

実用的な電子投票方式の実装および実験

An Implementation and an Experiment of a Practical and Secure Voting Scheme

藤岡 淳* 阿部 正幸* 大久保 美也子* 星野 文学*
Atsushi FUJIOKA Masayuki ABE Miyako OHKUBO Fumitaka HOSHINO

あらまし 最近、世界中で試験的に実装されている電子投票方式 (FOO 方式) の投票者の利便性 (非待機性) を向上させた方式を紹介し、その実装 (および公開実験) について述べる。この方式では、開票者を複数おき、投票内容を開票者が分散復号可能な閾値暗号で暗号化することにより、公平性と非待機性を両立させている。また、この方式の実装を試み、方式全体の評価や実用性についての検討を行ない、今後予定している公開実験について述べる。

キーワード 電子投票、実装、インターネット

1 まえがき

近年、現代暗号理論を駆使した様々な暗号プロトコルが考案されており、国内外で盛んに研究されている電子投票方式もその一つである。この電子投票方式には、いくつか実用的な方式が提案されているが、実際に実装されたり、現実に利用を試みたものは少ない [Cr00]。

1992 年に提案された FOO 方式 [FOO92] は実用的な電子投票方式であり、その提案後に複数の団体により実装され、また、それを用いた実験が行なわれた数少ない方式である [Cr00]。この実装例としては、Sensus [CC96] と E-Vox [He97] が挙げられる。

しかしながら、この FOO 方式には、実用面、すなわち、投票者の利便性において大きな欠点が存在している。この方式に基づいている Sensus や E-Vox の両実装においても、この欠点を回避することを試みているが、それがために、あらたな問題が生じたり、冗長なプロトコルとなっている [Oetal99]。

ここでは、実用面での欠点を解消した新方式 [Oetal99] を紹介し、また、これの実装による評価、および、公開実験について述べる。

以下の議論のため、電子投票方式が満たすべき要件として、以下の九条件を挙げておく [FFO95, OY97]。

完全性 不正がなければ、正しく投票が行なわれるこ。

健全性	投票を混乱させることができうこと。
有権者確認可能性	有権者のみが投票者になれること。
二重投票不能性	有権者が一回のみ投票できること。
無記名性	投票者と投票の関係が不明なこと。
公平性	途中経過が漏洩しないこと。
検証可能性	開票結果を検証できること。
非待機性	投票者は投票後に拘束されること。
無証拠性	投票者は投票内容を偽れること ¹ 。

2 実用的な電子投票方式

2.1 FOO 方式

2.1.1 FOO 方式のプロトコル

FOO 方式は、ブラインド署名 [Ch85] を利用した電子投票方式である。この方式は、ブラインド署名と匿名通信路 [Ch81] を用いることで、二重投票不能性と無記名性を両立させている [FOO92]。

FOO 方式は、投票者、選挙管理者、開票者の三者からなり、そのプロトコルは、以下の通りである。

- 「認証」フェーズ
 - 投票者は投票内容を拘束し、それに対する選挙管理者の署名をブラインド署名で入手する。

¹ 本稿では、無証拠性 [BT94] については考慮しないものとする。これは、今までのところ、無証拠性を満足する実用的な方式は提案されていないからである。

* 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所, 〒 239-0847 神奈川県横須賀市光の丘 1-1, NTT Information Sharing Platform Laboratories, 1-1 Hikarinooka, Yokosuka-shi, Kanagawa-ken, 239-0847 JAPAN

- 「投票」フェーズ
 - 投票者は、選挙管理者の署名付き（拘束された）投票内容を匿名通信路で、開票者に送付する。
 - 開票者は署名付き（拘束された）投票内容を公表する。
- 「開票」フェーズ
 - 投票者は、投票内容の開示に用いる情報を匿名通信路で、開票者に送付する。
 - 開票者は、受信した情報で投票内容を開示する。

ここで、投票内容は、「投票」フェーズにおいて、投票者の選んだ bit commitment 関数により拘束され、「開票」フェーズでは、この bit commitment に用いた情報を投票者が送信することで開示されている。

2.1.2 FOO 方式の欠点

しかしながら、この FOO 方式において、投票者は投票内容を開示するために「開票」フェーズにも従事せねばならず、これは非待機性を満足していないことを意味している²。そもそも、FOO 方式では、公平性を満足することを主眼に提案された方式であり、非待機性については、考慮されていなかった。

この公平性と非待機性の関係は、二重投票不能性と無記名性の関係のように、一見矛盾するように思える。

公平性を満足するためには、投票内容は「投票」フェーズが終了するまで、明らかになってはならず、単純な解決としては、この FOO 方式のように「開票」フェーズにも投票者が参加させることであるが、これでは非待機性が満足されなくなる。

逆に、非待機性を満足するためには、投票内容は投票者の参加なしに開票されなくてはならないため、「投票」フェーズでの公平性が脅かされる危険が存在することになる。

2.2 BAR 方式

これらの、一見矛盾する問題を解決するために提案された方式が BAR 方式である [Oetal99]。

この方式は、開票者を複数おき、投票内容を bit commitment 関数により拘束するのではなく、その複数の開票者が分散復号 [DF89] することにより開示されるような暗号化関数を用いて拘束するものである。

- 「認証」フェーズ
 - 投票者は投票内容を開票者の公開鍵で暗号化し、それに対する選挙管理者の署名をブラインド署名で入手する。

² 非待機性と無証拠性を除く七条件は満足している [FOO92]。

- 「投票」フェーズ
 - 投票者は、選挙管理者の署名付き（暗号化された）投票内容を匿名通信路で、開票者に送付する。
 - 開票者は署名付き（暗号化された）投票内容を公表する。
- 「開票」フェーズ
 - 開票者は、暗号化された投票内容を協調して復号化し、開票する。

これにより、投票者は、「開票」フェーズまで参加する必要がなくなり、また、公平性はすべての開票者が不正を行なわないかぎり満足されることになる [Oetal99]。

3 実用的な電子投票方式の実装

3.1 構成

本章では、上に紹介された BAR 方式をインターネット上で運用するに適した実装について述べる。

BAR 方式を実装する上において、最も問題となる点は、この方式が匿名通信路という物理的な仮定を用いていることである。現在のインターネットでは、匿名で通信するという機能は提供されていないために、この機能を満足するモジュールも実装する必要がある。

この匿名通信機能を満足する現実解として、MIX-net [Ch81] があり、これで、匿名通信路を代用することを考える。また、検証可能性の観点から、通信履歴などを公開する必要があるため、この機能を満足するものとして、公開掲示板を用いる。すなわち、1991 年に浅野らにより提案された匿名書き込み可能な掲示板 [AMI91] の考え方を拡張し、各 MIX が書き込み可能な掲示板経由でデータのやりとりを行ない、実際の機能として、匿名通信を行なうものとする。

今回の実装では、

- 複数の投票者 (client)
- 単一の掲示板管理者 (bubo)
- 単一の選挙管理者 (admin)
- 複数の開票者 (coco)
- 単一のプライバシ保護者 (mix)

を実現するモジュールを置き、また、具体的な暗号・署名方式としては、選挙管理者の署名方式に Schnorr 署名 [Sc91] を、開票者の暗号方式に 閾値付き ElGamal 暗号 [DF89] を用いている。更に、MIX-net としては、暗号化方式に、単純に ElGamal 暗号 [El85] だけを用いたもの（以下、Simple MIX と呼ぶ）と Diffie-Hellman 鍵共

有 [DH76] と DES 暗号 [NBS77] を組合せたもの [Oh00] (以下, Hybrid MIX と呼ぶ) の二種類を実装した.

これらは, SunOS 4.1.X, Digital UNIX 4.0, FreeBSD 2.2.X, Linux 2.0 上で稼働し, 各モジュールは,

- 演算部: 独自の多倍長演算ライブラリ
- 通信部: ソケット
- 格納部: Berkeley DB

を用いて実装されている.

3.2 プロトコル

ここでは, 実装された個々のモジュール間の通信について概略を示す.

- 「認証」フェーズ

- client (投票者) は投票内容を coco (開票者) 全体の公開鍵で暗号化し, admin (選挙管理者) とプロトコルを開始する.
- admin は, 有権者リスト, および, 受付リストをチェックし, ブラインド署名を発行する.
- client は, (暗号化された) 投票内容に対する admin の署名を入手する.

- 「投票」フェーズ

- client は, admin の署名付き (暗号化された) 投票内容を mix (プライバシ保護者) の鍵で暗号化する.
- client は, 暗号化されたデータを自分の署名付きで bubo (掲示板管理者) に送付する.
- bubo は, client の署名を検証し, 合格したデータを保存する.

- 「開票」フェーズ

- bubo は, 合格したデータをすべて mix に送付する.
- mix は, 受信したデータを復号し bubo に送付する.
- bubo は, 受信したデータ (admin の署名付き暗号化された投票内容) の admin の署名を検証し, 合格したデータを保存する.
- bubo は, 合格したデータをすべて coco それぞれに送付する.
- それぞれの coco は, 自分の所有する秘密鍵で受信したデータを復号し, bubo に送付する.
- bubo は, 受信したデータから投票内容を構築する.

この実装において, mix が存在するために, すべての投票は「投票」フェーズが終了するまで, coco に届かないことになる. よって, 公公平性を満足するための投票内容の開票者に対する暗号化は, 実際には不要である. しかし, 以下で行なうように, 各フェーズでの処理時間を評価するため(例えば, モジュール coco の処理時間を評価するため)に, 冗長ではあるが二重の暗号化を行なった. また, 将来的には, 別種の匿名通信路を用いた場合に備えて, 匿名通信部分は電子投票方式の実装に対する別モジュールとして切り分けることを考えている.

3.3 性能

ここでは, シミュレーションの結果について述べる. 以下は, platform として, Pentium II 400MHz (Linux 2.0) を用い, 十人の投票者に対するそれぞれのプロセスにかかる時間である(シミュレーションのため, 通信時間は考慮されていない). また, 開票者の暗号方式としては, (3,7)-閾値暗号(すなわち, 七名中四名が開票に協力すれば復号可能)を用いている. また, 開票者は, 七名中二名が協力しなかった場合を想定している.

表 1: 各モジュールの処理時間 [単位: sec]

Program	Simple MIX	Hybrid MIX
admin	00.20	00.20
client	04.95	02.84
mix	02.52	00.81
bubo	04.08	04.08
coco	03.05	03.04
Total	14.83	10.99

ここで, 投票者 (client) の処理時間は, 十名の処理時間の総和である. よって, どちらの MIX を用いた場合でも, 投票者の処理時間は一秒以下であることが分かる.

以下, 単純計算で, 十万人規模の選挙に適用した場合について考察する. 各処理時間を十分の十万倍, すなわち, 一万倍して求めるとする.

選挙管理者 (admin) の処理時間は, 約 33.4 分である. 次に, 掲示板管理者 (bubo) と開票者 (coco) の処理時間は, それぞれ約 11.4 時間と約 8.5 時間となる. また, プライバシ保護者 (mix) の処理時間は Hybrid MIX を用いた場合で約 2.3 時間, Simple MIX では約 7.0 時間である.

まず, 「認証」フェーズにおける処理時間は, そのまま約 33.4 分であることが分かる. 次に, 「投票」フェーズ・「開票」フェーズを合わせた処理時間は client, mix, bubo, coco それぞれの処理時間の合計と考えられるので, Hybrid MIX を用いると, およそ 22.2 時間, Simple MIX

の場合、約 26.9 時間となる。よって、十万人規模の現実の選挙に対して、Pentium II (400MHz) マシンのような普通のコンピューター一台を用いたとしても、一日程度で開票が可能となることが分かる。

しかしながら、以上の考察は通信部分を考慮していないものであり、また、推定した処理時間もシミュレーションで得られた値の線形推測に過ぎない。よって、今後は、実際に、インターネットを用いて、複数の大学（中央大学、東海大学、東京大学、横浜国立大学、早稲田大学（五十音順）を予定）を結び、数十から数百人規模の公開実験を行なうことで、このモジュールの性能評価などを行なう予定である。

4 まとめ

最近、世界中で試験的に実装されている電子投票方式 (FOO 方式) の投票者の利便性（非待機性）を向上させた方式を紹介し、その実装（および公開実験）について述べた。本方式では、開票者を複数おき、投票内容を開票者が分散復号可能な閾値暗号で暗号化することにより、公平性と非待機性を両立させている。また、この方式の実装を試み、方式全体の評価や実用性についての検討を行ない、今後予定している公開実験について述べた。

謝辞

本稿に対し、御協力頂いた東海大学菊池 浩明講師東京大学古原 和邦技官、早稲田大学上岡 祐一氏、早稲田大学西本 聰氏、早稲田大学福元 徳広氏、横浜国立大学井上 大介氏、横浜国立大学田中 直樹氏に感謝する。

参考文献

- [AMI91] 浅野、松本、今井，“公平な電子無記名投票について”，SCIS91, 12A (Feb., 1991).
- [BT94] J. Benaloh and D. Tuinstra, “Receipt-Free Secret-Ballot Elections”, STOC94, pp.544–553 (Feb., 1994).
- [Ch81] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, *Commun. ACM*, Vol.24, No.2, pp.84–88 (Feb., 1981).
- [Ch85] D. Chaum, “Security without Identification: Transaction systems to Make Big Brother Obsolete”, *Commun. ACM*, Vol.28, No.10, pp.1030–1044 (Oct., 1985).
- [Cr00] L. F. Cranor, “Electronic Voting Hot List”, <http://www.ccrc.wustl.edu/~lorracks/sensus/hotlist.html> (Jan., 2000).

- [CC96] L. F. Cranor and R. K. Cytron, “Design and Implementation of a Practical Security-Conscious Electronic Polling System”, Technical Report WUCS-96-02, Department of Computer Science, Washington University, St. Louis (Jan., 1996).
- [DF89] Y. G. Desmedt and Y. Frankel, “Threshold Cryptosystems”, in *CRYPTO '89*, LNCS 435, Springer-Verlag, pp.307–315 (1990).
- [DH76] W. Diffie and M. Hellman, “New Directions in Cryptography”, *IEEE Trans. on Information Theory*, Vol. IT-22, No.6, pp.644–654 (Nov., 1976).
- [El85] T. ElGamal, “A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms”, *IEEE Trans. on Information Theory*, Vol. IT-31, No.4, pp.469–472 (July, 1985).
- [FFO95] 藤岡、藤崎、岡本，“電子投票方式”，*NTT R&D*, Vol.44, No.10, pp.939–976 (Oct., 1995).
- [FOO92] A. Fujioka, T. Okamoto, and K. Ohta, “A Practical Secret Voting Scheme for Large Scale Elections”, in *AUSCRYPT '92*, LNCS 718, Springer-Verlag, pp.244–251 (1993).
- [He97] M. A. Herschberg, “Secure Electronic Voting Over the World Wide Web”, Master Thesis in Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology (1997).
- [NBS77] “Data Encryption Standard”, (Federal Information Processing Standards Publication 46), U.S. Department of Commerce, National Bureau of Standards, (1977).
- [Oetal99] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto, “An improvement on a Practical Secret Voting Scheme”, in *ISW'99*, LNCS 1729, Springer-Verlag, pp.225–234 (1999).
- [Oh00] 大久保，“暗号文の長さが不变な Hybrid Mix”，SCIS2000, B29 (Jan., 2000).
- [OY97] 岡本、山本, 現代暗号理論, 産業図書 (1997).
- [Sc91] C. P. Schnorr, “Efficient Signature Generation for Smart Cards”, *Journal of Cryptology*, Vol.3, No.4, pp.239–252 (1991).