電子投票･アンケート諸方式に対する比較考察

山口 浩　NEC ソフト(株)
大久保 美也子　NTT 東日本電信電話(株)
北沢 敦　NEC ソフト(株)
辻井 重男　中央大学

あ ら ま し

投票者のプライバシを守りつつ不正投票を防止する方式としてこれまでにブラインド署名、ミックスネット匿名チャンネル、準同型暗号系を利用した方式が提案されている。これら方式の特長を研究の流れに沿って列挙、比較検討を行う。また近い将来、これら提案された方式を適用した電子投票システムの実用化が近いことを考慮し、計算機器、通信機器がこれら提案された方式において必要とされる計算量、通信量、信頼性にどの程度対応可能であるかを考察する。併せて運用性の問題も考察する。

Overview of Comparisons and Future Work of Electronic Voting Scheme

Hiroshi Yamaguchi　NEC Soft, Ltd.
Miyako Ohkubo　NTT EAST
Atsushi Kitazawa　NEC Soft, Ltd.
Shigeo Tsujii　Chuo University

Abstract

Many papers have been written on the electronic voting schemes discussing the required properties of elections, among which are privacy, universal verifiability and various forms of robustness, Recent advancements have also been concerned with performance aspect. We will compare different features of three schemes using blind signatures, mix-net anonymous channel, and partially compatible homomorphisms. We also discuss the new properties particularly concerned with the computation and communication capabilities, reliability of computer and communication systems and operationability.

1 まえがき

近年、電子・投票アンケート方式に関してプライバシ保護、投票・集計／開票の正当性の検証可能性、堅牢性等の満たすべき要件に関し様々な方式が提案されている。また計算・通信量に関する効率化、ならびに一部においては実際に実装し実用性の評価、利用する例も発表されている。そこで本稿ではこれまで提案された方式をブラインド署名、ミックスネット匿名チャンネル、準同型性暗号を利用した三つの方式に分類し、研究の流れ、ならびに各方式の特徴を比較し、また近い将来の本格的実用化に備え、新たに解決すべき要件を挙げその必要性を考察する。

2 電子投票方式が満たすべき要件

電子投票方式が満たすべき要件を以下に示す。

プライバシ保護
投票者の投票内容がいずれの参加者にも漏れないことを保証する。

有権者確認可能性
有権者のみが投票できること。

二重投票不可能性
有権者が一回のみ投票できること。

検証可能性
投票、集計、開票の正当性を検証可能なこと。

堅牢性
意図的であるないに関わらず何らかの誤りが混入した場合にそれを排除できること。

公平性
投票の途中経過を誰も知りえないこと

その他、買収不可能性、非待機性等も存在する。

3 電子投票方式の研究の流れ

3.1 ブラインド署名方式

信頼できる署名管理センタ、匿名通信路、集計センタで構成される［Cha85］により最初に提案され［AMI91］が公平性問題を［SK92］が異議申立て問題を解決。［FOO93］は署名管理センタが不正をした場合にも投票者の匿名性と公平性を保持可とし、さらに［OMAFO99］では投票者が集計ステージに参加することなしに公平性を解決している。

3.2 ミックスネット方式

複数の Mix-server と呼ばれる管理センタ、掲示板で構成される。［Cha81］により最初に提案され［PIK94］が ElGamal 暗号系の秘密鍵を各管理センタが分割保有することにより暗号文の長さが Mix-server の数に独立な方式を提案。［SK95］はシャッフル、復合化の正当性を検証することにより Universal な検証可能性を実現し、［AbOO］は Cut-and-Choose 方式を用いることなく Universal な検証可能性を満たしつつ堅牢性を実現し、［OA01］は Hybrid 暗号系を利用して、暗号文の長さが Mix-server の数に独立であり、且暗号化するテキストの長さに関係なく効率的に処理可能とした。

3.3 準同型性暗号方式

複数の管理センタ、掲示板で構成される。［CF85］により最初に提案され、［SK94］が［CY85］と同じ信頼

性を保ちつつ処理量、通信量を大幅に減少化、[CFSY86]が投票内容の正当性を検証する効率のよいプロトコルを、[CGS97]が投票者に要求される処理量、通信量が管理センタ数に依存しない方式を提案した。[TYK98]では2種の管理センタで構成した二重暗号化によるプライバシの保護プロトコルを提案し、[Sch99]は管理センタ数の変更に伴う公開鍵の再配布を不要としている。この他、EPOC暗号 Paillier暗号の適用も提案されている。各方式に関し研究例を第一表に示す。

4 各方式の比較

4.1 ブラインド署名方式

一番特長的なのは計算量、通信量の少量であることであり計算能力の小さい携帯デバイスへも適用可能。匿名チャンネルが必要ではあるが選挙に求められる匿名性、信用性の度合いに応じシステムを構成すれば実用上問題ないと考えられる。

4.2 ミックスネット方式

ブラインド署名方式とともに、投票内容に制約がないためアンケート調査も含め、様々な選挙・調査に適用可能である。プライバシ保護、公平性を保つ目的でシャッフル、復号を投票締切後に行う為の処理時間が他方式に比べ多くなる。

4.3 準同型性暗号方式

投票内容が二値に限定される反面、暗号化された票を準同型性を利用して集計でき、復号が一回で済む利点がある。また、この集計に当たって、現時点における票の正当性の検証プロトコルの実施が他の方式に比べ必要になる。

5 要求される新たな要件

以上に紹介したように電子投票方式の研究が進展してきた現在、三種の方式とも電子投票で満たすべき要件のほとんどを満たしていると言える。計算量、通信量の減少化にも多くの提案がなされ、またいくつかの実証実験や実際に利用する例も見られる。[FA0H00]では[F0093]の投票者の利便性を向上させた方式を含めて方式の実装、評価を行い公開実験を行っている。また[YKT00]では高次剰余暗号系の復号性能を実測し大規模選挙にも適用しうることを示し、また Biglobe を用いて公開実験を行い、実用性の検証を行っている。そこで我々は電子投票の実現が数年程先と予想して、その時点で存在する計算機器、通信機器を適用した場合のシステム構成の問題点、ならびに運用性の問題が新たな満たすべき要件になると考え考察する。

5.1 計算機器の能力に関する要件

現在の計算機器の計算能力をベースにムーアの法則に従って数年後の計算機器の計算能力を推定し必要とされる計算量に対する計算時間を考察する。

尚、通信能力に関しては最近提案されている各方式とも通信量は少なく、現在の通信機器適用において性能的な問題は少ないと考えるので割愛する。必要とされる計算量に関連するポイントとして次の二点を挙げる。

・選挙規模

住民台帳を管理する選挙管理委員会が選挙の電子化に伴っても当面は選挙の管理、開票を行うことが予想される。ここでは選挙規模を有権者100万人と仮定して考察する。

・計算処理上のボルトネック

RSA、ElGamal、高次剰余等、電子投票方式に適用される暗号系では指数・剰余計算が行われ、この計算量が他の計算に比べ圧倒的な割合を占める。そこで、本稿ではこの指数・剰余計算をベースに必要とされる計算時間を考察する。

(1)応答性能

・ピーク時における投票頻度：入 $_{PEAK}$（票数 $_{PEAK}$／秒）（投票発生はポアソン分布と仮定）

・管理センタのメッセージ処理時間：T（平均処理時間／票）ここでメッセージ処理内容の主なものは署名確認

・ピーク時の処理待メッセージ個数：Q_{PEAK}

$$Q_{PEAK}=\frac{入_{PEAK}\cdot T}{1-入_{PEAK}\cdot T}$$

ピーク時のトラヒック強度 $P_{PEAK}=入_{PEAK}\cdot T$ において P_{PEAK} は 0.6 以上となると指数的に増大するので 0.6 以下に保つことが必要。例えば T＝50msec、P＝0.5 と仮定すると入 $_{PEAK}$＝10（票数 $_{PEAK}$／sec）。ピーク時に 30 万票が集中するとして、約 100 票／sec であり、複数の計算機器にトラヒックを分散させる必要がある。必要とされる計算機器数：U_{resp}＝10（ユニット）となる。

(2)復号処理性能

復号時間を 50msec と仮定すると 100 万票の復号に約 15 時間要する。

現行の手作業による開票に比べ、電子化に伴い、より速い開票時間が期待されることを考え合わせると複数台の計算機器が必要となる。(1)、(2)を合わせ、計算能力の問題は(1)の方がボトルネックと言えよう。

5.2 計算機器の信頼性

EC システム、電子政府システムなど Web ベースのシステムに於いては従事の銀行の勘定系システムのようなミッションクリティカル性が要求されつつあり、高信頼性を実現する新たな方式が普及しつつある。

(1)システム（ハードウェア）の信頼性向上策

演算ユニット、メモリユニット、バス、ディスクの信頼性向上策として計算機器を多重に接続、処理結果比較を行うフォルトトレラントシステムが普及されつつある。多重化による計算機器数を U_{FT} とする。現在は 2 重化が主流であるが今後は 4 重化にも発展していくことが考えられる。

(2)システム（ソフトウェア）の信頼性向上策

ソフトウェア障害によるシステムダウン（OS パニック）、アプリケーション（投票プロトコル）エラーに関してはリソース管理プログラムなどにより障害監視を行い、ソフトウェア障害時に待機ノード切り替え、自動再起動するクラスタシステムが普及している。クラスタを構成する計算機器数を U_{CLST} とする。電子政府における電子住民台帳管理システムでは 4 重のフォルトトレラントシステムと 4 クラスタシステムも提案されており、電子住民台帳の管理と同一レベルの信頼性を要求される電子投票システムにおいても同様のシステム構成が望まれることが考えられる。

第一表　無記名電子選挙プロトコル

ブラインド署名方式	**Chaum [Cha85] [Cha88]** ○ブラインド署名(個人の匿名性を守りつつ、確かな署名である事が検証できる署名方式)を提示。 ○[Cha88] では複数の選挙管理センタを必要とせず、単独の選挙管理センタで構成。 ○開票作業は投票者全員が協力して一斉に同時に行わなくてはならない。 ○自分以外のすべての投票者が結託しない限りにおいて、個人のプライバシは保たれる。 ○indevidually verifiable(個別検証可能)な方式。 ○RSA 暗号ベースのブラインド署名を利用。 ○anonymous channel を物理的仮定として設定。	**太田[Oh88]** ○単独の選挙管理センタで構成できる方式の提案。 ○方式は、投票者、信頼できる選挙管理センター、集計センター、匿名通信路、および掲示板で構成される。 ○集計センタは著名確認後、掲示板に表示、各投票者は、掲示板で自分の票が存在する事を確認する事で individually verifiable(個別検証可能) な方式となっている。 ○投票者による 2 重投票を防止できる方式でき、もし行われた場合は、誰が行ったかを特定できる方式。 ○計算量・通信量共に実用的な範囲に抑えた。 ○不正が起きた場合、クレームを挙げる場合の投票者のプライバシが無い。 ○RSA 暗号ベースのブラインド署名を利用。 ○選挙管理センタと集計センタが結託しても投票者の匿名性を保護可能。 ○大規模選挙向け。 ○anonymous channel を物理的仮定として設定。 ○同時期に Chaum も anonymous channel を利用した方式を提案。
ミックスネット方式	**Chaum[Cha81]** ○匿名通信路：Mix-net を最初に提案。 ○RSA 型暗号に基づいて Mix-net を構成し、匿名性を確保。 ○複数の mix-server がカスケードの配置。 ○全ての mix-server が正しく動かなくては正確な出力は出ない。 ○投票者は、各 mix-server が保有する公開鍵で多重に暗号化した電子メールを投票。 ○投票者が送信する暗号文は、mix-server の数に依存し、増加する。 ○各 mix-server は各電子メール同士の順番をシャッフルし入力との対応をとれなくし、且つ復号処理を行う。 ○individually verifiable(個別検証可能) な方式。	**Park, 伊藤, 黒澤[PIK94]** ○ElGamal 暗号に基づいて構成。 ○暗号化されたテキスト長が mix-server 数に独立。 ○公平性を実現。 ○公平性を保つためには、各投票者の通信量は、ビット数 O(nk) ビット以上が好ましい。(ここで、n はビット長、k は mix-sever の数) ○全ての mix-server が正しく動かなくては正確な出力は出ない。 ○indevidually verifiable(個別検証可能) な方式。
準同型性暗号方式	**Benaloh,Yung [CY85][Ben86][Ben87]** ○投票者、n 個のセンタ、掲示板で構成 ○投票内容は賛成、反対の二値方式（以降、準同型暗号方式）を用いた提案はすべてこの二値方式 ○各センタは r 次剰余暗号（確立的暗号）を構成 ○投票者は自分の票を定数項とするランダムな(t-1)次多項式を構成、各センタの公開鍵で暗号化して公開し(t-1)次の多項式であることを証明 ○票の内容が 0 または 1 であることを暗号カプセルプロトコルを用いて証明[Ben86] ○各センタは自分に送られてきたものを復号、(t-1)次の多項式である為、t 個以上のセンタが正しく処理していれば結果を復元可 ○集計値の正当性を零知識証明プロトコルで証明 ○以上の証明に対する検証は誰でも（投票者、センタに限らず）掲示板上の情報を元にして行うことが出来る：Universal Verifiability	**佐古[SK94]** ○投票者、複数のセンタ、掲示板で構成 ○[CY85]と同じ信頼性を保ちつつ処理量、通信量を大幅に減少 [CY85]と比較して処理量 1/4、データ量を 1/80）投票時、投票者は仮投票に付加する情報を送付するのみ ○仮投票データ（１又は、-１）を事前に作成、提出し、正当性（暗号処理の正当性、仮投票内容の正当性）を零知識証明で誰でも検証可としている。重い計算やデータ転送は投票前に実施し実際の投票時に要する通信量、処理量を大幅に軽減 ○不正集計防止手段として、準同型暗号 E（X）=g^xmodq(X:平文、g,q 公開定数）を用い公表されたサブ集計とすべての投票文の一致性を準同型性を利用して暗号文のまま、誰でも検証可。[CY85]は準同型暗号として１対多に写像される確立暗号を用いるため零知識証明を使用

電子投票の各方式における管理センタと計算機器との関連で、ごく小規模の選挙においては一台の計算処理機器が複数のセンタの処理を実行可能な場合もあろうが、通常は一つの管理センタに関して複数台の計算処理機器が必要となる。
システム全体で必要な計算処理機器の台数は（管理センタ数：n）×（応答性能、復号処理性能条件を満たすべく分散化された計算処理機器台数：U_{RESP}）×（信頼性向上策に必要な計算処理機器台数：$U_{FT} \times U_{CLST}$）でその数は莫大なものになる。指数計算チップの開発や、投票方式のさらなる再考察が必要の場合もありうるだろう。

ブラインド署名方式	**浅野, 松本, 今井[AMI91]**	**佐古[Sk92]**
	○公平性問題を解決 ○不正が起きた場合、クレームを挙げる場合の投票者のプライバシが無い。 ○選挙管理センタが不正行為を行った場合に、投票者のプライバシが犯される。 ○選挙管理センタが各投票文に対する総当りの計算により投票内容を求めるような攻撃をしない範囲において、その公平性を保てている。 ○選挙管理センタが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○anonymous channel を物理的仮定として設定。	○集計センタの不正に対し、自己の票の内容を公開することなし異議申立てを行え、プライバシを保てる方式 ○異議申立ては有権者のみが提示できる Vote-tag を公開する事で行う。 ○賛成 or 反対 の 2 択の選挙において有効。 ○投票を破棄する投票者がいない事を仮定として設定。 ○RSA 暗号ベースのブラインド署名を利用。 ○署名は、投票内容を含まないメッセージに対してもらう。 ○選挙管理センタと集計センタが結託しても投票者の匿名性を保護可能。 ○集計センタが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○untappable channel（物理的に盗聴不可能な通信路）を物理的仮定として設定。
ミックスネット方式	**佐古, Killian[SK95]**	**Jakobsen[J98]**
	○[PIK93]の方式をベースに、ゼロ知識証明(Cut -and-Choose 方式)を利用しており、全体検証可能(universally verifiable)で、公開検証可能な方式。 ○無証拠性の性質を実現。 ○匿名通信路を物理的仮定として設定。 ○全ての mix server が正しく動かなくては正確な出力は出ない。 ○攻撃（n-2 サーバの結託で anonymity が破れる）が示されているが、容易に修正可能である。 ○堅牢性の性質を付加した方式が、1998 年に尾形、黒澤、佐古、高谷らにより提案されている。その閾値は 1/2 であり、不正な mix-server の数が 1/2 以下の場合、正確な結果を出力可能とした。 ○更に、頑健性の性質に加え、検証者の計算量を軽減させた方式が 1998 年に阿部により提案されている。	○閾値付き El Gamal 暗号に基づき構成。 ○効率の向上、各 Mix-Server の計算量は O(tN)。(ここで、t 閾値) ○1/N の確率で cheating が成功してしまう。(ここで、N は投票者の数)。その為、N の大きな大規模選挙向けの方式である。 ○全体検証可能(universally verifiable)であるが、公開検証可能ではない為、検証して納得できるのは mix-server 自身のみ。 ○[J98]方式は、Euro2000 で Desmedt、Kurosawa により攻撃方法が示されている。改善方法は提示されていない。代わりに、[J98]とは全く異なる方式も提示されている。 ○99 年に新たに方式を提案したが、その方式に関しては、Asiacrypto2000 にて Mitomo, Kurosawa により攻撃方法と改良方法とが発表されている。
準同型性暗号方式	**Gramer,Franklin,Schoenmakers,Yung [CFSY96]**	**Gramer,Gennaro,Schoenmakers, [CGS97]**
	○投票者、複数のセンタ、秘密通信路、掲示板で構成 ○離散対数問題に基づく準同型な暗号系を適用 ○マスク票に秘密情報を付加したものを票とする ○秘密情報を定数項とする(t-1)次の多項式を構成 ○上記多項式の各定数を暗号化し公開 ○マスク票を定数項とする(t-1)次の多項式を構成し、秘密通信路を用いて管理センタに送る ○多項式の正当性を 3-move プロトコルで検証 ○集計；t 個までの正しいセンタが集まると正しい集計値を得ることが出来る ○センタ数が 10 の場合、投票者に要求される通信量は約 10K ビット（離散対数方式における $\|P\|$=512 ビット, $\|q\|$=160 ビット）	○[CFSY96]ではセキュリティ強度の向上の目的等でセンタの個数を増加させる場合、投票者の作業量はセンタ毎に分割した票を作成、検証する方式の為、センタ数に比例して計算量、通信量が増加 ○本方式は投票者の計算量、通信量がセンタの個数に独立、投票者はシステムでただ一つの公開鍵で暗号化し、検証するのみ ○鍵生成 各センタが保有する分割秘密鍵 Sj を持ちより Lagrange 係数法により秘密鍵 S を生成（Shamir's(t-n)-Threshold secret sharing schem）.$h=g^s$ を公開鍵とする ○暗号系は ElGamal 暗号を適用、投票内容は G 又は 1／G ○票内容の正当性（G 又は 1/G）を検証する 3-move プロトコルを提案 ○票の集計に準同型性を利用 ○開票：指数部にある集計値をシーケンシャル検索法にて求める ○高次剰余暗号系も適用

5.3 運用性

通常、管理センタの公開鍵の発行に関しては、管理センタが認証局に依頼し、認証局がその鍵の有効期間（執行期間）を規定し発行する。中、小規模の選挙、あるいはアンケート調査においては選挙・調査間での管理センタの管理者の入れ替え、増減はしばしば発生する。このような管理者の入れ替え、増減が発生しても管理センタの公開鍵の再生成、再配布は不要にすることは投票者、アンケート回答者にとって望ましい機能であろう。

ブラインド署名方式	**藤岡，岡本，太田[F0093]**	**大久保，三浦，阿部，藤岡[OMAFO99]**
	○公平性、匿名性を両立させた方式。 ○公平性実現にはビットコミットメントを方式に組み込む事で実現。 ○投票内容は、2 択以外の内容にも対応可能。 ○投票者の集計処理への参加が必要。 ○選挙管理センタと集計センタが結託しても投票者の匿名性を保護可能。 ○集計センタが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○大規模投票に向いている。 ○anonymous channel を物理的仮定として設定。 ○sensus や e- vote 等を筆頭に実装・公開実験などが実施されている。 ○分かりやすい構成であるため、広く実用化されている。	○[FOO92]を改良。 ○walk-awayness（投票者は集計ステージに参加する必要がなく、投票の後は束縛されない性質）を実現。 ○公平性、匿名性を両立。 ○公平性を保つために用いられていたビットコミットの代わりに Threshold 暗号を用いている事により、公平性と匿名性の両性質を実現しつつ、ユーザの利便性を向上した方式。 ○選挙管理センタと集計センタが結託しても投票者の匿名性を保護可能。 ○集計センタが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○大規模投票に向いている。 ○anonymous channel を物理的仮定として設定。Mix-net による匿名通信路の実装も提示。
ミックスネット方式	**阿部[Ab00]**	**大久保，阿部[OA01]**
	○MIX への入出力数が N に対して、2 入力 2 出力の permutation を多段に組み合わせる構造。 ○2 入力 2 出力の permutation により、入出力が N である Mix-net を構成する最適な組み合わせについて解析。 ○全体検証可能(universally verifiable) であり、且つ公開検証可能である方式であり、且つ堅牢性を保持できる方式として、Cut-and-Chooose 方式を用いずに実現した初めての方式。 ○従来方式の多くは、mix-server 間の通信が頻繁に行われるものが多いが、この方式では各 mix-serbver のプロトコルへの参加を極端に抑える事が出来ている。 ○2 方式提案されており、各 mix-server の処理が 1 度の方式と 2 度の方式とがある。 ○Permutation Network の計算量は O(t N logN)。 ○N がそれほど大きくならない小・中規模の投票に適している。 ○修正と高速化が[AH01]で示されている。 ○２べき以外の入力数の効率的な扱いが[Su01]で示されている。	○Hybrid 型暗号系を利用(ElGamal 暗号と共通鍵暗号とに基づく方式)。 ○各 mix-server の公開鍵の生成方法に工夫があり、前段の server の公開鍵を元に生成される。 ○投票者は平文(投票内容)を共通鍵暗号で n 多重に暗号化する。(ここで、n は mix-server の数) ○共通鍵暗号による平文の暗号化に用いる共通鍵は、各 mix-server の公開鍵に基づき生成。 ○暗号化されたテキストの長さが mix-server の数に独立。 ○ElGamal 暗号に基づく Mix-net では一度に処理できる平文の長さが公開鍵の長さによって制限されるが、 この方式では固定任意長の平文を処理できる。 ○計算量・通信量共に効率的な方式。 ○投票者・閾値以下の mix-server の不正に対しては、堅牢性を保持できる方式。
準同型性暗号方式	**辻井、山口、北沢、黒澤 [TYK98]**	**Scheumaker[Sch99]**
	○有権性確認・集計及び開票を行う二種の管理センタ及び公開ボードで構成 ○準同型性特性を有する高次剰余暗号系を適用、暗号化されたままの各票を掛け合わせることにより集計 ○高次剰余暗号系の秘密鍵を保有する開票センタにより各個人各票を開票されるのを防ぐ目的で高次剰余暗号系で暗号化された票をさらに RSA 暗号系（有権性確認集計センタが秘密鍵保有）で暗号化したものを公開ボードに表示 ○二重暗号化された票が賛成、反対票の条件を満たしていることを Benaloh の暗号カプセルに機能追加して検証可とした。 ○正しく集計していることの検証プロトコルを提案 ○復合処理時間を実測し大規模選挙にも適用可の事を証明[YKT00] ○Biglobe を使用した実証実験を行い実用性の検証を行った[YKT00]	○Public Verifiable Secret Sharing(PVSS,Stadler により提安)方式であり、藤崎、岡本[FO98]の効率向上版 ○投票内容 $V \in \{0,1\}$ に秘密情報 S を付加し Diffie -Herman 仮定の下 $U=G^{s+v}$ を公開 ○秘密情報 S を定数項とする(t-1)次の多項式を構成し、各センタの公開鍵で暗号化し公開 ○上記多項式の各定数 αj より $g^{\alpha j}$ を求め公開 ○多項式の正当性の正当性を検証する ○[CGS97]方式において、各センタが保有する分割秘密鍵を持ち寄って秘密鍵を生成する方式においてはセンタ管理者、センタ数の変更に伴い公開鍵の再生成が必要であるが本方式はこの再生成が不要 ○CFSY96 は分割秘密情報を秘密通信路を介して送る方式であるが、本方式は秘密通信路の必要はない ○CFSY96 は各票を一つ一つ復号するが本方式は加算（集計）された票を復号するのみ

6 まとめ

電子投票・アンケート方式に関し三つの方式に分類し、研究の流れに沿って特長を列挙し比較を行った。近い将来の実用化に向けて適用する計算機器の性能、信頼性を考慮した場合の問題点を考察した。

謝辞

本研究の一部は、通信、放送機構の ”超楕円暗号を核とした ”高性能セキュリィの実現と電子社会への応用プロジェクト ” の支援により行った。

参考文献

[Ab00] M.Abe,Universally Verifiable Mix-Net with Verification Work Independent of the Mumber of Mix-Servers,IEICE TRANS,Fundamentals, Vol.E83-A,No.7.July, 2000

[AMI91] T.Asano,and T.Matsumoto, and H.Imai, A Study on Some Schemes for Fair Electronic Secret Voting, The Proceedings of the 1991 Symposium on Cryptography and Information Security,SCIS [13-18,1991]

[Ben86] J.Benaloh, Cryptographic capsules: A disjunctive primitive for interactive protocols, Proc. of CRYPTO '86, LNCS 263m, pp.213-222, 1986.

[Ben87] J.Benaloh, Verifiable Secret-Ballot Elections, PhD thesis,Yale University,Department of Computer Science Department,New Haven,CT, 1987

[BY85] J.Benaloh, and M.Yung. Distributing the power of a government to enhance the privacy of voters,In Annual Symposium on Principles of Distributed Computing,pp.52-62,1985

[Cha81] D.Chaum, Untraceable electornic mail, return addresses, and digital pseudonyms,Communications of the ACM, pp.84-88, ACM, 1981.

[Cha85] D.Chaum, Security without identification. Transaction Systems to Make Big Brother Obsolete, Comm.of the ACM, pp.1030- 1044, ACM, 1985.

[Cha88] D.Chaum, Election with Unconditionally- Secret Ballots and Disruption Equivalent to Breaking RSA, in Advance in Cryptology-EUROCRYPTO '88, Lecture Notes in Computer Science330, Springer-Verlag, Berline,pp.177-182,1988

[CFSY96]R.Cramer,M.Franklin,B.Schoenmakers, and M.Yung, Multi-authority secret ballot elections with linear work. In Advances in Cryptology-EUROCRYPT'96, volume 1070 of Lecture Notes in Computer Science, Springer-Verlag,Berlin,1996

[CGS97] R.Cramer, R.Gennaro and B.Schoenmakers, A secure and optimally efficient multi- authority election scheme, Advances in Cryptology-EUROCRYPT'97, volume 1233 of Lecture Notes in Computer Science, Springer-Verlag, Konstanz, pp.103-118, 1997.

[FAOH00]A.Fujioka,M.Abe,M.Ohkubo,and F.Hoshino,An Implemtation and Experiment of a Practical and Secure Voting Schme,SCIS200-C48,The 2000 Symposium on Cryptography and Information Security,Japan,2000

[FO98] E.Fujisaki, and T.Okamoto, A Practical and provably Secure Scheme for Publicly Verifiable Secret Sharing And Its Applications,In Advances in Cryptology-EUROCRYPT'98,volume 1403 of Lecture Notes in Computer Science,pp.32-46,Berlin,1998,Springer-Verlag.

[FOO93] A. Fujioka, T.Okamoto, and K.Ohta,A practical secret voting scheme for Largescale elections,in Advances in Cryptology-AUSCRYPTO'92,Lecture Notes in Computer Science718,Springer-Verlag, Berlin, pp.244-251, 1993

[J98] M.Jakobsson, A Practical mix, in ed.K.Nyberg, Advances in Cryptology-EUROCRYPT'98 8,vol.1403, Lecture Notes in Computer Science,pp.448-461, Springer-Verlag,1998

[OA01] Miyako Ohkubo, and M Abe,A Robust Length-invariant Hybrid Mix,Technical Report of IEICE,E-84-A,pp.931 -940,2001

[OMAFO99]M.Ohkubo,F.Miura,M.Abe,A.Fujioka, and T.Okamoto, an Improvement on a Practical Secret Voting Scheme,pp.226-234,1999

[Oh88] K.Ohta, An Electrical voting scheme using a single dministrator, IEICE Spring National Convention Record A-294, pp.296, 1988.

[PIK94] C.Park,K.Ithoh,and K.Kurosawa, Efficient anonymous channel and all/nothing election scheme, in ed.T. Helleseth,Advances in Cryptology-EUROCRYOT'93, vol.765,Lecturer Notes in Computer Science, pp.248-259,Springer -Verlag,1994

[SK92] K.Sako,Electronic Voting System with Objection to the ,SCIS92-13C.,1992

[SK94] K.Sako, and J.Kilian, Secure voting using partially compatible homomorphisms, In Advances in Cryptology－CRYPTO'94 Science, pp.411-424, Springer-Verlag, Berlin, 1994.

[SK95] K.Saklo, and J.Kilian,Receipt-Free Mix-Type Voting Scheme-a Proactical Solution to the Implementation of a voting booth,In Advances in Cryptology-Eurocrypt'95,volume921,pp.393-403,199

[Sch99] B..Shoenmakers, A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting,

[TYK98] S.Tsujii, H.Yamaguchi, A.Kitazawa, and K.Kurosawa, A Method for Voting Protocols with regards to Privacy, Technical report of EICE, ISEC98, PP45-51, 1998

[YKT00] H.Yamaguchi, A.Kitazawa, T.Kimura, and S.Tsujii, A Method for Voting Protocols with Regards to Privacy -No.3-, Experimental Results,Technical report of IEICE, ISEC2000, pp163-170, 2000.