A Practical Secret Voting Scheme for Large Scale Elections

Atsushi Fujioka Tatsuaki Okamoto Kazuo Ohta

NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-2356 Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan

Abstract. This paper proposes a practical secret voting scheme for large scale elections. The participants of the scheme are voters, an administrator, and a counter. The scheme ensures the privacy of the voters even if both the administrator and the counter conspire, and realizes voting fairness, i.e., no one can know even intermediate result of the voting. Furthermore fraud by either the voter or the administrator is prohibited.

1 Introduction

Secret voting schemes have been proposed by many researchers from both the theoretical and practical points of view.

In the scheme using the multi-party protocol [GMW87, BGW88, CCD88], all procedures are managed by just the voters, however, it takes many communication acts to prove that all acts were performed correctly. Therefore, this approach is interesting theoretically, but is impractical. A practical secret voting scheme requires additional participants, e.g., a trusted center or an administrator.

There are two types of this approach: one is the voter sends the ballot in an encrypted form and the other is voter sends the ballot through an anonymous communication channel.

The first type have been proposed by Benaloh (Cohen) *et al.* and Iversen [CF85, BY86, Iv91], and their schemes utilize the higher degree residue encryption technique. The scheme in [CF85] needs distributed centers to protect voter privacy, however, the voter must prove that the distributed ballot is valid, so all voting must be done at the same time. Iversen [Iv91] evades this problem by using the technique proposed to realize electronic money [CFN90]. However, the essential drawback of this approach is that if all centers conspire, the privacy of voters is violated. Moreover, these schemes are less practical for large scale elections, since it takes a lot of communication and computation overhead when the number of voters is large.

As a scheme of the second type, Chaum proposed a voting scheme that used an anonymous communication channel, and it provides unconditionally security against tracing the voting [Ch88b]. Independently Ohta proposed a practical secret voting scheme using only one administrator in similar manner [Oh88]. These schemes are more suitable for large scale elections, since the communication and computation overheads are reasonable even if the number of voters is large.

However, both schemes have the same drawbacks: the problems of fairness and privacy. As the fairness problem, these schemes don't ensure voting fairness, i.e., the center knows the intermediate result of opening the ballot, so he can affect the voting by leaking the result. As the privacy problem, voter's privacy is violated, when a voter notices that his voting was not counted correctly, and claims it by showing his voting.

Recently, Asano *et al.* proposed a scheme which overcomes the fairness problem [AMI91]. This scheme, unfortunately, is not secure against disruption by the administrator. Subsequently, Sako proposed a scheme to solve the privacy problem [Sa92]. This scheme, however, doesn't overcome the fairness problem and voting is limited to only yes/no.

Therefore, no practical and secure secret voting scheme has been proposed which is suitable for large scale elections (or based on the second type) and solves the privacy and fairness problems at the same time.

This paper solves these problems: we propose practical and secure secret voting scheme which is suitable for large scale elections and solves the privacy and fairness problems at the same time. That is, our scheme ensures the privacy of the voters even if both the administrator and the counter conspire, and voting fairness, i.e., no one can know even intermediate result of the voting. Furthermore fraud by either the voter or the administrator is prohibited.

Section 2 defines the security needed by a practical secret voting scheme. In **Section 3**, a practical secret voting scheme is proposed and we prove that the proposed scheme is secure, and we conclude this paper in **Section 4**.

2 Security of Secret Voting Scheme

In this paper, we discuss the security of the secret voting scheme using the following definition.

Definition 1. We say that the secret voting scheme is *secure* if we have the following:

- *Completeness* ... All valid votes are counted correctly.
- *Soundness* ..... The dishonest voter cannot disrupt the voting.
- *Privacy* ..... All votes must be secret.
- *Unreusability* .... No voter can vote twice.
- *Eligibility* ..... No one who isn't allowed to vote can vote.
- *Fairness* ..... Nothing must affect the voting.
- *Verifiability* ..... No one can falsify the result of the voting.

3 Proposed Voting Scheme

3.1 Model of Proposed Scheme

Our model consists of voters, an administrator, and a counter (the counter can be replaced with a public board), and the voters and the counter communicate through an anonymous communication channel [Ch81, Pf84, Ch88a]. The

scheme requires the bit-commitment scheme [Na90], the ordinary digital signature scheme [DH76], and the blind signature scheme [Ch85].

Every voter has his own ordinary digital signature scheme, and the administrator has blind signature scheme. The counter only creates a list of ballots, and publishes it.

3.2 Notations

In this paper, we use the following notations.

V_i: Voter i
A: Administrator
C: Counter
$\xi(v,k)$: Bit-commitment scheme for message v using key k
$\sigma_i(m)$: Voter V_i's signature scheme
$\sigma_A(m)$: Administrator's signature scheme
$\chi_A(m,r)$: Blinding technique for message m and random number r
$\delta_A(s,r)$: Retrieving technique of blind signature
ID_i: Voter V_i's identification
v_i: Vote of voter V_i

3.3 Structure of Proposed Scheme

In this subsection, we propose a practical secret voting scheme based on the model described in **Subsection 3.1**. The proposed scheme is secure in the sense of **Definition 1**.

First we outline the proposed scheme. The scheme consists of the following stages executed by the voters, the administrator, and the counter.

PREPARATION:	Voter fills in a ballot, makes the message using the blind signature technique to get the administrator's signature, and sends it to the administrator.
ADMINISTRATION:	Administrator signs the message in which the voter's ballot is hidden, and returns the signature to the voter.
VOTING:	The voter gets the ballot signed by administrator, and sends it to the counter anonymously.
COLLECTING:	Counter publishes a list of the received ballots.
OPENING:	The voter opens his vote by sending his encryption key anonymously.
COUNTING:	Counter counts the voting and announces the result.

Roughly speaking, the voter prepares a ballot, get a administration, and vote anonymously. Administrator gives a administration to an eligible voter, and counter only collects the ballots and published a list.

On the communication between the voter and the administrator, voter gets qualification, and after it, voter acts anonymously. The blinding signature technique provides the separation between the identification and anonymous communication.

Here we explain the scheme in detail.

- PREPARATION
  - Voter V_i selects vote v_i and completes the ballot $x_i = \xi(v_i, k_i)$ using a key k_i randomly chosen.
  - V_i computes the message e_i using blinding technique $e_i = \chi(x_i, r_i)$.
  - V_i signs $s_i = \sigma_i(e_i)$ to e_i and sends $\langle ID_i, e_i, s_i \rangle$ to administrator.
- ADMINISTRATION
  - Administrator A checks that the voter V_i has the right to vote. If V_i doesn't have the right, A rejects the administration.
  - A checks that V_i has not already applied for a signature. If V_i has already applied, A rejects the administration.
  - A checks the signature s_i of message e_i. If they are valid, then A signs $d_i = \sigma_A(e_i)$ to e_i and sends d_i as A's certificate to V_i.
  - At the end of the ADMINISTRATION stage, A announces the number of voters who were given the administrator's signature, and publishes a list that contains $\langle ID_i, e_i, s_i \rangle$.
- VOTING
  - Voter V_i retrieves the desired signature y_i of the ballot x_i by $y_i = \delta(d_i, r_i)$.
  - V_i checks that y_i is the administrator's signature of x_i. If the check fails, V_i claims it by showing that $\langle x_i, y_i \rangle$ is invalid.
  - V_i sends $\langle x_i, y_i \rangle$ to the counter through the anonymous communication channel.
- COLLECTING
  - Counter C checks the signature y_i of the ballot x_i using the administrator's verification key. If the check succeeds, C enters $\langle l, x_i, y_i \rangle$ onto a list with number l.
  - After all voters vote, C publishes the list. (The list can be accessed by all voters.)

Table 1. List of the ballots (in the COLLECTING stage)

Entry	Ballot & additional information
1	x_j, y_j
⋮	⋮
l	x_i, y_i
⋮	⋮

- OPENING
  - Voter Vi checks that the number of ballots on list is equal to the number of voters. If the check fails, voters claim this by opening r_i used in encryption.
  - V_i checks that his ballot is listed on the list. If his vote is not listed, then V_i claims this by opening $\langle x_i, y_i \rangle$, the valid ballot and its signature.
  - V_i sends key k_i with number l, i.e., $\langle l, k_i \rangle$ to C through an anonymous communication channel.
- COUNTING
  - Counter C opens the commitment of the ballot x_i, retrieves the vote v_i (or C adds k_i and v_i to the list), and checks that v_i is valid voting.
  - C counts the voting and announces the voting results.

Table 2. List of the ballots (in the COUNTING stage)

Entry	Ballot & additional information
1	x_j, y_j, k_j, v_j
$\vdots$	$\vdots$
l	x_i, y_i, k_i, v_i
$\vdots$	$\vdots$

3.4 Security

Theorem 1 (Completeness). *If every participant (the voters, the administrator, and the counter) is honest, the result of the voting is trustable.*

Sketch of Proof. It is clear. □

Theorem 2 (Soundness). *Even if a voter intends to disrupt the election, there is no way to do it.*

Sketch of Proof. The only way to disrupt the elections is for the voter to keep sending invalid ballots, however, this can be detected in the COUNTING stage. Furthermore, the votes are bound by using the bit-commitment scheme, so the voter cannot change his mind. □

Remark. It is possible to assume that the voter sends an illegal key which cannot open the vote. In this situation, there is no way to distinguish between a dishonest voter or a dishonest counter. To prevent this, the voter should send his key to several independent parties, e.g., the candidates of the election, who are assumed not to collaborate.

Theorem 3 (Privacy). *Even if the administrator and the counter conspire, they cannot detect the relation between vote v_i and voter V_i.*

Sketch of Proof. The relation between the voter's identity ID_i and the ballot x_i is hidden by the blind signature scheme. The ballot x_i and the key k_i are sent through the anonymous communication channel. So no one can trace the communication and violet the privacy of the voters. It is unconditionally secure against tracing the voting.

In addition, when the voter claim the disruption by the administrator or counter, he need not release his vote v_i.

In VOTING stage, when the administrator sends the invalid signature, the voter only show the pair $\langle x_i, y_i \rangle$ to claim the cheating.

In OPENING stage, when the counter doesn't list the voter's ballot, the voter only show the pair $\langle x_i, y_i \rangle$ to claim the disruption.

So he can claim the disruption with keeping his vote v_i secret. This ensures the voter's privacy. □

Theorem 4 (Unreusability). *Assume that no voter can break the blind signature scheme. Then, the voter cannot reuse the right to vote.*

Sketch of Proof. To vote twice, voter must have two valid pairs of the ballot and the signature. He can get one signature by right procedure, however, he has to create another pair by himself. This means that he can break the blind signature scheme, and it contradicts the assumption. □

Theorem 5 (Eligibility). *Assume that no one can break the ordinary digital signature scheme. Then, the dishonest person cannot vote.*

Sketch of Proof. In the opposite direction, assume the dishonest person can vote. The administrator checks the list of voters who have the right to vote. So the dishonest person must create a valid pair of the ballot and the signature by himself. This contradicts that no one can break the ordinary digital signature scheme. □

Theorem 6 (Fairness). *The counting of ballots doesn't affect the voting.*

Sketch of Proof. The COUNTING stage is done after the VOTING stage, and the votes are hidden by using the bit-commitment scheme. So it is impossible that the counting of ballots affects the voting. □

Theorem 7 (Verifiability). *Assume that there is no voter who abstains from the voting and no one can forge the ordinary digital signature scheme. Then, even if the administrator and the counter conspire, they can not change the result of the voting.*

Sketch of Proof. It is clear that only disruption is for the counter not to list a valid ballot to the list. However, this disruption can be easily proved by showing

the valid pair of the ballot and the signature by the valid voter. So we only consider the disruption by the administrator in the following.

If there is no voter who abstains from the voting (i.e., he sends a ballot even if he abstains), there is no way for the administrator to dummy vote. So only valid voters can vote, and the result is trustable.

If the list overflows, every voter claims that he is an eligible voter and he was given a valid signature by the administrator. To claim it, the voter open the number r_i which he used in the blinding technique, and requires the administrator to show the voter's signature. By opening r_i, the message e_i is fixed, so the signature which the administrator must show is determined. If the administrator is honest, he can show the signatures for all requests. However, when he dummy voted, there remains the ballots which were not shown the signature because he cannot forge the digital signature scheme. The fraud is detected here. □

Remark. The following procedure is followed after the ADMINISTRATION stage if fraud by the administrator or counter is proved by one or more voters. First, the usual voting protocol is followed and disputed votes are omitted. If the number of omitted votes changes the result, the voting process is invalidated and is restarted. If the number of omitted votes fails to change the result, the voting process is accepted. In any case, the fraudulent party should be appropriately punished.

4 Conclusion

This paper proposed a practical secret voting scheme for large scale elections. The scheme ensures the privacy of the voters and prevents any disruption by voters or the administrator. Furthermore, voting fairness is ensured.

Acknowledgement

The authors would like to thank Choonsik Park for pointing out the illegal key problem. We would also like to thank Kazue Sako, Tsutomu Matsumoto, and Tomoyuki Asano for their valuable comments about the dishonesty of the administrator and the counter.

References

[AMI91] T. Asano, T. Matsumoto, and H. Imai, "A Study on Some Schemes for Fair Electronic Secret Voting" (in Japanese), The Proceedings of the 1991 Symposium on Cryptography and Information Security, SCIS91-12A (Feb., 1991).

[BGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation", Proceedings of the 20th Annual ACM Symposium on Theory of Computing, pp.1–10 (May, 1988).

[BY86] J. Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Votes", Proceedings of the 5th ACM Symposium on Principles of Distributed Computing, pp.52–62 (Aug., 1986).

[Ch81] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, Vol.24, No.2, pp.84–88 (Feb., 1981).

[Ch85] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete", *Communications of the ACM*, Vol.28, No.10, pp.1030–1044 (Oct., 1985).

[Ch88a] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", *Journal of Cryptology*, Vol.1, No.1, pp.65–75 (1988).

[Ch88b] D. Chaum, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", in *Advances in Cryptology — EUROCRYPT '88*, Lecture Notes in Computer Science 330, Springer-Verlag, Berlin, pp.177–182 (1988).

[CCD88] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty Unconditionally Secure Protocols", Proceedings of the 20th Annual ACM Symposium on Theory of Computing, pp.11–19 (May, 1988).

[CF85] J. Cohen and M. Fisher, "A Robust and Verifiable Cryptographically Secure Election Scheme", 26th Annual Symposium on Foundations of Computer Science, IEEE, pp.372–382 (Oct., 1985).

[CFN90] D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash", in *Advances in Cryptology — CRYPTO '88*, Lecture Notes in Computer Science 403, Springer-Verlag, Berlin, pp.319–327 (1990).

[DH76] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.644–654 (Nov., 1976).

[GMW87] O. Goldreich, S. Micali, and A. Wigderson, "How to Play Any Mental Game or a Completeness Theorem for Protocols with Honest Majority", Proceedings of the 19th Annual ACM Symposium on Theory of Computing, pp.218–229 (May, 1987).

[Iv91] K. R. Iversen, "A Cryptographic Scheme for Computerized General Elections", in *Advances in Cryptology — CRYPTO '91*, Lecture Notes in Computer Science 576, Springer-Verlag, Berlin, pp.405–419 (1992).

[Na90] M. Naor, "Bit Commitment Using Pseudo-Randomness", in *Advances in Cryptology — CRYPTO '89*, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp.128–136 (1990).

[Pf84] A. Pfitzmann, "A Switched/Broadcast ISDN to Decrease User Observability", 1984 International Zurich Seminar on Digital Communications, IEEE, pp.183–190 (Mar., 1984).

[Oh88] K. Ohta, "An Electrical Voting Scheme using a Single Administrator" (in Japanese), 1988 Spring National Convention Record, IEICE, A-294 (Mar., 1988).

[Sa92] K. Sako, "Electronic Voting System with Objection to the Center" (in Japanese), The Proceedings of the 1992 Symposium on Cryptography and Information Security, SCIS92-13C (Apr., 1992).