A New Coercion-Resistant and Receipt-Free Electronic Voting System with Verifiability and Secrecy

Ying-Ching Chiu
Department of Computer Science
and Information Engineering
Tamkang University
New Taipei City, Taiwan, ROC
896410247@s96.tku.edu.tw

Wen-Bing Horng
Department of Computer Science
and Information Engineering
Tamkang University
New Taipei City, Taiwan, ROC
horng@mail.tku.edu.tw

***Abstract*—The coexistence of verifiability and voting receipts in an electronic voting system is a contradictory issue. Because the electronic vote is in a virtual form, voters rely on voting receipts to verify the integrity of the votes. However, the voting receipts also become the evidence for intimidators to confirm their vote-buying results. In this paper, we propose a new coercion-resistant and receipt-free electronic voting scheme with verifiability and secrecy. A voter can verify his/her voting result without any voting receipts. After all votes are casted, an electronic bulletin board is used to display all the ballots for public verification. With the careful design of "protective color," the private voting result will not be revealed. The voter can verify the integrity of his/her voting result by bare eyes. When counting the ballots, the decryption factor is used to remove the protective color. The privacy is kept as everyone is able to see all the ballots without knowing what they mean. Since there are no voting receipts, the chance of voter intimidation becomes impossible.**

Keywords-coercion-resistance; electronic voting; receipt-freeness; secrecy; verifiability; voting receipt

I. INTRODUCTION

Using information technology for electronic voting has many advantages, such as convenience, high efficiency, and low cost. However, these advantages can be achievable only when electronic voting is conducted in a fair and trustworthy way. This also has been a challenge for developing electronic voting systems.

Verifiability is one of the important security requirements in an electronic voting system. In general, this can be achieved by electronic signatures. Through the voting receipt, the voter can verify his/her voting result. However, this voting-receipt verifiability may cause serious criminal problems because it provides the evidence when the voter is coerced to vote for a specific candidate. Therefore, the coexistence of verifiability and the voting receipts in electronic voting systems has been a conflicting issue. Because electronic voting uses virtual ballots, many voters would like to verify their voting results. The voting receipts serve as an important means for verifiability. However, they also become the evidence for intimidators to confirm the voting results.

This research was partially supported by the National Science Council, Taiwan, ROC, under project number NSC 99-2511-S-032-004-MY3.

In this paper, we propose a new coercion-resistant and receipt-free electronic voting scheme with both verifiability and secrecy. A voter can verify his/her voting result without any voting receipts, while all the ballots are displayed publicly on an electronic bulletin board after votes are casted. Since we design the protective-color mechanism, the actual private voting result will not be revealed. The voter can verify the integrity of his/her voting result by bare eyes without any software and hardware. This is because he/she has set up the camouflaged rule by himself/herself. When counting the ballots, the decryption factor is used to remove the protective color. The secrecy is kept as everyone is able to see the all ballots without knowing what they mean. Since there are no voting receipts, the chance of voter intimidation becomes impossible.

The rest of the paper is organized as follows. In Section 2, we give a briefly introduction to electronic voting and related studies. In Section 3, we propose a new coercion-resistant and receipt-free electronic voting system to provide verifiability and secrecy. Finally, we conclude the paper in the last section.

II. ELECTRONIC VOTING AND RELATED STUDIES

A. Requirements of Electronic Voting

Fujioka et al. [1] first pointed out some basic requirements of electronic voting systems. Later, more perspectives were proposed in [2,3,4]. The major requirements of these studies include the following three criteria:

- *Verifiability*: Electronic voting must allow voters to verify whether their votes are altered.
- *Secrecy*: Though electronic voting requires verifiability, the secrecy of voters' voting results must be kept and remained unknown to the third party. Thus, the voters are able to cast a vote in his/her free will.
- *Receipt-free*: To achieve both verifiability and secrecy, verifiable voting receipts should be avoided.

Other requirements for electronic voting systems include fairness, soundness, eligibility, unreusability, and mobility.

B. Blind Signature

The earliest electronic voting scheme is proposed by Chaum [5]. In addition, he is also the first researcher who proposed the concept of blind signature [6]. The design of blind signature is that the requester does not reveal the message contents to the signer, while the receiver can verify if the message is signed by the signer or not.

The steps of a blind signature are as follows. The requester first adds a blind factor, C, to the message, M, to be sent. The message is sent to the signer as C(M), and the signer signs C(M) with his/her private key, S', to become S'(C(M)). The encrypted S'(C(M)) is then sent back to the requester. The requester uses C' to remove the blind factor to get a signed message as C'(S'(C(M))) = S'(M). Everyone is able to verify the message M using the signer's public key, S, because S(S'(M)) = M.

Therefore, blind signatures are suitable for the purpose of anonymity. It is also commonly used in electronic payment [7,8] and electronic voting [1,9,10,11,12,13,14]. Many studies regarding electronic voting adopt blind signatures to fulfill the requirements of verifiability and secrecy.

C. Receipt-Free Voting

The concept of receipt-free voting was first proposed by Benaloh and Tuinstra [15]. They established a physical voting booth, which can safeguard the secrecy and security. However, it disables the mobility of electronic voting. Later, Hirt and Sako [16] proposed a universal verifiability approach which does not require physical voting booths. The universal verifiability approach uses an electronic bulletin board to publish the verification information regarding the votes. In order to prevent the third party from interfering the voting, multiple ballot counting centers are required and the communications between ballot counting centers must be in secure channels.

IC card can also be used for electronic voting [17]. The voter uses his/her own IC card when casting a vote. This approach is trustworthy in terms of security and verifiability. Nevertheless, voting can be done only when a card reader is available. In addition, this approach is not entirely mobile.

In recent years, several receipt-free and coercion-resistant solutions are proposed in [18,19,20], which not only fulfill the basic requirements of electronic voting but also avoid problems of force voting and bribery. Therefore, enhancing the coercion-resistance in electronic voting such that intimidators have no way to know the private voting result is also one of the key points of our proposed scheme.

III. The Proposed Electronic Voting Scheme

A. Entities

There are four entities involved in our proposed electronic voting scheme: the Certificate Authority (CA), the Registration Center (RC), the Voting Center (VC), and the Ballot Center (BC). The Certificate Authority is for voters to apply electronic certificates, the Registration Center verifies a voter's identity, the Voting Center accepts the votes, and the Ballot Center counts the ballots.

B. Flow

Fig. 1 illustrates the flow of the proposed electronic voting scheme, including the relationship between the voters and aforementioned four entities as well as an electronic bulletin board (Board).

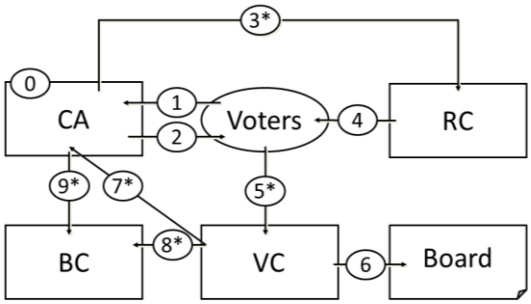

Figure 1. Flow of the proposed electronic voting scheme.

- **Stage 0**. In order to encrypt the transmitted messages in the process, the four entities in the scheme are required to have their own certificates.
- **Stage 1**. The Certificate Authority restricts the legitimate voters to apply their certificates for voting within a period of time, where the legitimate voters are determined based on a pre-approval electoral roll. Voters register their "protective colors" (to be discussed in the subsequent subsection) to protect their voting results in the Certificate Authority.
- **Stage 2**. After the Certificate Authority verifies the voter's identity, a private key specifically for voting will be issued to the voter.
- **Stage 3**. Before voting starts, the Certificate Authority submits the legitimate voter list to the Registration Center. To ensure the confidentiality and integrity of the message, the transmission process is encrypted, which is marked by an asterisk (*) in Fig. 1. Similarly, the transmissions in Stages 5, 7, 8, and 9 are all encrypted.
- **Stage 4**. The legitimate voter collects a ballot from the Registration Center. Each ballot has a random and unique serial number. The design of the serial number as random and unique makes the numbers unpredictable, so that duplicated voting or counterfeiting voting can be avoided. The serial number is used by the voter as an identifier to recognize which ballot is his/hers in the afterward process of public ballot displaying.
- **Stage 5**. The voter adds his/her "protective color" to the ballot before casting. Then, the ballot is sent to the Voting Center.
- **Stage 6**. The ballots received by the Voting Center are displayed in the electronic bulletin board.
- **Stage 7**. In the ballot counting process, the Voting Center will first rearrange the ballot order which was originally in serial number sequence order. The information of the rearranged order is kept secret such that the Voting Center is the only entity who knows about which serial number

corresponds to which voter. By rearranging serial number sequence order, the Voting Center then sends each voter's information to the Certificate Authority and makes a query regarding the decryption factor of the voter's protective color. In this step, the Certificate Authority only knows about whom the Voting Center is asking but does not know which ballot the query is linked to.

- **Stage 8**. At the same time when the Voting Center sends the query to the Certificate Authority, it also sends the voting results to the Ballot Center. The information sent to the Ballot Center contains no personal information but only the serial numbers and the camouflaged voting results marked by the "protective color." In this step, the Ballot Center knows about which ballot it is counting, but it does not know about who owns which ballot.

- **Stage 9**. Responding to the query made by the Voting Center, the Certificate Authority sends the voter's decrypted factor of the "protective color" information to the Ballot Center, rather than the Voting Center. In this step, the Ballot Center converts information from the Voting Center and the Certificate Authority to the real voting result. By doing so, none of the entities in the voting flow owns complete voter's information, and therefore the voter's results shall not be revealed.

In the above flow, Stages 7 and 8 proceed simultaneously, and Stage 9 comes right after Stage 7. The combination of Stages 8 and 9 determines a vote count, and Stages 7, 8, and 9 are repeated until all the ballots are counted.

C. *Protective Color*

The design of the "protective color" in our scheme is to prevent the malicious third party from knowing about the voters' real voting results. The *protective color* is a simple special mark (i.e., color) predefined by the voter; when the ballot result is displayed, the voter is able to verify his/her voting result by identifying the predefined special mark (color). Because others do not know about this special mark (color), they will not be able to know about the voter's real voting result. When counting the ballots, the special marks of the ballots will be removed, just like the removal of the protective colors, as shown in Fig. 2.

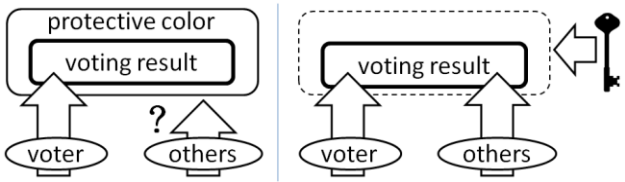

Figure 2. Usage and removal of protective color

The design of the simple special mark in our proposed scheme is the selection of a predefined color as the true color of the voter and all others are false colors. The voter predefines a true color to represent the voting result, as shown in Stage 1 of Fig. 1. The predefined true color is like a key. The use of different colors as special marks makes others people not able to know about the real voting results, just like encrypting with a symmetric key. However, this approach is different from the approach of using the same key for encryption and decryption in that the key owner can read key-encrypted information without the key, while others can only read the information with the key. Because of this, the feature is called the "protective color" in this paper.

For example, suppose that a voter predefines blue as his/her true color and that the serial number 1001089 is assigned on his/her ballot. How does he/she cast a vote? He/she appoints his/her true color to his/her preferred candidate, while all other candidates are appointed with different colors. The voter can find his/her ballot from the electronic bulletin board based on the serial number 1001089, as shown in Fig. 3, and can verify his/her voting result based on his/her predefined true color. The voter can also cheat the intimidator by saying that his/her true color is green or other colors.

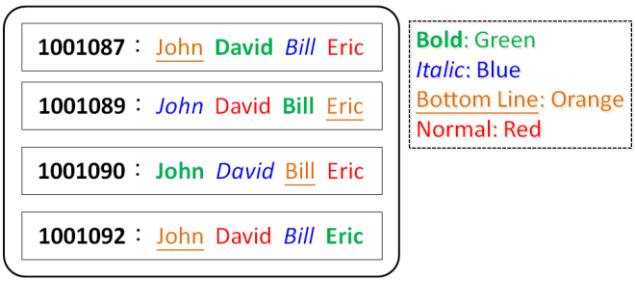

Figure 3. An example of the electronic bulletin board

The reason why adopting colors as the special marks is that colors contain no implication regarding sequence or size. These features make colors more neutral for camouflaging against the intimidator. No one knows about the voter's true color. As a result, no one is able to learn about the actual voting result either by observing the bulletin or by asking. With this design, the voter's true color information is critical and its confidentiality and security should be safeguard. The true color information in our scheme is registered and protected in the Certificate Authority.

D. *Ballot Counting Process*

The ballot counting process is shown in Stages 7 to 9 in Fig. 1 and Fig. 4 illustrates the details of this counting process. The protective-color decryption factor is the voter's true color. In Fig. 4, the Voting Center sends queries to the Certificate Authority regarding every voter's true color, which will be sent to the Ballot Center. The Voting Center also sends information of ballot serial number and voting results with protective color to the Ballot Center. Once the Ballot Center receives the above information, it can identify the actual voting results by removing protective colors from ballots with true color. The Ballot Center has the following properties.

- *Not able to add ballots*: The Voting Center has to make query to the Certificate Authority regarding the voter's true color and thereafter count an effective ballot. The illegal additional ballot will be discovered because such ballot does not have corresponding voter registered in the Certificate Authority.

- *Not able to delete or alter ballots*: As the bulletin reveals the voting results for the voters to do the verification, the

activities of ballot deletion and alteration from the Voting Center will be notified by the voters.

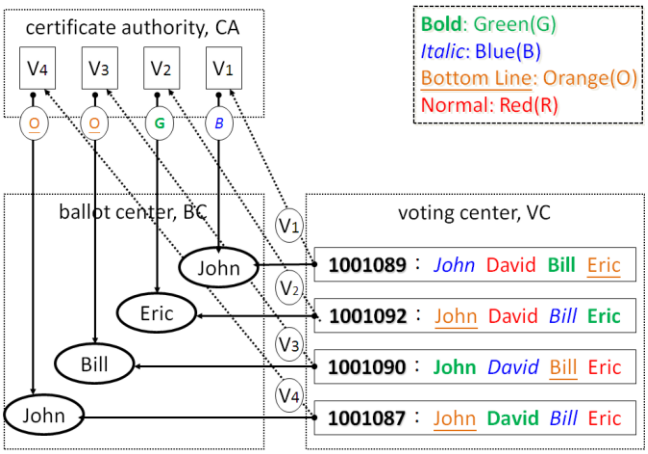

Figure 4. Ballot counting process

E. Design of Secrecy

The complete voter information in the proposed scheme includes (1) the association between the voter and the serial number, (2) the voter's true color information, and (3) the vote with the protective color. Only when all the above information is obtained does one know about the voter's ballot contents. In the voting flow proposed in our scheme, there is no entity that owns all the complete voting information.

Table I shows the information that each entity owns. The Certificate Authority owns only (2), the Voting Center holds (1) and (3), and the Ballot Center receives (2) and (3). The combination of (2) and (3) presents the actual voting result by removing the protective color. Without (1), no one is able to associate the ballot with a specific voter. Hence, the voter's voting result in the ballot counting process is safeguarded.

TABLE I. DISTRIBUTION OF VOTER'S INFORMATION

Voter's Information	CA	VC	BC
(1) The association between the voter and the serial number		○	
(2) The true color predefined by the voter	○		○
(3) The vote with the protective color		○	○

IV. CONCLUSION

Secrecy is one of the important principles in traditional voting systems so that the ballots cannot be displayed. In this paper, we proposed a new electronic voting scheme to provide secrecy as well as verifiability. In our scheme, the design of the protective colors on the ballots will keep the secrecy of the voting result. In addition, our scheme requires no additional hardware or software while retaining the verifiability without the voting receipts, which cleverly solves the contradiction of the coexistence between the voting receipts and verifiability. Therefore, in our proposed scheme, the voter is able to verify the voting result in the electronic bulletin board while the secrecy is still reserved. In addition, due to receipt-free, our scheme is also coercion-resistant.

REFERENCES

[1] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," Advances in Cryptology: Proceedings of AUSCRYPT'92, LNCS 718, 1993, pp. 244–251.

[2] A. Riera, J. Borrell, and J. Rifà, "An uncoercible verifiable electronic voting protocol," Proceedings of IFIP SEC'98, IT Global Security, 1998, pp. 206–215.

[3] J. Karro and J. Wang, "Towards a practical, secure, and very large scale online election," Proceedings of the 15th Annual Computer Security Applications Conference, 1999, pp. 161–169.

[4] L. F. Cranor and R. K. Cytron, "Sensus: a security-conscious electronic polling system for the Internet," Proceedings of the 30th Hawaii International Conference on System Sciences, 1997, pp. 561–570.

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

[6] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology: Proceedings of CRYPTO'82, 1983, pp. 199–203.

[7] C. I. Fan and C. L. Lei, "Low-computation partially blind signatures for electronic cash," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E81-A, no. 5, 1998, pp. 818–824.

[8] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," Advances in Cryptology: Proceedings of CRYPTO'88, LNCS 403, 1990, pp. 319–327.

[9] E. Mohammed, A. E. Emarah, and Kh. El-Shennawy, "A blind signature scheme based on ElGamal signature," Proceedings of the 17th National Radio Science Conference, 2000, pp. C25/1–25/6.

[10] J. L. Camenisch, J. M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," Advances in Cryptology: Proceedings of EUROCRYPT'94, LNCS 950, 1995, pp. 428–432.

[11] M. Stadler, J. M. Piveteau, and J. Camenisch, "Fair blind signatures," Advances in Cryptology: Proceedings of EUROCRYPT'95, LNCS 921, 1995, pp. 209–219.

[12] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," Proceedings of the 5th International Workshop on Security Protocols, LNCS1361, 1998, pp. 25–35.

[13] S. von Solms and D. Naccache, "On blind signatures and perfect crimes," Computers & Security, vol. 11, 1992, pp. 581–583.

[14] Y. Mu and V. Varadharajan, "Anonymous secure e-voting over a network," Proceeding of the 14th Computer Security Applications Conference, 1998, pp. 293–299.

[15] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 1994, pp. 544–553.

[16] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," Advances in Cryptology: Proceedings of EUROCRYPT'00, LNCS 1807, 2000, pp. 539–556.

[17] J. K. Jan and C. C. Tai, "A secure electronic voting protocol with IC cards," Proceedings of the 29th IEEE International Carnahan Conference on Security Technology, 1995, pp. 259–265.

[18] S. Delaune, S. Kremer, and M. Ryan, "Coercion-resistance and receipt-freeness in electronic voting," Proceedings of the 19th IEEE Computer Security Foundations Workshop, 2006, pp. 28–42.

[19] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pp. 61–70.

[20] S. G. Weber, R. Araújo, and J. Buchmann, "On coercion-resistant electronic elections with linear work," Proceedings of the The 2nd International Conference on Availability, Reliability and Security, 2007, pp. 908–916.