通信路には一方向

* 九州大学大学院システム情報科学府 〒 812-8581 福岡市東区箱崎 6-10-1, Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan
† 九州大学大学院システム情報科学研究院 〒 812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan

通信路を使用している．

1.3 電子投票システムの要求事項

本論文での目標は不在投票者の投票を含む安全な電子投票システムである．これのために以下の要求事項を満足しなければならない [2, 3, 4].

■ 秘密性
投票の内容と投票者の関係は第三者に知られてはいけない.

■ 票–取消
様々な選挙法により投票を取消さねばならない場合が発生する．いくつかの違法な投票者によって投票を中断できないことである．本論文では集計過程で秘密性を保障しながら, 票を取消する手法を提供する.

■ 検証性
投票者は集計で自身の投票が正確に集計されたかを確認できなければならない.

■ 無証拠性
投票者が特定政党と特定候補に自身の投票方法や投票内容について第三者に証明出来てはいけない.

■ 公平性
投票に影響を与える要素があってはならない.

1.4 貢献

本論文では, 我々は提案になった無証拠性手法と他の方式を比較する．最近提案されている無証拠性手法は複数の通信路複数のセンターを利用する．これらの提案方式は電子投票の実現が複雑になる．無証拠性の目的は投票の販売を防ぐという方式である．電子投票では, 投票者が政党でも候補者に自身の投票内容を証明することが出来なくなければならない．また, 無証拠を実現するために, 二つの独立機関を利用した二重暗号を基盤とした. これにより, シンプルで効率的なシステムが実現する. また, 不在者投票のための票-取消手法も実現する.

2 提案する投票システムの構成

■ 投票者
投票者は有権者と不在者に分類できる．本論文で, 我々は不在者投票の観点で電子投票を説明する．不在者ては, 選挙日に特別な理由により, 投票出来ない有権者である. したがって, 選挙前の特定の日に投票をして, 郵便等を通し投票内容が転送される．投票の終了後に一般投票と一緒に集計さなる.

■ 管理センター
管理者センターは適法な不在者のリストを持っている. 投票が適法でないか, 二重投票かどうかをチェックできる．管理センターの役割は以下の通りである.
- 不在者投票が適法かを確認して,
- 掲示板に表示をする.
- 投票の終了後, 投票をした投票者の数を計算する.

■ 集計センター
集計センターの役割は以下の通りである.
- 投票の結果を計算する.
- 管理者センターが 計算した投票者の数と比較する.
- 掲示板に投票結果を送る.

■ 掲示板
掲示板の内容はあらゆる人が見ることが出来るが, 削除したり内容を書き変えることはできない.

3 提案する手法

■ 記号

- 投票者
  - 投票者: V_i
  - 投票者の ID: ID_i
  - 投票者の投票内容: v_i ($v_i = 0$ or 1)
  - σ_i : 投票者の署名
  - e_i : ブラインド署名
  - r_i : ブラインド要素

- 管理センター
  - 管理センターの公開鍵 : $< e_A, N_A >$
  - 管理センターの秘密鍵 : $< d_A, p_A, q_A >$
  - p_A, q_A: 素数
  - k_i: 不在者投票権の変数 ($k_j = 0$ or 1)
  - M: 投票結果の合計
  - σ_A : 管理者の署名

- 集計センター
  - 集計センターの公開鍵 : $< N_T, y_T >$
  - 集計センターの秘密鍵 : $< p_T, q_T >$
  - p_T, q_T : 素数

■ 段階 1: 二重暗号
本段階では, 投票内容は管理センターと集計センターの公開鍵 $< N_T, y_T >< e_A, N_A >$ で暗号化する．大部分の既存の電子投票システムは投票内容の暗号化のために投票者の公開鍵や暗号鍵を使用する．これが他の電子投票システムと相違点である．投票者 V_i が候補者 v_i を選択した後, 投票は二つの公開鍵によって暗号化されるため, 投票者は自身が特定政党, 特定候補に投票したことを証明することができない．また, 管理センターと集計センターは相互独立的な関係であるため一つのセンターで投票内容を見ることができない [11]．投票内容に対する二重暗号の順序は以下のようである.
- 不在者 V_i は選挙管理委員会に不在者登録をする.
- 不在者 V_i は投票内容 v_i を投票する; ($v_i = 0$ or 1)

- 不在者 V_i は管理センターの公開鍵 $< e_A, N_A >$ を利用して投票内容を暗号化する．

$$Z_i = y_T^{v_i} x^{r_{vi}} \mod N_T$$

- 不在者は集計センターの公開鍵 $< e_A, N_A >$ を利用して Z_i を暗号化する．

$$C_i = Z_i^{e_A} \mod N_A$$

■ 段階 2: ブラインド署名

電子投票システムでは, 投票者は自分の投票が正しく集計に反映されてみるのか確認したりという要求がある．これは電子投票の universal verifiability である．電子投票システムではこのような universal verfiability を満足しなければならない．提案システムでは, 投票者は二重暗号化した投票内容に対する管理センターの署名 y_1 とブラインドの要素 r_i を持つことができる．管理センターの署名とブラインドの要素を用いることにより, 投票内容が変えられていたことを確認するできる．また, 投票者が自身の投票が正確に集計されたかを確認する時, 管理センターの署名, ブラインドの要素, 管理センターと集計センターの秘密することにで確認することができる．したがって, 提案する投票システムは universal verfiablity を満足でする．投票者は V_i 下記のように C_i をブラインドする．

$$e_i = x(C_i, r_i)$$

- 投票者は e_i を署名する．: $s_i = \sigma_i(e_i)$
- 管理センターに $< ID_i, e_i, s_i >$ 送る．
- 管理センターは次の部分をチェックする．
  ． s_i は e_i の正しい署名か?
  ． ID_i は投票者のリストにあるのか?
  ． v_i は正しい投票か?
- これらのチェック後に, 管理センターは d_i に下記のように署名をして, 投票者にそれを送る．

$$d_i = \sigma_A(e_i)$$

- 投票者は署名 y_i を得るために d_i を次のように復号化する．

$$y_i = \delta(d_i, r_i)$$

- 投票者はメッセージ x_i に対する署名 y_i が正しい署名なのか, チェックする．
- チェックが失敗すれば, 投票者は $< C_i, y_i >$ を掲示板に送る．
- 成功すれば, 投票者は $< C_i, y_i >$ を管理センターに送る．

■ 段階 3: 投票-取消手法

本段階で, 我々は管理センターと集計センター間に投票内容に対する有効性を証明できる．管理センターはこの中で暗号化がされた投票内容を復号化する．しかし, 管理センターは集計センターの公開鍵によりすることに暗号化されているため投票の内容をわからない．管理センターは投票結果に対する公正性のために, 投票を実施した有権者の数を計算した後に掲示板に送る．集計センターは最終投票結果を計算する前に再び有権者の数を計算して管理センターの計算結果と比較する．
- 管理センターは C_i の署名 y_i をチェックする．
- チェックが成功すれば, 管理センターは秘密鍵 $< d_A, p_A >$ を利用して C_i を復号化をして, Z_i を得る．
- 管理センターは投票権をチェックしてその結果を掲示板に送る．(有効投票: k_i =1, 無効投票: k_i =0)
- 管理センターは下記のように集計する．

$$Z_c = \prod_{i=1}^{h} Z_i \mod N_T$$

管理センターは ID (ID_A) を作って, 管理センターの秘密鍵 $< d_A, p_A, q_A >$ を利用して暗号化する．

$$(ID_A)^{d_A}, Z_c \mod N_A$$

- 管理センターにより計算された結果 Z_c を確認するために, 集計者は下記のように計算する．

$$C_v = \prod_{i=1}^{h} (C_i)^{k_i} \mod N_A$$

$$C_e = (Z_c)^{e_A} \mod N_A$$

- 集計センターは C_v と C_e を比較する． $C_v = C_e$ ならば, 管理センターは 計算された Z_c が正しいことを確信する．
- 集計センターは暗号化された投票内容 Z_i を復号化して, 各 Z_i を下記のように計算する．

$$Z_c = \prod_{i=1}^{h} (Z_i)^{k_i} \mod N_T$$

$$= \prod_{i=1}^{h} (y_T)^{v_i} x^{r_{v_i}} \mod N_T$$

$$= \prod_{i=1}^{l} (Z_i)^1 \prod_{i=l+1}^{n} (Z_i)^0$$

$$= \prod_{i=1}^{l} (Z_i)$$

($h = l + n, h$: 全体の投票数, l : 有効票, n : 無効票)

$$Z_l = \prod_{i=1}^{l} (Z_i)^1 : \text{有効票}$$

$$Z_n = \prod_{i=l+1}^{n} (Z_i)^0 : \text{無効票}$$

- 投票の最後の結果は下記のように計算する．

$$Z_l = \prod_{i=1}^{l} (Z_i)^1 \mod N_T$$

$$= \prod_{i=1}^{h} (y_T^{v_i} x^{r_{v_i}}) \mod N_T$$

$$= y_T^M x^{r_{v_i}} \mod N_T$$

$$M = \sum_{i=1}^{l} v_i$$

4 提案するシステムの安全性

4.1 秘密性

提案された電子投票システムは, 投票の内容が二重暗号で処理される．投票者は投票後, 投票の内容が管理センターと集計センターの公開鍵を利用して以下のように暗号化される; $Z_i = y_T^{v_i} x^{r_{vi}} \mod N_T$ and $C_i = Z_i^{e_A} \mod N_A$．この方式では投票者の暗号鍵を使用しない．管理センターと集計センターも相互独立的な関係として, 暗号化された投票内容は相互の秘密鍵に依存する．集計センターと管理センターのうち, どれが一つのセンターだけでは投票内容を見ることができない．

投票内容に対して二つのセンターの共謀による変造を防止するために, 投票者は二重暗号化された投票内容 C_i に対して ブラインドの要素 r_i を利用してブラインドする: $e_i = x(C_i, r_i)$．そして, 投票者の署名を添加して $s_i = \sigma(e_i))$ 自身の識別情報と一緒に $< ID_i, e_i, s_i >$ を管理センターに送る．管理センターは転送された署名を確認した後に管理センターの署名 d_i を添加して投票者に送る．投票者は管理センターの署名と二重暗号化された投票内容を確認する．投票内容は管理センターの公開鍵, 集計センターの公開鍵, 投票者のブラインドの要素で暗号化されたいるため, 投票者の認証と秘密性を維持できる．

4.2 二つの独立的なセンターの安全性

管理センターは投票者の認証をチェックして, 投票者の数を計算する． 集計センターは最終の投票結果を計算して, 管理センターにより計算された投票者の合計と比較する．

4.3 投票内容の安全性

我々は投票者の暗号鍵の代りに投票の安全性のためにブラインド署名を利用する．投票者が投票した後, 管理センターと集計センターの公開鍵を利用して暗号化する．その時, 投票者は暗号化された投票内容をブラインドしてそれを管理センターに送る．投票者は管理センターの署名値を受けることができる．投票者が自身の投票内容を確認したいならば, 投票内容は管理者から受けた署名値を利用して確認することが出来る．

4.4 投票内容の有効性

■ 投票者 - 管理センター

投票内容に対する投票者と管理センター間の有効性は 4.1 章で説明をした．

■ 管理センター - 集計センター

投票の終了後, 管理センターは二重暗号化された投票内容を自身の秘密鍵を利用して復号化する．しかし, 投票内容は集計センターの公開鍵で暗号化されたあるために管理センターは投票の内容を知ることが出来ない．管理センターは以下のようにして投票者に発行した署名鍵の数を計算する．

$$M = \sum_{i=1}^{l} v_i$$

復号化にされた投票内容の数を以下のようにして計算する．

$$Z_c = \prod_{i=1}^{h} Z_i \mod N_T$$

二つの計算結果を比較して, 計算結果を自身の秘密鍵で暗号化させた後, 掲示板に送る．集計センターは管理センターの計算結果を掲示板から持ってくる．集計センターは自身も投票者の数を計算して, その結果と管理センターの計算結果を比較する．

$$C_v = \prod_{i=1}^{h} (C_i)^{k_i} \mod N_A$$

$$C_e = (Z_c)^{e_A} \mod N_A$$

提案する方式では, 二つのセンターによる計算結果を比較して, 投票結果に対する信頼性と安全性を高めることができる．

4.5 他の要求条件

■ 検証性

提案するシステムでは投票内容と不在者の選挙権に対する判断, 投票結果などを暗号化して公開掲示板に書き込む．これにより, 投票者は管理センターの署名値とブラインドの要素を通し, 自身の投票結果を確認することができる．

■ 公平性

提案するシステムは不在者を含む投票者, 掲示板, 集計センター, 管理センターで構成する．それぞれの機関は相互独立的に情報を共有する．投票結果は 投票の終了後に不在者の選挙権に対する判断後に集計される．ゆえに投票途中には影響を与えない．

5 無証拠性手法の比較

■ HS-2000 の手法 (図 1 参照)

この手法は複数の機関と盗聴防止可能な通信路を利用する．投票内容は複数の機関らによりランダム一順序で暗号化される [14]．各機関は盗聴防止可能な通信路でを利用して投票内容をランダム一 順序 (shuffling) 伝達する．投票者は各機関によりランダム一順序で通過した自身の投票内容を特定政党でも特定人に証明をすることが出来ない．しかし, インターネットのようなネットワークは盗聴防止可能な通信路ではなく, 盗聴可能な通信路である．盗聴防止可能な通信路を実現することが実現することが難しいと指摘されている．また, 複数の機関に対する信頼性が基盤ならなければならない問題点も持っている．

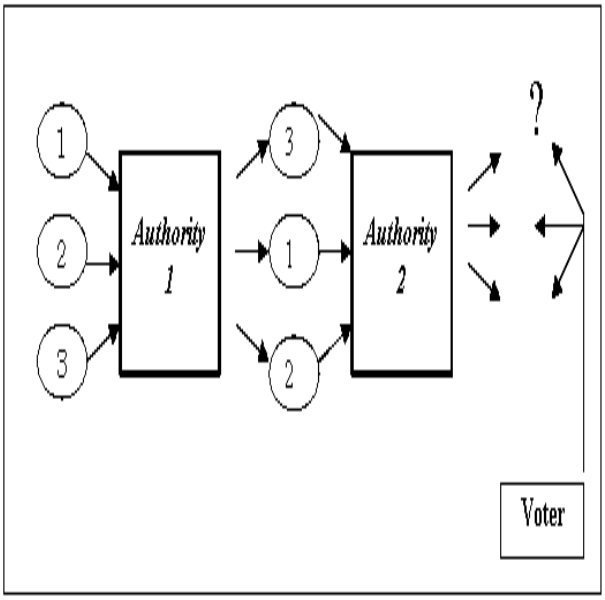

図 1: HS-2000 の手法

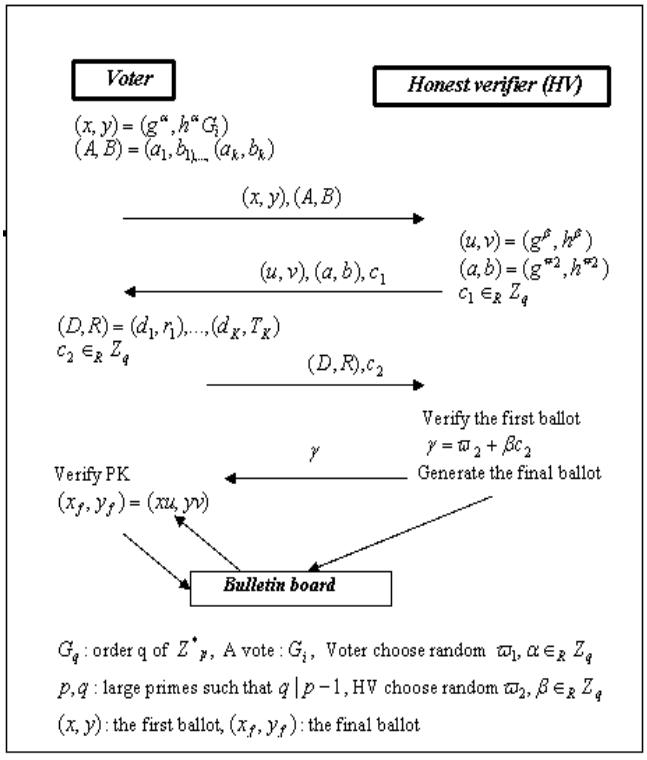

図 2: LK-2000 の手法

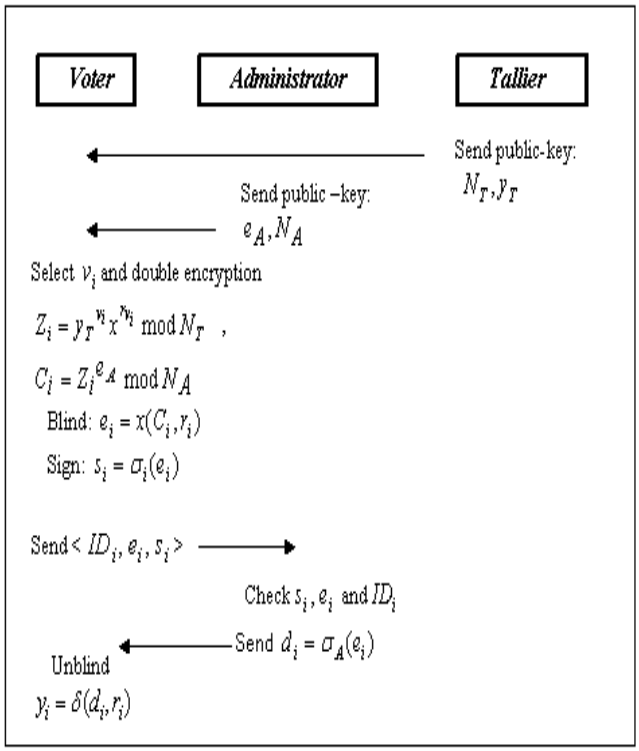

図 3: 我々の手法

■ LK2000 の手法 (図 2 参照)
$LK2000$ は無証拠性のために ElGamal 暗号化と (t, n) $threshold$ 手法を利用している [16]．そして, 信じることができる認証者 (HV) をおく． 初めの投票は投票者により生成され, 最後の投票は投票者と認証者により生成される．それで, 投票者は特定党と特定候補への投票の内容を証明出来ない手法である．

表 1: 提案手法と HS2000 の手法の比較

	提案手法	HS2000 の手法
暗号技術	RSA r-剰余暗号	ElGamal 暗号 (t, n)threshold
無証拠性	管理センターと集計センターの秘密鍵に依存	HV のランダム変数 β に依存
特徴	投票者の暗号化鍵を使用しない	二回投票 (初めて投票, 最後の投票)

■ 提案手法 (図 3 参照)
提案手法は投票内容を暗号化する時, 投票者の暗号鍵を使用せず二つの独立的な機関の公開鍵を使用する．投票者は暗号化にされた内容を復号化することが出来ないだけでなく外部に証明することもない．また, 一つの認証機関を使用する場合は安全性に対する依存性と危険性が増加してしまうので本論文の無証拠性手法はこのような

点を考慮して独立的な二つの機関を使用した．表 1 で提案手法と HS2000 の手法の相違点を示す．

6 まとめ

電子投票システムにはいくつかの条件が必要となる．この条件中から無証拠性手法はネットワークを基盤とするシステムで非常に重要な要素である． 最近, 様々な無証拠性手法は現実的な電子投票システムのために提案されている．本論文では簡単で効率的な無証拠性の手法を提案した．私々が提案するシステムは二つの独立的な機関を基盤として二重暗号を使用している．また, 不在者投票のための票-取消手法を提案した．秘密性を維持しながら, 投票の進行中に発生する状況に対する未然の防止が可能である．今後の課題は提案した無証拠性の手法に対する実装行い効率性と安全性に対して検討する．

謝辞

本研究は一部，21 世紀 COE プログラム「システム情報科学での社会基盤システム形成」の支援と文部科学省科学研究費補助金学術創成研究課題番号 14GS0218「社会基盤を構築するためのシステム LSI 設計手法の研究」(研究代表安浦寛人九州大学システム LSI 研究センター長) の支援を受けている．

参考文献

[1] D.Chaum *“Untraceable electronic mail, return addresses, and digital pseudonyms”* In Communications of the ACM, pp84-88, 1981.

[2] J.D Cohen and M.J. Fischer *“A robust and verifiable cryptographically secure elelction schme”* In Proc.26th IEEE Symp. on Foundation of Comp.Science, pages 372-382, Portland, 1985.IEEE.

[3] A.Fujioka, T. Okamoto, K.Ohta. *“A Practical Secret Voting Scheme for Large Scale Elections”* in Advaces in Cryptology-AUSCRYPT ’92, LNCS718, Springer-Verleg, Berlin, pp.244-251, 1993,

[4] C.Park, K.Itoh, K.Kurosawa *“Efficient Anonymous Channel and All / Nothing Election Scheme”* EUROCRYPT ’93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.

[5] J.Cohen Benaloh and D.Tuinstra . *“Receipt-Free Secret-Ballot Elections”* In STOC 94, pp544-553.1994

[6] K.Sako, J.Kilian *“Receipt -Free Mix-Type Voting Scheme”* EUROCRYPT ’95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995.

[7] L.F. Canor and R..K. Cytron *“Design and Implementation of a Practical Security-Conscious Electronic Polling System”* WUCS-96-02, Department of Computer Science, Washington University, St. Louis, Jan, 1996

[8] R.Cramer, M.Franklin, B, Schoenmakers, M.Yung *“Multi-Authority Secret-Ballot Elections with Linear Work”* EUROCRYPT ’96, LNCS1070, Springer-Verlag, Berlin Heidelberg 1996.

[9] M.A.Herschberg *“Secure Electronic Voting Over the World Wide Web”* Master Thesis in Electronic Engineering and Computer Science, Massachusetts Institute of Technology, 1997

[10] R. Cramer, R.Gennaro and B.Schoenmakers *“A secure and optimally efficient multi-authority election scheme”* European Transactions on Telecommunication, 8:481-489, Eurocrypt 1997.

[11] S.Tsujii, H.Yamaguchi, A.Kitazawa, K.Kurosawa *“A Method for Voting Protocols with regards to Privacy”* ISEC98-42, 1998.

[12] B.W. DuRette *“Multiple administrators for electronic voting”* http://theory.lcs.mit.edu/ cis/theses/DuRette-bachelors.pdf May, 1999

[13] M.Ohkubo, F.Miura, M.Abe, A. Fujioka, T.Okamoto *“An Improvement on a Practical Secret Voting Scheme”* ISW’99, LNCS 1729, pp225-234, 1999.

[14] M.Hirt , K.Sako *“Efficient receipt-free voting based on homomorphic encryption”* Eurocrypt 2000, LNCS1807, pp539-556, 2000.

[15] O.Baudron, P.-A. Fouque, D.Pointcheval, G.Poupard, J.Stern *“Practical Multi-Candidate Election System”* ACM 2001

[16] A.Juels, M.Jakobsson *“Coercion-resistant Electronic Elections”* http://eprint.iacr.org/2002/165/, Nov,2002

[17] http://www.votehere.com

[18] http://www.mainichi.co.jp/ (June.24.2002)