1998 International Computer Symposium
Workshop on Cryptology and Information Security
December 17-19, 1998, N.C.K.U., Tainan, Taiwan, R.O.C.

AN EFFICIENT ELECTION SCHEME FOR RESOLVING TIES

Chun-I Fan*, Chin-Laung Lei**, and Chih-Yuh Chang**

*Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
12, Lane 551, Min-Tsu Road Sec. 3
Yang-Mei, Taoyuan, Taiwan 326, R.O.C.
Email: fan@fractal.ee.ntu.edu.tw

**Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
Email: lei@cc.ee.ntu.edu.tw

ABSTRACT

In many daily election activities, it is quite often that we have to perform the voting process more than once to resolve ties, such as several candidate professors may receive the same highest votes when electing the chairman of a department, or several candidate players may tie for the last available position of a national basketball team elected by a group of coaches. With typical electronic election schemes in the literatures, it is necessary to hold the election again to deal with the above situations. In this paper we propose an efficient election scheme to cope with the problem. In the proposed scheme, every voter can obtain an intention attachable vote which contains all possible intentions of the voter, and he just needs to attach his new intention to his previous vote when an extra round of voting is required. Comparing with several possible solutions of the re-voting problem, the proposed protocol does not need an extra digital signature scheme for a voter, and it requires only one round of registration action and O(1) storage for every voter.

1 INTRODUCTION

Due to the fast progress of networking technologies, many advanced network services have been proposed in the literatures. Among these services, electronic voting is a popular one, since this service makes it possible for every voter in a remote site to submit his vote through electronic communication networks [1, 2, 7, 8, 13, 15, 16, 18, 27, 28, 29, 32].

Typically, an electronic election scheme consists of two types of participants, a tally center and a group of voters. Every voter registers with the tally center, and requests a vote with his own individual intention from the center. The voters cast their votes by anonymously sending them to the center at a proper time. Finally, the center computes and publishes the result of the election.

Especially, in many daily election activities, it is quite often that we have to perform the voting process more than once to resolve ties, such as several candidate professors may receive the same highest votes when electing the chairman of a department, or several candidate players may tie for the last available position of a national basketball team elected by a group of coaches. Hence, it is required to develop a robust election scheme to cope with the above re-voting problem. With typical electronic election schemes proposed in the literatures [1, 2, 7, 8, 13, 15, 16, 18, 27, 28, 29, 32], it is necessary to hold the election again to deal with the above situations. In this paper we introduce an efficient election scheme to solve the problem. The proposed scheme makes it possible for every voter to anonymously attach his intention of an extra round of voting process to his previous vote without an extra registration action. This is referred to as the *intention attachability* property. In the proposed election scheme, the voter's intention of an extra round of voting action is not required to be determined until it is really necessary, and anyone else cannot modify the voter's intention in his vote. In addition, the privacy of every voter is protected against any others in the proposed scheme. Comparing with several possible so-

lutions of the re-voting problem, the proposed protocol does not need an extra digital signature scheme for a voter, and it requires only one round of registration action and O(1) storage for every voter.

The rest of the paper is organized as follows. We present a generic blind signature scheme in section 2. Based on the generic blind signature scheme, we propose an efficient election scheme to resolve ties in section 3. Finally, we make a conclusion of this paper in section 4.

2 A GENERIC BLIND SIGNATURE SCHEME

The proposed election scheme is based on the techniques of blind signatures [3, 5, 11, 12, 22, 23]. Blind signatures are developed to prevent digital signatures from being forged and to protect the privacy of users [5]. Due to the unlinkability property [3, 5, 11, 12, 22, 23], blind signatures are usually applied to construct anonymous electronic election schemes [2, 7, 13, 15, 18, 32].

Two kinds of roles, a signer and a group of users, participate in a blind signature protocol. A user blinds a message by performing an encryption-like process (or a blinding process) on the message, and then submits the blinded message to the signer to request the signer's signature of the message. The signer signs the blinded message by using its signing function, and then sends the signing result back to the user. Finally, the user unblinds the signing result to obtain the signer's signature of the message by performing a decryption-like operation (or an unblinding operation) on the signing result he receives. The signer's signature of the message can be verified by checking if the corresponding public verification formula with the signature-message pair as parameters is true.

In a secure blind signature scheme, it must be computationally infeasible for the signer to derive the link between a signature and the instance of the signing protocol which produces that signature. This is the unlinkability property [3, 5, 12, 22, 23]. With the help of unforgability and unlinkability properties, the technique makes it possible to prevent an authorized document from being forged and to protect the privacy of the document's owner.

Let M be the underlying set of messages, and R be a finite set of random integers. Formally, a blind signature scheme X consists of four elements (B_X, S_X, U_X, V_X), where

(1). $S_X : M \to M^K$ is the signing function which is kept secret by the signer where K is a positive integer, $M^K = M^{K-1} \times M$ when $K \geq 2$, and $M^K = M$ when $K = 1$. Given a message $m \in M$, it is infeasible to compute $S_X(m)$ except the signer.

(2). $V_X : S_X(M) \times M \to$ {true, false} is the verification formula which is public. For every valid signature-message pair $(S_X(m), m)$, the formula $V_X(S_X(m), m)$ is true.

(3). $B_X : M \times R \to M$ is the blinding function of X. For every $m \in M$ and $r \in R$, it is infeasible for the signer to compute m from $B_X(m, r)$. The integer r is called the blinding factor of m.

(4). $U_X : S_X(M) \times R \to S_X(M)$ is the unblinding function of X. For every $m \in M$ and $r \in R$, we have that $U_X(S_X(B_X(m, r)), r) = S_X(m)$, and it is computationally infeasible for the signer to derive $S_X(m)$ from $S_X(B_X(m, r))$.

The details of the blind signature protocol are described as follows.

(1) Blinding: A user chooses a message $m \in M$ and selects a blinding factor $r \in R$. The user computes $B_X(m, r)$ which is said to be a blinded message of m. To request the signer's signature of m, the user submits $B_X(m, r)$ to the signer.

(2) Signing: After receiving $B_X(m, r)$, the signer applies the signing function S_X to $B_X(m, r)$, and then sends the signing result $S_X(B_X(m, r))$ to the user.

(3) Unblinding: After receiving $S_X(B_X(m, r))$, the user performs the unblinding operation $U_X(S_X(B_X(m, r)), r) = S_X(m)$. Thus, he obtains the signature-message pair $(S_X(m), m)$.

(4) Verifying: The pair $(S_X(m), m)$ can be verified by checking whether the public verification formula $V_X(S_X(m), m)$ is true or not.

In a secure blind signature scheme, given the signature-message pair $(S_X(m), m)$ produced by the protocol, the signer cannot link $(S_X(m), m)$ to $(S_X(B_X(m, r)), B_X(m, r))$ since it is infeasible for the signer to compute m from $B_X(m, r)$ and to perform the unblinding operation to convert $S_X(B_X(m, r))$ into $S_X(m)$. In the literatures, several blind signature schemes have been proposed to realize these goals [3, 5, 11, 12, 22, 23]. Besides, to avoid the possible

multiplicative attacks which produce an illegal signature by multiplying two or more valid signatures, we can let the message m contain appropriate redundancy or apply a one-way hash function to m in advance.

3 AN EFFICIENT ELECTION SCHEME FOR RESOLVING TIES

In a typical electronic election scheme, there are two kinds of participants, a center and a group of voters. Basically, an electronic election protocol consists of three stages : (1) initialization, (2) registration, and (3) voting. In the initialization stage, the center publishes the necessary information such as the subject of this election, the list of candidates of the election, and the public keys of the center. In the registration stage, every identified voter obtains a vote with his own individual intention in a blinded version from the center. In the voting stage, a voter unblinds his blinded vote and sends the vote to the center, and then the center verifies and tallies all the votes received from the voters.

We define the re-voting problem in an electronic election as follows: How to deal with the situation where an extra round of voting process has to be performed to resolve ties? There are four possible solutions to cope with the re-voting problem.

Solution 1: Perform another round of registration and voting processes to resolve ties. This solution requires an extra round of registration action between every voter and the center. The overheads of the solution are heavy since a registration action includes voter identification and vote requesting for every voter.

Solution 2: By the multi-recastable election protocol [10], every voter requests n recastable tickets from the center to form a recastable vote of the voter since every recastable ticket has only two values "yes" and "no" where n is the amount of the candidates in the election. A recastable ticket can be reused more than one times, so that this solution can cope with the re-voting problem. Although this solution needs only one round of registration action, every voter requires $O(n)$ storage to record these n recastable tickets, and every cast vote is also of size $O(n)$. Moreover, another mechanism must be added to the scheme to guarantee that only one ticket among the n ones in a cast vote is "yes" value.

Solution 3: Every voter randomly chooses the public and secret keys of a digital signature scheme, and let his vote contain the public key and his intention of the election. Hence, if an extra voting action is required, the voter can use the digital signature scheme with his chosen secret key to sign his intention of the extra round of voting, and then submits the signing result to the center. The signing result can be verified through the public key shown in the previous vote of the voter. Clearly, an extra digital signature scheme is needed for every voter in the solution. In addition, almost digital signature schemes proposed in the literatures require modular exponentiation or inverse computations, which are time-consuming [14, 17, 19, 25, 26, 31, 33].

Solution 4: Based on the generic blind signature scheme of section 2, we propose an efficient election protocol to cope with the re-voting problem. Especially, the proposed scheme requires only one round of registration action and O(1) storage for every voter. Furthermore, our scheme does not need an extra digital signature scheme for a voter. The details of the proposed election scheme are described below.

The proposed election protocol is based on the blind signature scheme of section 2 where the center and the voters of the election scheme are regarded as the signer and the users of the blind signature protocol of section 2, respectively. The proposed election protocol consists of four stages, initialization, registration, voting, and re-voting, shown as follows.

(1) **Initialization:** The center publishes the necessary information of this election, such as the subject of the election, the list of candidates, and the public keys of the center. Let n be the amount of candidates, and these candidates are numbered from 1 to n. G and H are two public one-way hash functions [9, 24, 31]. Let $G^i(u) = G(G^{i-1}(u))$ and $H^i(v) = H(H^{i-1}(v))$ for every inputs u and v where i is a positive integer, $G^0(u) = u$, and $H^0(v) = v$. Define $u_i = G^{n-i}(u)$ and $v_i = H^{n-i}(v)$ for every $i \in \{1, 2, ..., n\}$.

(2) **Registration:** A voter chooses a message $m \in M$ with his own intention of the election. Then the voter selects a blinding factor $r \in R$ and randomly chooses u and v. He computes and submits $B_X((m||\alpha), r)$ to the center where $\alpha =$

Table 1: Comparisons among the four solutions of the re-voting problem

	Solution 1	Solution 2	Solution 3	Our Solution
No Extra Registration Action	No	Yes	Yes	Yes
O(1) Storage for a Vote	Yes	No	Yes	Yes
No Extra Signature Scheme	Yes	Yes	No	Yes

$(G^n(u)||H^n(v))$ and $||$ is the string concatenation operator. After receiving $B_X((m||\alpha),r)$, the center applies the signing function S_X to $B_X((m||\alpha),r)$, and then sends the signing result $S_X(B_X((m||\alpha),r))$ to the voter.

(3) **Voting:** After receiving $S_X(B_X((m||\alpha),r))$, the voter performs the unblinding operation $U_X(S_X(B_X((m||\alpha),r)),r) = S_X(m||\alpha)$, and submits his vote $(S_X(m||\alpha),(m||\alpha))$ to the center through an anonymous channel [4, 6] in the voting stage. The center verifies the vote by checking if the public verification formula $V_X(S_X(m||\alpha),(m||\alpha))$ is true, and then the center publishes the vote. In addition, the center publishes all the other votes it receives, and then computes and publishes the result of the election. We assume that every registered voter must submit his vote to the center in this voting stage.

(4) **Re-Voting:** If an extra voting process is required to resolve ties, every voter just needs to perform another voting action without an extra round of registration action. First, every voter determines his intention $t \in \{1,2,...,n\}$ for the re-voting stage. Then the voter computes $u_t = G^{n-t}(u)$ and $v_{n-t} = H^t(v)$, and sends his vote $(S_X(m||\alpha),(m||\alpha),t,u_t,v_{n-t})$ to the center through an anonymous channel [4, 6]. After receiving the vote, the center verifies the vote by checking if

$$\begin{cases} V_X(S_X(m||\alpha),(m||\alpha)) = \text{true, and} \\ \alpha = G^t(u_t)||H^{n-t}(v_{n-t}). \end{cases}$$

In the re-voting stage, if the voter submits two votes $(S_X(m||\alpha),(m||\alpha),t,u_t,v_{n-t})$ and $(S_X(m||\alpha),(m||\alpha),t',u_{t'},v_{n-t'})$ with $t \neq t'$ to the center, the center can find them out through the common parameter α, and these two votes are considered to be invalid. Finally, the center publishes all the votes it receives, and then computes and publishes the result of the re-voting stage. In most cases, an extra voting stage is enough to resolve ties. However, by applying the same method, the protocol can be modified to contain more than two voting stages.

Note that a simple variant of the proposed scheme can completely preserve the unlinkability property. Let every voter request two independent tuples $(S_X(m),m)$ and $(S_X(\alpha),\alpha,t,u_t,v_{n-t})$, instead of the combined one $(S_X(m||\alpha),(m||\alpha),t,u_t,v_{n-t})$ of the above protocol, from the center. The tuple $(S_X(m),m)$ is cast as a vote of the first voting stage, and the tuple $(S_X(\alpha),\alpha,t,u_t,v_{n-t})$ is cast as a vote of the re-voting stage if necessary. Since $(S_X(m),m)$ and $(S_X(\alpha),\alpha,t,u_t,v_{n-t})$ are independent, the variant version of the proposed protocol does not affect the unlinkability property.

In the proposed protocol, once t is determined by a voter in the re-voting stage, it is computationally infeasible for anyone else to modify t into another $t' \in \{1,2,...,n\}$ because that G and H are one-way.

In the proposed scheme, a voter has to perform $2n$ extra hashing computations to obtain an intention attachable vote. However, the integer n is usually small, say $n < 50$ or even $n < 10$, in a practical implementation, and hashing computations are efficient [31], so that these extra hashing computations do not reduce the efficiency of the scheme.

Through only one round of registration action and O(1) storage for every voter, the proposed election protocol can efficiently solve the re-voting problem without an extra digital signature scheme for a voter. Finally, the comparisons among the four solutions of the re-voting problem are summarized in table 1.

4 CONCLUSIONS

In this paper we have proposed an efficient election scheme to resolve ties. The scheme realizes that every user can anonymously attach his desired intention to his previous vote when an extra round of voting process is needed, and the attached information cannot be modified by any others. In addition, the proposed election protocol efficiently copes with the re-voting problem through few hashing computations.

REFERENCES

[1] J. Borrell and J. Rifa, "An implementable secure voting scheme," *Computers & Security*, vol. 15, no. 4, 1996, pp. 327-338.

[2] C. A. Boyd, "A new multiple key ciphers and an improved voting scheme," *Advances in Cryptology-EUROCRYPT'89*, LNCS 434, Springer-Verlag, 1990, pp. 617-625.

[3] J. L. Camenisch, J. M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," *Advances in Cryptology-EUROCRYPT'94*, LNCS 950, Springer-Verlag, 1995, pp. 428-432.

[4] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, 1981, pp. 84-88.

[5] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology-CRYPTO'82*, Springer-Verlag, 1983, pp. 199-203.

[6] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, 1988, pp. 65-75.

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

[8] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yumg, "Multi-authority secret-ballot elections with linear work," *Advances in Cryptology-EUROCRYPT'96*, Springer-Verlag, 1996, pp. 72-83.

[9] A. Evans, W. Jr. Kantrowitz, and E. Weiss, "A user authentication scheme not requiring secrecy in the computer," *Communications of the ACM*, vol. 17, no. 8, 1974, pp. 437-442.

[10] C. I. Fan and C. L. Lei, "A multi-recastable ticket scheme for electronic elections," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, Springer-Verlag, pp. 116-124, 1996. (A complete version appears in *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E81-A, no. 5, 1998, pp. 940-949.)

[11] C. I. Fan and C. L. Lei, "User efficient blind signatures," *Electronics Letters*, vol. 34, no. 6, 1998, pp. 544-546.

[12] N. Ferguson, "Single term off-line coins," *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, Springer-Verlag, 1994, pp. 318-328.

[13] A. Fujioka, T. Okamoto, and K.Ohta, "A practical secret voting scheme for large scale elections," *Advances in Cryptology-AUSCRYPT'92*, LNCS 718, Springer-Verlag, 1992, pp. 244-251.

[14] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, 1985, pp. 469-472.

[15] K. R. Iversen, "A cryptographic scheme for computerized general elections," *Advances in Cryptology-CRYPTO'91*, LNCS 576, Springer-Verlag, 1991, pp. 405-419.

[16] M. Michels and P. Horster, "Some remarks on a receipt-free and universally verifiable mix-type voting scheme," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, Springer-Verlag, 1996, pp. 125-132.

[17] NIST FIPS PUB XX, Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 1993.

[18] H. Nurmi, A. Salomaa, and L. Santean, "Secret ballot elections in computer networks," *Computers & Security*, vol. 10, 1991, pp. 553-560.

[19] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery schemes," *The first ACM Conference on Computer and Communications Security*, 1994, Fairfax, Virginia.

[20] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," *Advances in Cryptology-CRYPTO'92*, Springer-Verlag, LNCS 740, 1992, pp. 31-53.

[21] S. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, vol. 24, 1978, pp. 106-110.

[22] D. Pointcheval and J. Stern, "Provably secure blind signature schemes," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, Springer-Verlag, 1996, pp. 252-265.

[23] D. Pointcheval and J. Stern, "New blind signatures equivalent to factorization," *Proceedings of the 4th ACM Conference on Computer and Communication Security*, 1997, pp. 92-99.

[24] G. P. Purdy, "A high security log-in procedure," *Communications of the ACM*, vol. 17, no. 8, 1974, pp. 442-445.

[25] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. Jan. 1979.

[26] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120-126.

[27] K. Sako, "Electronic voting schemes allowing open objection to the tally," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E77-A, no. 1, 1994, pp. 24-30.

[28] K. Sako and J. Kilian, "Secure voting using partially compatible homomorphisms," *Advances in Cryptology- CRYPTO'94*, LNCS 839, Springer-Verlag, 1994, pp. 411-424.

[29] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme," *Advances in Cryptology-EUROCRYPT'95*, Springer-Verlag, 1995, pp. 393-403.

[30] C. P. Schnorr, "Efficient identification and signatures for smart cards," *Advances in Cryptology-CRYPTO'89*, Springer-Verlag, LNCS 435, 1990, pp. 235-251.

[31] G. J. Simmons, Contemporary Cryptology: The Science of Information Integrity, IEEE Press, N.Y., 1992.

[32] P. H. Slessenger, "Socially secure cryptographic election scheme," *Electronics Letters*, vol. 27, no. 11, 1991, pp. 955-957.

[33] H. C. Williams, "A modification of the RSA public-key encryption procedure," IEEE Transactions on Information Theory, vol. 26, no. 6, 1980, pp. 726-729.