ELSEVIER

Computers & Security Vol. 15, No. 3, pp. 249–263, 1996

0167-4048/96 $15.00

S0167-4048(96)00006-5

refereed paper

A conventional approach to secret balloting in computer networks

Jing-Jang Hwang

Institute of Information Management, National Chiao Tung University,
Hsinchu, Taiwan 30050, ROC (jjhwang@cc.notu.edu.tw)

Cryptography has been applied to ballot voting in computer networks. Several proposals satisfy the objectives of privacy protection and sound security management. Social acceptance is another challenge to meet if this application is to be moved from theory to practice. In this paper cryptographic instruments are inserted into the conventional secret-voting procedure: preparing, distributing, casting, accumulating, and tabulating ballot papers. The conventional approach has a better chance of gaining social acceptance due to adequate social controls. Moreover, the scheme removes the assumption of existent anonymous-communication channels necessary for implementing several previous proposals, while using cryptographic instruments which are intelligible to usual voters and officials. Copyright © 1996 Elsevier Science Ltd.

Keywords: electronic voting protocol, group decision support systems, social acceptance, cryptography, ballot's confidentiality, digital signature, computer networks.

1. Introduction

Supporting group decisions has become a new area of computer applications. Since group decisions are usually accomplished through voting, organizations that frequently rely on voting to reach a consensus require a scheme for anonymous voting in computer networks. Such a scheme can be constructed in either Group Decision Support Systems (GDSS) [1] or Electronic Meeting Systems (EMS) [2], both of which are based upon computer communications. The scheme can also serve as a stand-alone utility in an information infrastructure within a company.

Contemporary cryptography has opened new visions for anonymous voting in computer networks. Previous investigators have proposed many secret-voting schemes (see Section 6.1 of [19]). Three common goals which most proposals have attempted to achieve include: (i) keeping the ballots confidential, (ii) preventing voters and officials from electoral misconduct, and (iii) warding off disruption. Fujioka *et al.* [4] refined the goals into seven clear objectives:

Completeness: all valid votes are counted correctly.

Soundness: the dishonest voter cannot disrupt the voting.

Privacy: all votes must be kept confidential.

Unreusability: no voter can vote twice.

Eligibility: no one who is not allowed to vote can vote.

Fairness: nothing must affect the voting.

Verifiability: no one can falsify the voting results.

Several protocols have been proven capable of theoretically satisfying the objectives; however, practical implementations remain rare. Recent democratic elections have utilized computing power to accelerate tabulation, but paper ballots remain the usual form. Using digital ballots to vote in computer networks will be the next step in evolving our democratic process through information technology. The question remains of how to move from theoretical protocols to actual practice.

Practitioners of information systems know that user acceptance is pivotal to successfully implement innovations. In this paper the term 'social acceptance' is used instead of 'user acceptance' because secret balloting is a societal activity. By adding social acceptance as another challenge to achieve, a new scheme is presented. The scheme also satisfies the goals of privacy protection and security management. To facilitate discussion, the seven objectives defined by Fujioka *et al.* [4] are reclassified into two categories: privacy protection and security management. Security management demands satisfying six of the seven objectives: completeness, soundness, unreusability, eligibility, fairness, and verifiability. The third goal of social acceptance, which is rather difficult to define in technical terms, involves the psychological status of a group's perception. The rest of this paper begins with the elaboration on the idea of social acceptance.

2. Social acceptance

Noticing the societal aspect of public elections in the UK, Slessenger [3] outlined two objectives for a socially secure election scheme: (i) assuring the voters that their votes have been accurately counted, and (ii) assuring the officials that they cannot be falsely accused of rigging the voting. Satisfying the two specific objectives not only demands a mechanism which allows a voter to check if his vote has been properly counted, but also another mechanism which allows an official to defend himself in case any doubt about his integrity arises.

Slessenger's two objectives for a socially-secure protocol are part of the requirements for social acceptance; however, eliciting social acceptance is far more challenging than designing a protocol which is secure. Social acceptance cannot rely entirely on purely technical measures. Non-technical measures such as social controls must be part of the solution. Such controls include organizational structures, segregation of duties, power-balanced assignments to official positions, detailed working steps for each position, and regulations over the officials' conduct. Controls over the integrity of computer codes are also essential, regardless of what cryptographic protocols are implemented.

Owing to adequate social controls, the conventional, non-computer, secret-voting scheme has been practiced worldwide. Many organizations often use paper ballots to conduct secret voting in order to ensure the credibility of group decisions. A typical procedure works as follows. The person presiding over a group decision process calls for voting when he wants a decision. Paper ballots are prepared. Each ballot contains a list of candidates or optional actions, such that a voter can make a choice simply with a mark or a circle. Each voter receives one ballot, goes to a curtained booth or where privacy is assured, marks or circles a decision on the paper, and then drops it in a collection box. Finally, representatives (appointed by the chair or elected by voters) supervise tabulation of the ballots in public. The process assures voters the confidentiality of their decisions since their votes are not counted individually but in aggregates. All parts, except the collection box and the booth, are disclosed. If the voting process prevents the box from deceptive manipulations and safeguards the booth as a private and safe place for every voter, the process assures voters that no fraudulent activities would occur. The officials can justify any of their actions if they perform their duties under public supervision. To curtail the leaking of partial results by officials, no ballot boxes are opened until they are all accumulated.

The question arises: 'Why do people accept the conventional procedure on trust?' Social acceptance lies in the social controls imposed on the conventional procedure.

Social control is indeed the basis of cryptography in many contexts. In this study we present not only a cryptographic protocol, but an organizational structure which allows adequate social controls to be imposed. We believe that the scheme can be implemented in organizations where corporate regulations make such controls work.

3. Literature review

Computer networks provide new environments for communication. Most human characteristics commonly found in face-to-face communications, e.g. body language and facial expressions, disappear in electronic messages. Networking computers alone, however, does not guarantee anonymity, since an electronic message may carry (explicitly or implicitly) information which reveals where the message originates. Chaum [5] proposed a solution in 1981. The solution allows messages to be received anonymously through a single intermediate 'mixer' or through a cascade or series of mixers, in which any honest mixer alone can force others to adhere to the rules. By using untraceable mail, the same paper continues to form rosters of digital pseudonyms, thereby functioning as a list gatherer of registered voters. Chaum [6] further proposed a voting scheme which also uses an anonymous-communication channel, but offers unconditional security against tracing any vote.

Whereas Chaum hid the identity of the voters, Benaloh (Cohen) *et al.* [7–9] used the high degree residue encryption technique to hide the contents of votes. Iversen [10] used the technique proposed to realize electronic money [11] to construct an election scheme. Iversen's scheme ensures independence between the voters in the sense that they do not have to be present at the same time or go through several phases together; as a result, it is applicable to 'voting by telephone'. Also designed for large-scale elections, the scheme of Fujioka *et al.* [4] requires the bit-commitment scheme [12], the ordinary digital signature scheme [13], and the blind signature scheme [14]. However, Fujioka *et al.*'s scheme returns to the assumption of existent anonymous-communication channels.

Other schemes have been proposed. Merritt's scheme [15] dispenses with the central tabulating authority but asks for several phases of secret-message passing between voters. Boyd [16,17] applied 'multiple key ciphers' to set up a scheme which also assumes voters can deliver their votes anonymously. Nurmi *et al.* [18] proposed another scheme which distributes an identification tag to each voter by using the ANDOS (All-or-Nothing Disclosure Of Secrets) protocol. ANDOS preserves the privacy of voters but is computationally demanding. In contrast, Slessenger [3] asserted, 'The use of cryptography in an election is in vain if a necessarily trusted third party is not trustworthy.' Alternatively, he presented a socially secure cryptographic election scheme which does not profess to keep votes confidential.

Several proposals have satisfied the seven objectives defined in the Introduction, at least theoretically acceptably. To be more acceptable in the real world, adequate social controls are indispensable to implemented systems. Most previous works focuses on the technical aspects, but implicitly assumes that necessary social controls are imposed when implemented. In this paper we contend that social control is equally as important as cryptographic instruments.

Furthermore, previous proposals either (i) use complicated mathematics to hide the contents of ballots, e.g. high-degree residue mathematical cryptography, or (ii) assume the existence of anonymous-communication channels. Complicated formulas would certainly not help social acceptance; we prefer technical simplicity. On the other hand, assuming anonymity of communications is unrealistic if secret balloting is to be conducted over open networks such as the Internet, in which the IP address would reveal where a message comes from. In proprietary networks, Chaum's mixers could hide the origin of each digital ballot, but the implementation of such anonymous-communication channels similarly demands adequate controls to guarantee that the codes are trustworthy. In this paper the assumption of existent anonymous channels is removed, while avoiding complicated mathematics.

4. Anonymous voting in organizations

An organization often conducts various types of group decisions: decisions involving people, strategic options, or times and methods to make decisions. Voting is not the only way to reach a group consensus, but is frequently adopted in institutions such as universities, nonprofit organizations, and companies with democratic traditions. Few characteristics distinguish this domain from civic elections. Firstly, organizations may call for voting much more frequently, whereas a government conducts an election for a civic office once every few years. The chair of a group meeting often calls for multiple sessions of voting in an hour—sessions to vote on what, when, who, how, or whether to vote. Any session of voting may go through a complete cycle: distribution of ballots, making individual decisions, casting votes, vote accumulation, and tabulation. Secondly, the number of voters participating in a group decision is much less than the number of citizens attending a civic election; the participants are, however, colleagues and are familiar with internal politics.

Effective management of cryptographic keys becomes crucial when an organization considers voting in computer networks to be a frequent organizational activity. To reduce the complexity of keys' management, the scheme must carefully classify keys according to cryptographic functions and develop different strategies correspondingly. As for internal politics, a voting scheme will not survive unless it balances the power over various interest subgroups; thus, distribution of responsibilities over various roles should be an essential part of the scheme. Furthermore, the scheme cannot function properly unless it is deemed acceptable by members of the organization; technical simplicity in cryptography would help to elicit acceptance.

5. Cryptographic instruments and terminology

Session keys

The scheme to be presented in the next section incorporates cryptographic instruments into a conventional, non-computer, procedure. Familiarity with some terminology is necessary. With respect to the subject of cryptography, Schneier's recent book *Applied Cryptography* [19] is an appropriate reference for customary terms such as one-way hash functions and the RSA (Rivest, Shamir, and Adleman) cryptographic system.

In particular, this work distinguishes cryptographic keys for a short period, referred to as session keys, from those durable for longer life cycles, referred to as durable keys. Users themselves generate session keys: no centralized control is necessary. In contrast, an authority certifies and disperses durable keys. Through separation of cryptographic functions, the scheme restricts session keys to the functions of encryption and decryption, and reserves durable keys for the functions of signature and verification. Session keys are proprietary, easily generated, and effective for only one session of voting. Durable keys are utilized to support reliable and accountable communications; their lives elapse throughout the entire course of a group decision process, and possibly over several sessions of voting. An organization desiring to adopt the scheme as a regular decision mechanism may authorize the keys' administration authority to certify durable keys for a long period (perhaps 1 year or longer) to reduce replacement cost.

Digital signatures

Analogous to the function of handwritten signatures on paper documents, digital signatures offer an instrument for authenticity verification and integrity control. A digital signature here is a bit string attached to an electronic document to convince the recipient that the signer has deliberately signed the document. Successful verification on a digital signature also ensures that contents of the document have not been altered.

The Digital Signature Standard DSS [20], recently adopted as an effective standard in the USA, and the well-known RSA [21] are two alternatives for implementing digital signatures. Both DSS and RSA run with a one-way hash function. Instead of signing a document, one signs the hash of the document. The one-way hash function for DSS is the Secure Hash Algorithm (SHA) [22], while RSA, not including such a function when invented, can adopt one of the later algorithms for message digests, e.g. MD5 [23] or SHA, as the associated one-way hash function. RSA, created for a broader application scope than DSS, is also capable of encryption and decryption, but if considered in this scheme, is restricted to signature and verification. This paper recalls the terms of 'encryption keys' and 'decryption keys' from RSA. For either selection of digital-signature implementations, the signature keys are also referred to as 'private keys', while the verification keys are interchangeable with the term 'public keys'.

Ballots, vote-tags, and votes

Digital ballots are ballots in a digital form used for computer processing and computer communication. As in previous literature, the adjective 'digital' is often omitted when there is no ambiguity. Each ballot contains names of candidates or options for available actions so that a voter can make a choice simply with a mark. The scheme also allows voters to enter their individual decisions, usually names not given in the candidates' list, in empty fields on the digital ballots. In contrast to handwriting on papers where the writers are usually recognizable, digitized information discloses nothing related to who fills in the information. Various forms of ballots are necessary for a variety of group decisions. Details on a ballot form, such as candidates' names and available options, may not be available until the group has reached certain agreements. The scheme utilizes a computer program to generate, in real time, ballots for various requirements when the chair announces a vote to be taken on the issue. Besides, the scheme utilizes another program to assist a voter to mark or fill in a decision on this voter's ballot. The former program is a tool for the chair or his assistant, while one copy of the latter should be distributed with a ballot to every voter. Both programs should be user friendly.

Different from paper ballots, a digital ballot in this proposed scheme also contains a data field named 'voter's self-verification code'. A voter may enter a large number into this field so that he can verify if his vote is accurately counted when the voting results are displayed.

Vote-tags, simply called tags, function as a second cryptographic instrument in the scheme. Being a digital identifier associated with a ballot, a tag contains two parts: (i) data for identification, and (ii) a digital signature signed upon the identification data. The identification data include, at least, a unique serial number and the time at which the voting is conducted, and, optionally, some descriptive items such as the descriptions of the issue to be voted upon and the title of the voting:

tag = (id-no. and time stamp, descriptive items,

authentic signature).

A tag is unique since the number included is unique. It is authentic if the digital signature proves to be valid. All tags for a single session of voting require a private key for generating signatures and a public key for verifying signatures. Generally, the chair, in charge of the group decision process, assumes responsibility for the signatures.

This section defines what a vote means in this context. A vote contains two parts: (i) a ballot and (ii) a tag:

vote = (ballot, tag).

Figure 1 illustrates an example of a vote.

Encryption key, decryption key, and certificate-for-decipherment

Digital signatures and tags cannot keep votes confidential. This is the exclusive and only function of the third cryptographic instrument: encryption and decryption. In this paper we classify all keys for encryption and decryption as session keys, and regulate their replacement for every session. The procedural steps in the next section provide further details.

Essentially, each voter should assume the responsibility for protecting his privacy, using a self-generated key to encrypt his ballot. Meanwhile, each voter sends a 'certificate-for-decipherment' to an official for later deciphering the ballot back to cleartext. A certificate-for-decipherment, or a certificate for short, combines a copy of a tag with the decryption key that belongs to the voter who obtained this tag. A certificate offers the authority to decipher an encrypted ballot.

There is, however, not much secrecy to protect. For instance, everyone can guess the content of a ballot with 0.2 probability of success if the vote is to elect one person from five candidates. More significantly, each key for encryption or decryption is only effective for a single session of voting. As a result, the two criteria, i.e. ease for keys' replacement and speed of processing, dominate the choice for the cipher. The simple XOR cipher could be a straightforward choice from a technical point of view. Voters could, however, reject XOR if they have prior knowledge that the cipher could not sustain the known-plaintext attacks. The attacks on XOR cipher could induce the candidate keys (ciphertext XOR known-plaintext = the key), actually out-of-date, from the limited possibilities of the voters' decisions so that voters would feel that their privacy has not been well protected. After all, the industrial standard DES (Data Encryption Standard) is a natural and safe choice. DES has some good attributes: fast processing speed, resistance to the known-plaintext attacks, and capability for self keys' generation (based on random-number generators). This selection is a single-key cipher: encryption and decryption use the same key.

6. The scheme

Officials who carry out the protocol

The scheme retains the official positions that the non-computer, paper-based protocol requires. Besides, it asks for one 'certificate collector' and one 'privacy mixer'. These positions and their responsibilities are described as follows:

Chair: the chair takes charge of the group decision process and sets the time schedule to proceed with the voting.

Registrar: the registrar maintains a register of the legitimate voters, which contains the voters' identification data and their public keys. The public keys of the officials, who may or may not be voters, are also contained in the register so that their signatures can be verified when necessary. Among the public keys, the chair's is necessary for verifying signatures contained in tags. A participant may use the same pair of private and public keys for both roles of a voter and of an official.

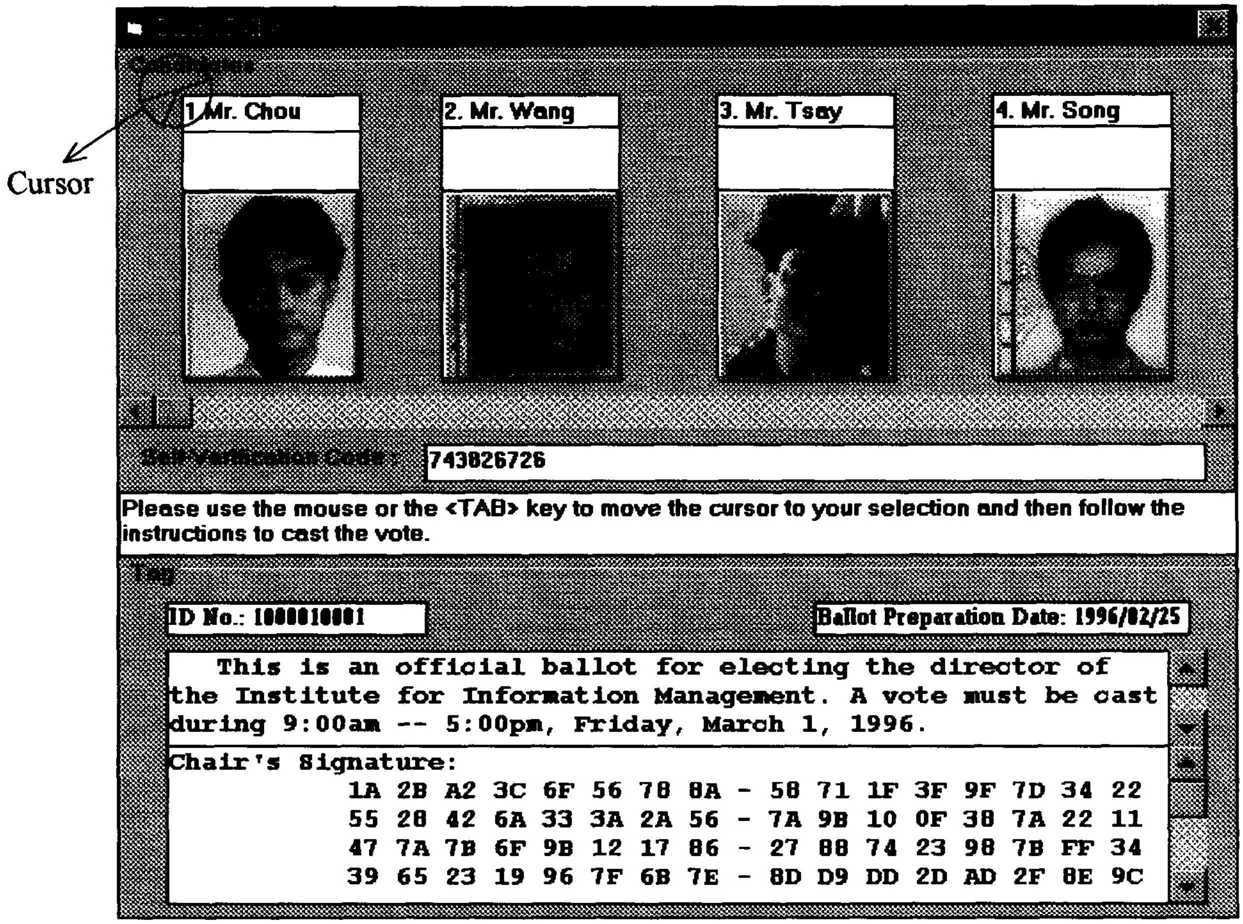
Distributor (optional): the distributor, on behalf of the chair, should pass out empty votes to participants. Each voter receives an empty vote that contains one ballot and one tag. The chair may distribute votes without the assistance of any distributor.

Vote Collector: this clerk accumulates all valid votes into a set.

Certificate Collector: this clerk accumulates certificates into a second set.

Privacy Mixer: this clerk runs a 'match/decipherment/detachment/shuffle program' to produce the cast ballots in plaintext, in aggregate, but with no tags.

Tally Clerk: by exactly mimicking the conventional



Self-Verification Code : 743826726

Please use the mouse or the <TAB> key to move the cursor to your selection and then follow the instructions to cast the vote.

ID No.: 1000010001

Ballot Preparation Date: 1996/02/25

```
   This is an official ballot for electing the director of
the Institute for Information Management. A vote must be cast
during 9:00am -- 5:00pm, Friday, March 1, 1996.
Chair's Signature:
              1A 2B A2 3C 6F 56 78 8A - 58 71 1F 3F 9F 7D 34 22
              55 28 42 6A 33 3A 2A 56 - 7A 9B 10 0F 38 7A 22 11
              47 7A 7B 6F 9B 12 17 86 - 27 88 74 23 98 7B FF 34
              39 65 23 19 96 7F 6B 7E - 8D D9 DD 2D AD 2F 8E 9C
```

Fig. 1. A digital vote on the screen.

tabulation process, the tally clerk runs a computer program to fully disclose the tally process on an electronic bulletin board.

An anonymous-voting process for a group decision begins with making appointments to the official positions. Among the appointments, the registrar can be a permanent position required for maintaining the registers of various group decisions. In addition, an organization can appoint an administrator to supervise generation, distribution, and replacement of durable keys, which are technically restrained by the chosen public-key cipher—DSS, RSA, or others. Durable keys are equally applicable to Electronic Data Interchange (EDI) or electronic commerce, since a digital signature often shows approval of a business transaction. Creating a role for administrating durable keys, we prefer a general-purpose position to a position exclusively for anonymous voting. The reason is to save cost. The administrator issues a private key to every person in the organization and opens the corresponding public key. Anyone is allowed not only to use the same pair of private and public keys for both roles of a voter and of an official, but also to extend the usage to EDI or other applications that also demand signatures.

Main ideas

This proposal utilizes session keys to keep votes confidential. Included in a certificate-for-decipherment, a DES key is generated by a voter and is used to encrypt the contents of his ballot. All encrypted ballots will not be deciphered until they are accumulated in a batch. Deciphering ballots in aggregate is similar to opening ballot boxes in conventional voting.

Assignments of officials to various roles have been described in the previous subsection. Each official performs his task by running a computer program that must have been publicly scrutinized. An official must run the program in public or be monitored by other appointees. In short, this proposal relies on the common-sense social controls to ensure that all programs are trustworthy.

The protocol makes use of the procedure—vote preparation, distribution, casting, accumulation, and tabulation—all of which are found in a typical non-computer system. Empty votes are prepared through the vote generation program, which is flexible enough to quickly prepare a set of empty votes for any group decision scenario. A voter obtains his vote, i.e. an empty ballot associated with a unique tag, through an authentication process. After marking and encrypting his decision, the voter cast his vote and his certificate (for decipherment) to the vote collector and the certificate collector, respectively. Every vote or certificate carries a tag as well as the voter's digital signature to its destination. Restated, voters cast their ballots with accountable mail, not through anonymous-communication channels.

The vote collector accumulates the valid votes into a set, while another collector accumulates the certificates into a second set. The collectors then send the sets to the privacy mixer. The privacy mixer uses the match/decipherment/detachment/shuffle program to execute a sequence of operations. The first operation matches each encrypted ballot with its certificate for decipherment, and the subsequent operations produce the ballots in aggregate and in cleartext. Final tallies follow and the process ends.

Procedural steps

(A) Before voting:

Step 1—register as voters, appoint officials. The registrar maintains a current voter register, including those members allowed to participate in this group decision. The officials are appointed. Moreover, the registrar makes sure that he has included in the register the officials' public keys.

Step 2—prepare votes. The chair, or the distributor on his behalf, prepares empty votes for all voters. Every vote, which contains one ballot and one tag, is a digital document. A computer program should accompany each vote so that a voter can easily mark or fill in a selection on the ballot.

Step 3—distribute votes. Each voter presents his identification to obtain one empty vote. (One voter can typically cast only one vote—however, the scheme can be easily modified to allow a voter to cast as many votes as permitted in some group decision scenarios.)

Many methods are available for user identification in computer networks. Checking passwords is fairly straightforward. Since public keys are available, the scheme can employ more secure methods such as the challenge-response or those using smart cards.

(B) Voting:

Step 4—make individual decisions. Each voter marks or fills in his selection on the ballot after validating the signature in the tag. Optionally, he may enter his chosen number as his 'voter's self-verification code'.

Step 5—generate DES keys and certificates. Each voter generates a DES key for the current session of voting, and then combines a copy of the DES key with a copy of his vote-tag to form a certificate-for-decipherment.

Step 6—cast votes and certificates. Each voter takes the following actions, in sequence, to cast a vote: encrypt the ballot, sign the vote (ballot and tag), attach his signature at the end of the vote, retain a copy, and send the vote (with the signature) to the vote collector. Each voter also takes a sequence of similar actions to send his certificate-for-decipherment to the other collector. At the beginning, the chair must announce a deadline for the actions regulated in this step.

Figure 2 illustrates the two documents that a voter sends to the designated collectors.

Step 7—acknowledge. Upon receiving a vote or a certificate, each of the two collectors returns a receipt with his signature to the voter. The chair must set a second deadline for any voter to claim the receipt(s). Upon accepting the claim, the chair provides the voter with a new vote and announces that the old tag is invalid.

(C) Accumulation:

Step 8—accumulate votes. The vote collector runs a computer program, referred to as the vote accumulation program, to validate the authenticity and uniqueness of every incoming vote. The program publishes the sender's signature when it determines that is inauthentic. It also publishes a duplicate or inauthentic vote when it finds that the tag is a copy or a forgery. The program then detaches the voter's signature from every vote and accumulates all valid votes into a set. The collector signs the set, attaches his signature at the end of the set, retains a copy, and sends it to the privacy mixer.

Step 9—accumulate certificates. In the same manner, the certificate collector accumulates the valid certificates into a set, displays the invalid certificates, and sends this second set together with his signature to the privacy mixer.

(D) After accumulation:

Step 10—match, decipher, detach, and shuffle. The privacy mixer runs the match/decipherment/detachment/shuffle program after validating the signatures received with the two sets. For every vote this program first matches it with a certificate that has an identical tag; second, decrypts its encrypted ballot; third, detaches the tag from itself. Upon completing the three operations for all votes, the program shuffles the remaining ballots and outputs the results in an aggregate form. The ballots are now in plaintext and in anonymity. A vote without a certificate is incomplete and must be excluded.

Figure 3 illustrates the inputs and outputs of the match/decipherment/detachment/shuffle program.

Step 11—tally ballots. Using the tabulation program, the tally clerk publicly tabulates the ballots on an electronic bulletin board. Finally, the chair announces the results.

The source codes of the programs are available from the author or from the National Science Council of his country. Figure 4 summarizes the documents flow of the scheme.

7. Privacy protection, security management, and social acceptance

Privacy protection

Segregation of duties contributes to privacy protection. None of the officials has complete information to discover the secrecy of any valid vote. The vote collector lacks the decryption key with which to decrypt an encrypted ballot; meanwhile, the certificate collector cannot access the cast votes at all. Lacking the voters' signatures, the privacy mixer cannot associate a tag with a voter as long as the distributor discloses no information related to who got which tag. Of course, the officials may impinge upon voters' privacy if they are able to share information.

To get rid of the opportunities for sharing information, establishing control over the information flow is necessary. The match/decipherment/detachment/shuffle program, which is most critical to privacy protection, must detach every tag in midway of processing and put off output of the deciphered ballots until they have been aggregated and shuffled, consequently, this program reveals no information related to individual votes. Similarly, the vote accumulation program must output the set of valid votes in aggregate and, at the same time, reveal no information about individuals. The certificate accumulation program must do the same for certificates. The denial to access

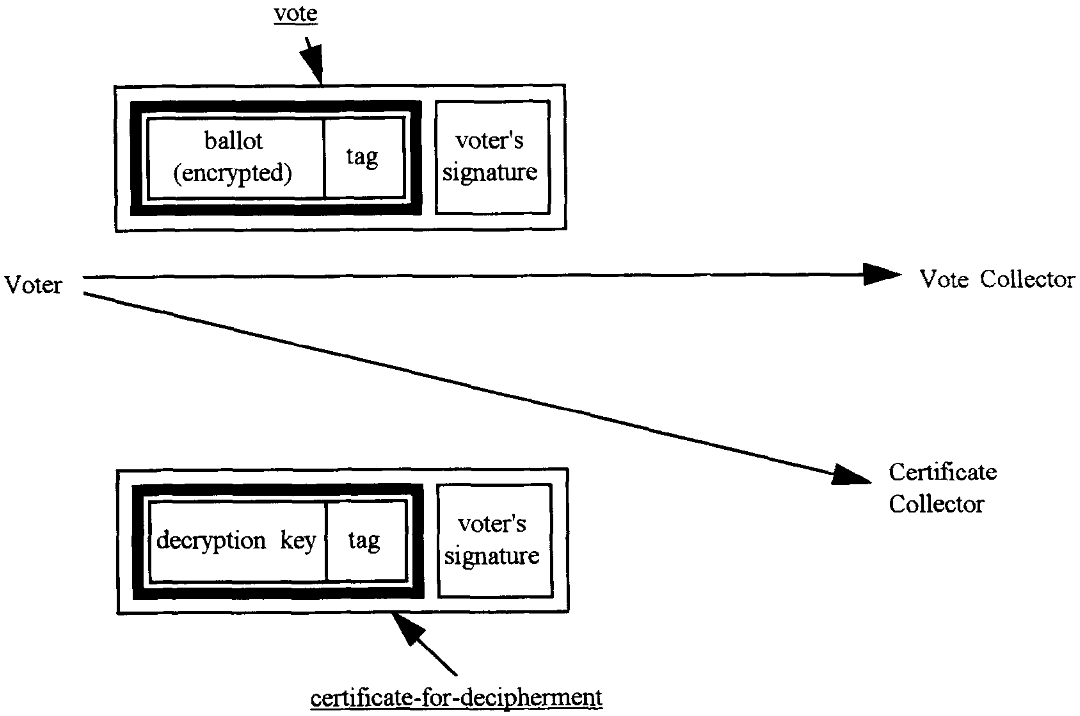


Fig. 2. Each voter sends two digital documents to the collectors.

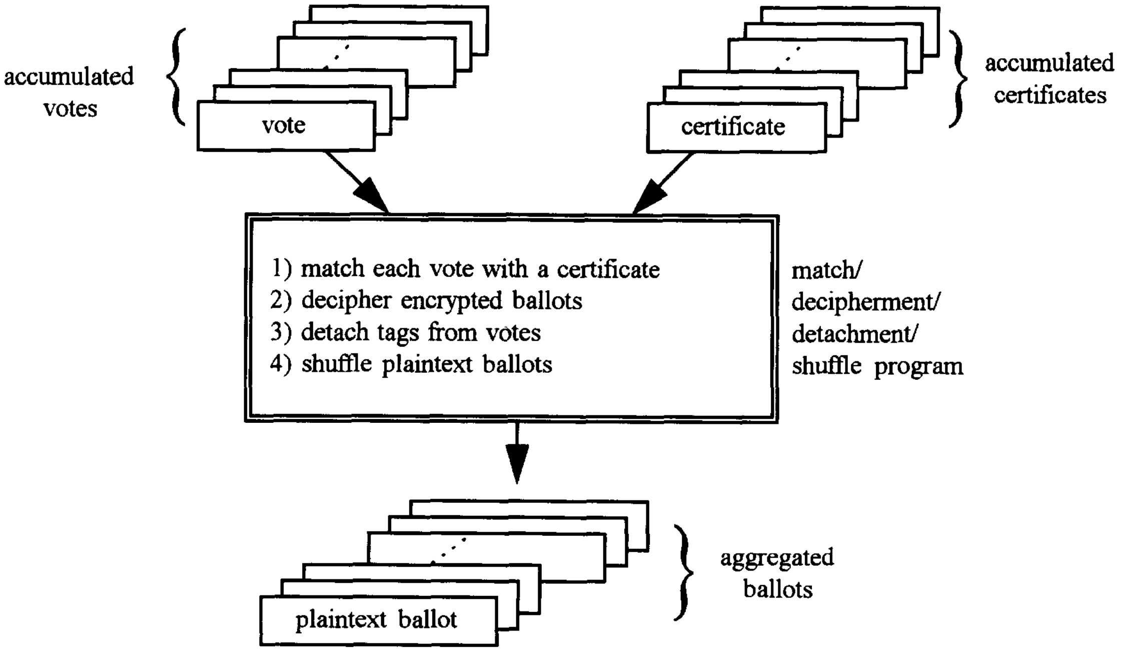

accumulated votes
vote
accumulated certificates
certificate
1) match each vote with a certificate
2) decipher encrypted ballots
3) detach tags from votes
4) shuffle plaintext ballots
match/ decipherment/ detachment/ shuffle program
plaintext ballot
aggregated ballots

Fig. 3. Functions of privacy mixing.

or display of an individual is analogous to that, in ballot-paper based voting, no one is permitted to peek at a ballot at the time the voter drops it into a collection box.

Another threat comes from illegally tapping the communication line to intercept votes and certificates. With intercepted certificates, interceptors can decrypt intercepted ballots. The threat, although less serious if the voting takes place in a building or a room for electronic meetings, can be easily unleashed with the well-known technique that the sender encrypts the sending document with the receiver's public key. The public key has been made available because the receiver is either a collector or the privacy mixer: no extra cryptographic keys are necessary.

Security management

The vote accumulation program classifies a vote as invalid if its tag is a forgery or a duplicate. Whether to count one vote for a set of duplicates is a relevant issue at the policy level. The program does not accumulate the invalid votes as it does the valid ones; it displays invalid votes together with their tags for public verification. Another policy issue is whether to display the signature that comes with an invalid vote since a voter may be dissuaded from voting if he is afraid of making a mistake and if his signature is to become public for the mistake. The program should, however, publish the inauthentic signatures, that could come from intruders. Equivalently, the certificate accumulation program also displays the invalid certificates and the inauthentic signatures.

The tags serve the scheme as an important instrument for security management. With the availability of the chair's public key, the uniqueness, integrity, and authenticity of a tag can be verified by all parties involved. Any honest appointee among the two collectors and the privacy maker should be able to detect any fraudulent vote. Without their full cooperation, a false vote would

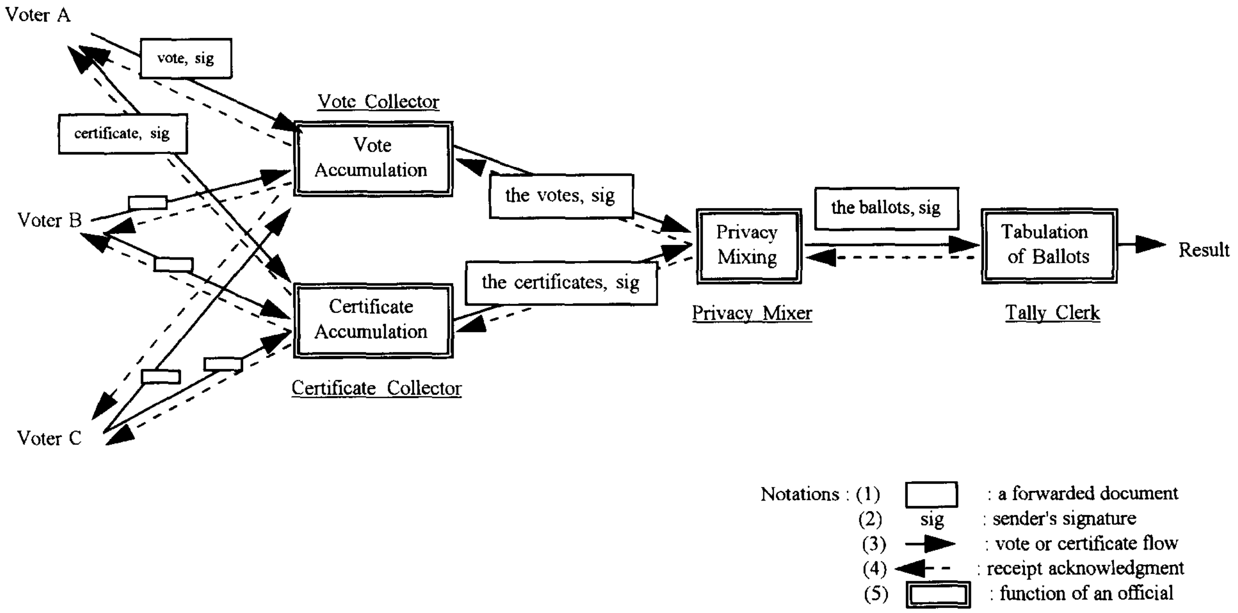


Fig. 4. Document flow.

have no opportunity of ending up in the aggregated ballots.

The signatures also help. The signer, either a voter or an official, must be responsible for the document he moved forward. In contrast to other cryptographic schemes that depend on untraceable mail to accomplish anonymous communications, all correspondence here is traceable and accountable. The scheme deters irresponsible messages, thereby preventing the process from being disrupted.

Some serious threats to security are parallel between the paper-based voting and this proposal. Manipulations over the ballots in the collection boxes are certainly the most crucial threat to the credibility of ballot-paper based voting. To avert such an attack, preventive measures include emptying the boxes before voting, safeguarding the boxes against illegal access, and publicly opening the boxes for final tallies. Similarly, the proposed scheme must enforce some measures to protect the three sets—(i) the valid votes, (ii) the certificates, and (iii) the aggregated ballots—from any illegal manipulation. Among the sets, the aggregated ballots are most vulnerable to attack, because they are not appended with tags and signatures. The match/decipherment/detachment/shuffle program must protect the aggregated ballots from cutting, pasting, and duplicating. To tightly control over the information flow, the scheme should allow nothing except the tally program to read individual names from the ballots. Protected with tags and encryption, the accumulated votes are less vulnerable to interference, yet the vote accumulation program may take a similar precaution to control information flow: grant the right to access individual votes to the subsequent program, the match/decipherment/detachment/shuffle program, and no others. Equally regulated is the certificate accumulation program. Lastly, the tally program should work as supposed. On an electronic bulletin board it displays the aggregated ballots in clear contents and shows the tabulations in detail.

Following the wisdom of the conventional paper balloting procedure, this scheme obviously satisfies the fairness objective since all ballots are opened (deciphered) at the same time. It also satisfies completeness and soundness, provided that the social controls ensure the integrity of the running programs—the two accumulation programs, the match/decipherment/detachment/shuffle program, and the tally program. A well-controlled register facility can guarantee the scheme satisfying the unreusability and eligibility objectives. Verifiability is achieved due to the adoption of the voter's self-verification code.

Social acceptance

Digital signatures are not indispensable as an instrument for security management because they duplicate the function of tags. They are, however, principal ingredients for accountability, a necessary condition for social acceptance. The signer of a document must be responsible for the document he moved forward. In case of a dispute, anyone can prove honesty by showing what he received and what he sent. Whoever is responsible for an error or a misconduct can be located. Therefore, any official can defend himself against any false accusations.

A scheme is socially acceptable if it is taken on trust. This scheme has several good qualities to inspire voters to place their trust in it. It resembles the traditional procedure with which people are most familiar. Familiarity provides users a motivation to participate in and to trust the voting process. Also, every official is regulated to perform a single program. Segregation of duties results in an organizational balance and, from that perspective, offers a certain degree of trust. Organizational flexibility is another good quality: more officials can be appointed to one position to run the designated program together, as required by internal politics or whatever related reasons. Voters can also serve as officials. Furthermore, this scheme makes use of cryptography in a very natural way so that most ciphers, for encryption and decryption or for signature and verification, can be adopted without modifications. The cryptographic instruments are intelligible to voters and officials, this also makes a contribution.

The degree of trust can be inspired further if every voter can see his vote actually being counted. Tags, signatures, or decryption keys, which all reveal clues to votes' or voters' identifications, are useless for this purpose for they have been removed before the final tallies. The voter's self-verification code serves this purpose. A voter can enter an identification number into this data field on his ballot. The number, different from the unique number in a tag, is chosen by the voter himself and should be sufficiently large to minimize duplicates. The number appears when the content in the ballot gets clear. Nurmi *et al.* [17], however, pointed out a drawback for such an option, "The incentives for selling and buying of votes become considerably stronger as the buyer can be sure that the seller also delivers the goods, i.e. votes as promised." Iversen also expressed the same concern at the end of his paper [10]. Even so, this option would help to elicit social acceptance in the context of supporting group decisions.

8. Conclusion

The scheme is societal: it resembles the conventional, non-computer, paper-based voting in basic procedures and organizational functioning. It is also robust because every computer message carries the sender's digital signature and is legally obligated. Accumulating the votes into an aggregate and tabulating them in public highlight the primary feature of this scheme, which is adopted from the conventional voting by ballot papers.

Many officials involved with this scheme can find their counterparts in the paper-based voting; the certificate collector and the privacy mixer are two new positions. This research has specified the computer programs to assist the officials to conduct their respective duties. Every computer program uses some of the cryptographic instruments—tags, signatures, encryption and decryption—to control the information flow. Among those programs, the match/decipherment/detachment/shuffle program, which substitutes the anonymous-communication channel necessary for implementing some previous proposals, is most critical to privacy protection and security management. This study has justified this substitution since no additional complicated cryptographic techniques have been introduced while removing the assumption of anonymous communications.

Social acceptance is the challenge to this type of cryptographic applications, as well as to this scheme. This scheme, however, offers a few good qualities to facilitate social acceptance—at least for supporting group decisions in organizations: resemblance to users' experience, segregation of duties, organizational flexibility, and technological simplicity. In a technical sense, the scheme also qualifies for civic elections; however, the legality of digital signature and formal regulations on social controls are necessary prior conditions for institutionalizing that application in the broader scope of civic affairs, at the city level or beyond.

Acknowledgements

The author would like to thank the referees for their thoughtful and helpful comments. He is indebted to his colleague Dr Chyan Yang and his old friends Drs Clinton H. Whitehurst and PeCheng Wang for many useful discussions. He also thanks his students, Mssrs Ching-Feng Lee, Chin-Jung Kuo, Shi-Min Ye, Yuh-Maw Tsay, Jong-Liang Nieh and Ms Min-Hui Lin for participating in computer programming and class discussion. This work has been partially supported by the National Science Council of the Republic of China under the Contract No. NSC-84-2213-E009-001.

References

[1] C.M. Jessup and D.A. Tansik, Decision-making in an automated environment—the effects of anonymity and proximity with a group decision support system, *Decision Sciences*, 21 (2) (1991) 266–279.

[2] J.F. Nunamaker, A.R. Dennis, J.S. Valaich, D.R. Vogel and J.F. George, Electronic meeting systems to support group work, *Communications of the ACM*, 34 (7) (1991) 40–61.

[3] P.H. Slessenger, Socially secure cryptographic election scheme, *Electronics Letters*, 27 (11) (1991) 955–957.

[4] A. Fujioka, T. Okamoto and K. Ohta, A practical secret voting scheme for large scale elections, in *Advances in Cryptology—CRYPTO'93*, pp. 244–251, Springer, Berlin, 1993.

[5] D.L. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 24 (2) (1981) 84–88.

[6] D.L. Chaum, Elections with unconditionally secret ballots and disruptions equivalent to breaking RSA, in *Advances in Cryptology—Eurocrypt'88 Proceedings*, pp. 177–182, Springer, Berlin, 1988.

[7] J.D. Cohen and M.H. Fisher, A robust and verifiable cryptographically secure election scheme, *Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science*, pp. 372–382, 1985.

[8] J. Benaloh and M. Yung, Distributing the power of the government to enhance the privacy of votes, *Proceedings of the 5th ACM Symposium on Principles of Distributed Computing*, pp. 52–62, Aug. 1986.

[9] J. Benaloh, Verifiable secret-ballot elections, Ph.D. dissertation, YALEU/DCS/TR-561, Yale University, CT, Sep. 1987.

[10] K.R. Iversen, A cryptographic scheme for computerized general elections, in *Advances in Cryptography—CRYPTO'91*, pp. 405–419, Springer, Berlin, 1992.

[11] D. Chaum, A. Fiat, and M. Naor, Untraceable electronic cash, in *Advances in Cryptology—CRYPTO'88*, pp. 319–327, Springer, Berlin, 1990.

[12] M. Naor, Bit commitment using pseudo-randomness, in *Advances in Cryptology—CRYPTO'89*, pp. 128–136, Springer, Berlin, 1990.

[13] W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, IT-22 (6) (1976) 644–654.

[14] D. Chaum, Security without identification: transaction systems to make big brother obsolete, *Communications of the ACM*, 28 (10) (1985) 1030–1044.

[15] M. Merritt, Cryptographic protocols, Ph.D. dissertation, GIT-ICS-83/6, Georgia Institute of Technology, GA, Feb. 1983.

[16] C. Boyd, Some applications of multiple key ciphers, in *Advances in Cryptology—Eurocrypt'88 Proceedings*, pp. 455–467, Springer, Berlin, 1988.

[17] C. Boyd, A new multiple key cipher and an improved voting scheme, in *Advances in Cryptology—Eurocrypt'89 Proceedings*, pp. 617–625, Springer, Berlin, 1990.

[18] H. Nurmi, A. Salomaa and L. Santean, Secret ballot elections in computer networks, *Computers & Security*, 10 (6) (1991) 553–560.