Uncoercible Anonymous Electronic Voting*†

Chun-I Fan and Wei-Zhe Sun

Department of Computer Science and Engineering
National Sun Yat-sen University
70, Lien-Hai Road, Kaohsiung 804, Taiwan
TEL: +886-7-5252000 ext. 4346
FAX: +886-7-5254301
E-mail: cifan@cse.nsysu.edu.tw

Abstract

Due to convenience and efficiency, electronic voting (e-voting) techniques gradually replace traditional paper-based voting activities in some developed countries. A secure anonymous e-voting system has to satisfy many properties, such as completeness, tally correctness, and uncoercibility, where the uncoercibility property is the most difficult one to be achieved. Since each voter can obtain a voting receipt in an electronic voting system, coercibility and bribe (vote-buying and vote-selling are included) become more and more serious in electronic voting environments than traditional paper-based voting environments. Unfortunately, most of the solutions, like *receipt-freeness* or *untappable channels*, proposed in the literature, are impractical owing to lack of efficiency or too complicated to be implemented. It will make uncoercible e-voting systems unacceptable by the people. In order to cope with the drawbacks of the previous schemes, this paper will present a generic idea, which is independent of the underlying cryptographic components, on electronic voting to achieve the uncoercibility property and other requirements. The proposed method is an efficient and quite practical solution to match the current environments of electronic voting.

Keywords: Uncoercibility, Receipt-freeness, Blind signatures, Anonymous channels, Security and privacy, Cryptography

1. Introduction and Basic Ideas

Owing to the fast progress of computer and communication technologies, many advanced services have been developed to take the advantages of the techniques. Among these services, electronic voting is a popular one since every voter can finish her/his voting process securely and rapidly. However, coercibility and bribe are always serious problems and hard to be overcome in e-voting systems. In this paper we will propose a practical e-voting scheme. Not only can it achieve the uncoercibility property, but also it can satisfy other essential requirements, such as anonymity and tally correctness.

1.1. The Idea of Dual Randomization

In most electronic voting protocols [5][6][7][8][9][10][11][12], each voter must randomly choose a string and attach the string to her/his own ballot to guarantee that all ballots are distinct one for the requirements of the unrecastability property. Unfortunately, it may become a threat against the uncoercibility property. Coercers or bribers can enforce the voter to follow their will to choose an intention and a string they assigned and then attach them to her/his ballot, where the string will form the random part of the ballot. After the ballot is published, the coercers or bribers can identify this vote according to the string they assigned previously and check whether the intention of the vote is identical to their will. Thus, the coercion is successful.

To cope with the problem, the idea of dual randomization will be applied to our voting protocol. In an electronic voting protocol with dual randomization, every voter randomly chooses a string and combines it with another string randomly selected by the center where the two strings are mixed and integrated into the random part of the voter's ballot. Not only can the idea make all ballots distinct one another, but also it can prevent the coercers or vote-

* This research was partially supported by the National Science Council of the ROC (Taiwan) under grant NSC 94-2219-E-110-001.

† This work was also supported in part by TWISC@NCKU under grant NSC 94-3114-P-006-001-Y.

buyers from linking some designated ballots to their assigned strings because that they cannot control the final values of the random parts in the ballots.

1.2. The Idea of Multiple Receipts

Basically, if a voter intends to ensure whether her/his ballot is counted in the result of an electronic voting, she/he must keep a verifiable token as a voting receipt and then examines whether the published voting result contains her/his ballot via the receipt. Obviously, in this case, vote-buyers or coercers can request or enforce a voter to show her/his voting receipt and a vote-seller can also present her/his own receipt to anyone, such that these illegal parties can link the receipt to the published ballot of the enforced voter or vote-seller. In other words, the coercibility and bribe can be achieved easily.

In order to deal with the above situation, the idea of receipt-freeness had been presented for the first time in the literature [1], where every voter can be convinced of the correctness of the voting result without keeping any voting receipt. Nevertheless, we have pointed out the drawbacks, such as heavy computation cost and impractical assumptions, in receipt-free voting mechanisms. Instead of receipt-freeness, we come up with an especial idea "*multi-receipts*" as an efficient and practical solution that can greatly eliminate the possibility of the coercibility or bribe resulting from single receipt. In our voting protocol, after casting a ballot, the voter obtains not only her/his own receipt but the receipts of some voters as well. Note that the anonymity and privacy of every voter is still preserved. Although the voter can show a receipt to others, they cannot be convinced that the receipt indeed belongs to her/him.

1.3. Generic Blind Signature Scheme with Dual Randomization

A typical blind signature scheme contains two kinds of participants, a signer and a group of users who request the signatures from the signer. The basic steps are described as follows: a user requests a signature from the signer and the signer computes and issues a blind signature to the user. There are two sets of messages known to the signer: (1) the signing results computed by the signer and (2) the signatures shown by the users for verification later. The key point is that the actual relation between these two sets of messages is unknown to the signer. This property is usually called the *unlinkability* or *untraceability* property [2][3]. Because of the unlinkability property, blind signature techniques are quite suitable for some applications, such as the untraceable electronic cash protocols [2][3] or anonymous electronic voting systems [5][6][7] [10][11][12], which have to protect the privacy of all users

In this subsection, we will describe a generic dual-randomized blind signature scheme by making use of generic function representation, which will be adopted to construct our electronic voting protocol. All components are briefly introduced as follows.

Let M be the underlying set of messages and R be a finite set of random strings chosen by the user. The generic randomized blind signature scheme contains five elemental functions (B', B, S, U, V) where

(1). ***B*:** $M \times R \times R \rightarrow M$ is a blinding function. It is impossible to determine the value of $m \in M$ from $B(m, r, u)$ without r where $r \in R$ is called the blinding factor of m and $u \in R$ is a randomization factor that is used to combine another randomization factor chosen by the signer. Besides, $B(m, r, u)$ is said to be the blinded message with a randomization factor.

(2). ***S*:** $M \times R \rightarrow M^K$ is a signing function that 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 pair $(m, x) \in M \times R$, it is computationally infeasible to form $S(m, x)$ or modify (m, x) embedded in $S(m, x)$ without this signing function S, where $S(m, x)$ is called the signer's signature on (m, x).

(3). ***B'*:** $R \times R \rightarrow R$ is a function for combining two randomization factors into a randomization parameter. Given x^* and $c = B'(u, x)$ where $(x^*, u, x) \in R^3$, the signer can derive $u^* \in R$ such that $B'(u^*, x^*) = c = B'(u, x)$. In addition, given u^{**} and $c = B'(u, x)$ where $(u^{**}, u, x) \in R^3$, anyone can derive $x^{**} \in R$ such that $B'(u^{**}, x^{**}) = c = B'(u, x)$.

(4). ***U*:** $M^K \times R \rightarrow M^K$ is an unblinding function. For each 4-tuple (m, r, u, x), $U(S(B(m, r, u), x), r) = S(m, c)$ where $c = B'(u, x)$. It is computationally infeasible to derive $S(m, c)$ from $S(B(m, r, u), x)$ without the blinding factor r.

(5). ***V*:** $M^K \times M \times R \rightarrow$ {true, false} is a public verification formula. $V(s, m, c)$ = true if and only if s is the signer's signature on the pair (m, c). Hence, $V(S(m, c), m, c)$ is always true for each $m \in M$ and $c \in R$.

The details of the generic dual-randomized blind signature protocols are described as follows:

(1). **Blinding:** First, a user chooses a message $m \in M$ and randomly selects two strings $(r, u) \in R^2$. Then the user computes the blinded message $\alpha = B(m, r, u)$ and transmits it to the signer.

(2). **Signing:** After receiving α, the signer randomly chooses a string $x \in R$ and computes

$$t = S(\alpha, x)$$

Then, the signer sends t back to the user. The parameter t is called a blind signature because the actual content of m embedded in α is unknown to the signer.

(3). **Unblinding:** After receiving t, the user derives

$$s = U(t, r) = U(S(B(m, r, u), x), r)$$

which is equivalent to $S(m, c)$ where $c = B'(u, x)$.

(4). **Verifying:** The parameter s is the signer's signature on the pair (m, c). The triple (s, m, c) can be verified by checking whether the verification formula $V(s, m, c)$ is true or not.

The signature s cannot be forged without the signing function S. This is called as the *unforgeability* property. Besides, it is information-theoretically impossible for the signer to derive the link between a signature s and the instance of the signing protocol which produces the blinded form t of s without r, that is, all of the signatures s's are indistinguishable from the signer's point of view without the corresponding blinding factor r's. This is the *unlinkability* property. In the blind signature scheme, the randomization parameter c is the combination of the randomization factor u, which is chosen by the user, and another randomization factor x selected by the signer. This is the *dual-randomization* property. Although the signer can be aware of the parameter c from (s, m, c), it cannot still link the triple to the instance of the signing protocol that produced t via the randomization factor x corresponding to c since there always exists a string $u^* \in R$ such that $B'(u^*, x^*) = c$ for each x^* selected by the signer in each different instance of the signing protocol.

2. The Proposed Scheme

The proposed e-voting scheme based on the generic dual-randomization blind signature is described in the following subsection 2.1. Especially, how to deal with coercibility or bribe will be explained in Section 2.2.

2.1. The Proposed Electronic Voting Protocol

The proposed scheme contains two types of participants, a tally center and a group of voters. The corresponding protocol consists of four stages, initialization, registration, voting, and verification. In the initialization stage, the center publishes some related information about this voting, such as the subject of the election, the list of candidates, the format of intentions, and so on. In the registration stage, a voter will be identified by the tally center through a secure identification mechanism, and then obtains an eligible ballot for the voting. In the voting stage, the voter will submit this vote to the tally center by using the technique of anonymous channels. In the final stage, the tally center will publish the final result of the election. Besides, there are some assumptions of the proposed scheme:

(1). Every vote has to prepare her/his smart card before performing the voting protocol.
(2). Every voter has to stay in the voting booth to accomplish the entire voting process.
(3). Every registered voter must accomplish the entire voting process without abstaining.
(4). The quality of networks between terminal sets and the center has to be guaranteed.

Then, details of the four stages will be described as follows,

(1). **Initialization stage**
Let M be the underlying set of messages and R be a finite set of random strings. The tally center chooses the five functions (B', B, S, U, V) of the generic dual-randomization blind signature scheme presented in Section 1.3. It makes the formats of B', B, U, V public, and lets the signing function S be kept secret. The center publishes the subject of the election, the list of candidates, the format of intentions, and other related information. Let $N \subset M$ be the public set of all possible intentions in this election. For example, if every voter can select one intention only in the election, such as the president election in a country, the number of elements in N will equal to the number of candidates in the election.

(2). **Registration stage**
When the voting day comes up, the voter takes her/his own smart card and enters a voting booth to start on performing the following steps.

Step 1. Identification

The tally center identifies a voter by an identification protocol or identifies each other by a mutual authentication scheme. We strongly suggest that the identification protocol can involve the biometric characteristics of the voter because that the biometric characteristics can help the center with confirming the identity of the voter physically without being masqueraded by anyone else. Besides, if a voter attempts to vote twice or more, the following voting steps will be terminated.

Step 2. Parameter generation

The identified voter chooses two strings $(r, u) \in R^2$ and decides her/his intention $m \in N$ for the election. The voter then computes

$$\alpha = B(m, r, u)$$

with her/his own smart card and submits α along with the voter's signature on the subject of the election (or on any other common information known by all voters) to the tally center.

Step 3. Signing

After verifying the voter's signature on the subject of the election, the center randomly chooses a string $x \in R$ and signs on the blinded message α to obtain

$$t = S(\alpha, x)$$

and sends t back to the voter.

Step 4. Vote obtaining

The voter performs the unblinding operation on t by computing

$$s = U(t, r)$$

and then forms the triple (s, m, c) where the randomization parameter $c = B'(u, x)$. The triple (s, m, c) represents a legitimate vote of the voter, and it can be verified by checking if

$$V(s, m, c) = \text{true}.$$

Step 5. Publication

At the last step of this stage, the center will publish the voter's signature on the subject of the election to show that the voter has indeed registered with the center. This step can convince all voters that the total amount of registered voters must equal to the total amount of the last tally result.

(3). **Voting stage**
At this stage, the voter will send her/his vote (s, m, c) to the tally center on an anonymous channel. After receiving the vote, the center will check that

(1). $m \in N$,
(2). $V(s, m, c) = \text{true}$, and
(3). the uniqueness of (s, c) among all received (s, c)'s.

After the checking progress, the center randomly chooses some valid votes for each intention i in N among the received votes and sends them to the voter. Finally, the voter is able to leave the voting booth.

(4). **Verification stage**
After the voting period ends up, the center will publish all valid votes and the tally result of the election. Every voter can verify if

(1). her/his vote is published (if not, the voter can submit her/his vote to the center again by an anonymous channel.);
(2). every published vote is correct through the verification formula; and
(3). the total amount of registered voters equals to the total amount of published votes.

2.2. The Ways to Overcome Coercibility and Bribe

Considering all possible ways of coercibility and bribe, we will explain how the proposed scheme can defend those attacks, respectively.

(1). **Observers**:
We make use of the voting booths to provide physical protection for all voters to guarantee that their behaviors cannot be observed when they are in the voting booths.

(2). **Masquerade:**
In the proposed scheme, we can adopt any identification mechanism to verify the identity of each voter as long as it is secure and effective. However, an identification scheme with the checking on the voter's biometric characteristics

is better since it can defend possible masquerade more effectively than a traditional one.

(3). **The selection of randomization factors:** There are only two randomly-chosen strings (u, x) existing in our scheme where u is selected by the user and x is selected by the center. In general, only the one chosen by the user can be controlled by a coercer. If the coercer enforces the voter to embed a designated string u^* into her/his ballot, then, after performing the proposed protocol, the voter can obtain a legitimate ballot (s, m, c). When all of the votes are published, the coercer has no idea to link the assigned u^* to the designated vote because that it can derive an corresponding x^* to satisfy $c = B'(u^*, x^*)$ for each published c. Consequently, the coercer cannot be convinced that the voter does follow its will to vote via the pre-assigned string u^*. Similarly, the voter cannot convince anyone else that the vote does belong to herself/himself via the u^* claimed in advance. It turns out that the action of vote-selling also fails through a pre-claimed randomization factor.

(4). **Voting receipts**: Instead of receipt freeness, we adopt the mechanism of multiple receipts in the proposed scheme such that each voter can receive a set of votes with all different intentions in N except her/his own vote when she/he is still in the voting booth. Thus, after the voter leaves the booth, the coercer cannot ensure whether the voter follows its will to vote or not according to these receipts. Also, the voter cannot convince any vote-buyer that some vote with some specified intention is her/his own vote through these receipts since the voter has a set of votes with all different kinds of intentions in N. Although the solution is not perfect, it is easily implemented. Especially, it is a practical solution when only a small portion of voters may be coerced or engage in selling their votes in an election.

3. Conclusions

In this paper, we have presented a generic idea, which is independent of the underlying cryptographic components, on electronic voting to achieve the uncoercibility property. Besides, the anonymity property is guaranteed through the techniques of blind signatures and anonymous channels in the proposed scheme. Moreover, due to the generic representation, the proposed scheme can be easily realized and it is flexible to satisfy efficiency and other requirements since it only depends on some basic cryptographic primitives.

References

[1] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," *Proc. 26th Symposium on Theory of Computing* (*STOC'94*), pp. 544-553, 1994.

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

[3] D. Chaum, A. Fiat, and M, Naor, "Untraceable electronic cash," *Advances in Cryptology-CRYPTO'88*, LNCS 403, Springer-Verlag, pp. 319-327, 1990.

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

[5] C. I. Fan and C. L. Lei, "Multi-recastable ticket schemes for electronic voting," *IEICE Transactions on Fundamentals*, vol. E81-A, no. 5, pp. 940-949, 1998.

[6] C. I. Fan and C. L. Lei, "An unlinkably divisible and intention attachable ticket scheme for runoff elections," *Journal of Network and Computer Applications*, pp. 93-107, 2002.

[7] C. I. Fan and C. L. Lei, "A universal single-authority election system," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E81-A, no. 10, pp. 2186-2193, 1998.

[8] 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.

[9] J. K. Jan and C. C. Tai, "A secure electronic voting protocol with IC cards," *Journal of Systems and Software*, vol. 39, no. 2, pp. 93-101, 1997.

[10] W. S. Juang and C. L. Lei, " A collision-free secret ballot protocol for computerized general elections," *Computers & Security*, vol. 15, no. 4, pp. 339-348, 1996.

[11] W. C. Ku and S. D. Wang, "A secure and practical electronic voting scheme," *Computer Communications*, vol. 22, no. 3, pp. 279-286, 1999.

[12] H. T. Liaw, "A secure electronic voting protocol for general elections," *Computers & Security*, vol. 23, no. 2, pp. 107-119, 2004.