An Electronic Voting System Immune to Coercion and Bribery from Cross Layers in Large Scale Election

Zhen-Yu Wu[1], Tzer-Shyong Chen[2], Yu-Fang Chung[3], Kuo-Kuang Huang[1]
[1] Department of Information Management, National Penghu University of Science and Technology, Taiwan
[2] Department of Information Management, Tunghai University, Taiwan
[3] Department of Electrical Engineering, Tunghai University, Taiwan
zywu@gms.npu.edu.tw; arden@thu.edu.tw; yfchung@thu.edu.tw; kkhuang@gms.npu.edu.tw

Abstract

This paper classifies the bribery and coercion prevention E-voting schemes into five levels and proposes a novel electronic voting scheme that can achieve Level 4 by using blind signature with subliminal channel. With the proposed scheme, under the threat of violence/allurement of substance, voter can still fulfill his/her own will to vote for his chosen candidate through subliminal channel. Besides, this study suggests the use of the smart-card mechanism to protect against the subliminal-free channel counter attack from the coercer or briber, and thus allows the Arbitration Authentication Center to easily and clearly identify the content of the subliminal message and determines which candidate the voter really intends to vote for.

Key words: Bribery, Coercion, Subliminal channel, Smart-card, Arbitration Authentication Center

1 Introduction

Chaum raised the concept of electronic election in 1981. Because it was an untraceable technique [1], it was readily applied to the electronic voting scheme. From then on, electronic voting scheme has been developing for the past 36 years. To facilitate the scheme, several security requirements have to be met, the overview of which is as follows:

(1) Anonymity: A legal ballot is kept confidential.

(2) Accuracy: A legal ballot cannot be altered, abolished or replicated.

(3) Eligibility: Voters should pass authentication examination before casting ballots.

(4) Fairness: The immediate result of election is kept confidential until official announcement.

(5) Mobility: The act of casting a ballot is feasible at any location.

(6) Uniqueness: An eligible voter can only cast a vote for once.

(7) Verifiability: Ballots can be checked for verification.

(8) Uncoercibility: The act of casting a ballot is not securely governed by bribery and coercion.

The first seven requirements are generally fulfilled but the last item of uncoercibility is occasionally failed to be satisfied, in whose description the words “bribery” and “coercion” are used. By definition, “bribery” is a situation where an entity, or briber, provides voters with benefits ranging from banquets, remuneration to valuables to compensate for their obedience. On the other hand, “coercion” is a situation where an entity, or coercer, intimidates voters by political or other types of threats. Whereas coercers issue orders for voters to passively obey out of timidity, bribers allure voters to irresistibly follow their instructions with something desirable. Besides unconscious or voluntary obedience to either commands or allurements, there is another alternative for voters, which is an ingenious E-voting scheme of coercion/bribery prevention. Voters are allowed to have an extra channel of freedom and of security. By “freedom,” we mean that voters can cast ballots out of free will; by “security,” we mean that whether voters faithfully obey bribers’/coercers’ instructions or commands cannot be inspected and verified.

It does not make any change even when coercer/briber is aware of the potentials of that extra channel. Bearing this consideration in mind, this study turns to one essential technique in steganography, subliminal channel, to resolve the problem of easy exposure to outsiders. The detailed explanations of the scheme are temporarily put aside since we shall first of all examine coercers’/bribers’ verification behavior to check whether voters have indeed followed their commands or instructions.

The safety requirement of uncoerciblity occasionally fails to be met because of the fact that coercers/bribers have numerous approaches to verifying the movements of voters, including verifying if voters cast ballots as instructed. Schemes cannot preclude all the approaches that coercers/bribers resort to but merely prevent a certain type of verification approach. For instance, some receipt-free voting schemes may propose that if

*Corresponding Author: Zhen-Yu Wu; E-mail: zywu@gms.npu.edu.tw
DOI: 10.3966/160792642019052003004

coercers/bribers do not own the election result receipt, then they cannot verify whether voters have voted accordingly. Nevertheless, since this verification approach with receipt is impracticable, coercers/bribers can still know voters' intentions by comparing the encrypted value of ballot, by forcing key ballot information out of them, and by substituting them to cast ballots.

Recent published studies on electronic election do not indicate the verification behavior of coercers/ bribers. However, to classify the bribery/coercion prevention e-voting schemes, examination of verification behavior is indispensable. As a consequence, in the following very first section this study shall focus on possible verification behavior of coercers/bribers.

1.1 The Classification of Coercer's/Briber's Verification Behavior

Coercers/bribers identify whether voters have conformed to their orders or notwith several types of verification behavior. This study classifies different verification behavior of coercers/bribers into five categories: receipt checking, intermediate value comparing, parameter acquiring, election procedure monitoring, major secret revealing. These five categories of verification behavior are graded based on the amount as well as the significance of ballot information that coercers/ bribers have retrieved. Therefore, the grading is also an illustration that coercers/bribers have put how many efforts and also an indication that an e-voting scheme is able to achieve what degree of the coercion/bribery prevention. The five categories are graded in hierarchy, where higher levels have the properties of lower levels. To be specific, Level- i have the properties of Level-i and those levels below Level-i. An e-voting scheme can be called a Level-i scheme because it can avoid verification behavior of coercers/bribers on Level-i and those levels below Level-i. Thus, it is theoretically correct that a Level-3 scheme is automatically a Level-2 scheme. If a scheme has a higher level, it is more secure. Take the lowest level, receipt checking, for example. Election receipt is the only thing that coercers/bribers ask for to make sure whether voters do what they have instructed. The other four verification behavior can employ similar explications. Table 1 shows the ranking of verification behavior.

Table 1. The levels of coercer's/briber's verification behaviors

Level 5	Level 4	Level 3	Level 2	Level 1
Major Secret Revealing	Election Procedure Monitoring	Parameters Acquiring	Intermediate Values Comparing	Receipt Checking

In the following sections, we will elaborate on the five levels of verification behavior and use some published e-voting schemes as examples to inspect the extent to which they can prevent the verification behavior.

1.1.1 Level 1: Receipt Checking

The Level 1 verification behavior is entitled "receipt checking," where coercers/bribers require voters to present election result receipt. If the later election result announced by Tally Center (TC) corresponds to the election result receipt desired, then it means that coercers/bribers successfully control voters to vote the intended candidates.

"Receipt checking" ranks the lowest because the receipts are the only ballot information-contained items that need to be exposed.

Many electronic voting schemes [1-2, 18, 20, 23] propose the use of election result receipts so as to meet the requirement of verifiability. There are pros and cons to the use of election result receipts. Receipts not only can be employed by voters to check whether their ballots have been counted fairly by the TC but they can also leave traces for coercers/bribers as a means to monitor the act of casting ballots. The convenient guidance of receipts proposed by these receipt-based schemes invites bribery and coercion.

To resolve the problem, Benaloh and Tuinstra initiated the concept of a receipt-free electronic voting scheme [3] in 1994, in which voting systems no longer provide voters with receipts as demonstration of voting. Many researchers have been contributing to the concept of receipt-free voting. Sako and Killian promoted anonymous mixnet. Okamoto invented trap-door bit-commitment and an untappable channel [15]. Chen et al. included a supervising center to oversee the announcement process of election result [7]. It is Fan and Sun that utilized multiple receipts [4]. Liaw applied smart card techniques to the proposed scheme of electronic voting [11]. The works mentioned above successfully excluded the possibility of the exposure of detailed election result [5-6, 8]. In other words, the election result does not reveal information about which ballots go to which candidates. Hence, it is impossible for coercers/bribers to know whether or not their coercion/bribery attempts have been successful. These published schemes significantly reduce the possibility of the "receipt checking" behavior of coercers/bribers.

1.1.2 Level 2: Intermediate Values Comparing

When a coercer/briber intercepts the original ballot transmission messages to monitor the voting, this behavior is called "intermediate values comparing". In this situation, the coercer/briber checks to see if the voter conformed to the request from the intercepted messages.

For example, consider the no-receipt scheme proposed by Chen et al. [7]. It encrypts one ballot

through the election center's public key so that the values of the ballot's contents can be pre-computed and compared against the intercepted ballots by the coercer/briber to determine the equivalency between the two objects and confirm the voter obeys his/her order. In addition, the interrupted values can be directly ascertained for if the voter indeed followed the coercer/briber's instruction based on the form of the ballot in these three no-receipt schemes [5-6, 21]. These e-voting schemes, though resist the "receipt checking" behavior, cannot prevent against this behavior, and it is designated as Level 2.

The following published e-voting schemes can withstand the Level 2 behavior. Liaw made the meaningless intermediate values avoiding an attempt of comparison by coercer/briber [11]. Carrollet al. applied the method of probability encryption leading the intermediate values can not identify. Benaloh and Tuinstra used a physical voting booth to prevent a coercer/briber from checking the message value as the voter is casting his ballot [3-4]. Sako and Killian used an untappable channel to guarantee that the voting channel can not be eavesdropped. Okamoto employed trap-door bit-commitment to make the vote indistinguishable [15]. Juels et al. allowed voters to create fake credentials to deceive the coercer/briber that the voter obeyed instructions [8]. However, the Juels et al. scheme has been shown to require vast computational overhead [13]. This leads to the methods published by Smith and Schweisgut which improve the efficiency.

1.1.3 Level 3: Parameters Acquiring

If the intercepted intermediate values of some schemes in Level 2 were encrypted with random values or mixed with nonpublic parameters, then the coercer/briber will not be able to assess the intercepted message against an expected value. In this case, the coercer/briber may resort to "Parameters acquiring", which is designated as Level 3 behavior. For "Parameters acquiring" the voters are asked to provide the parameters related to casting of the vote to the coercer/briber. These values are typically generated only temporarily for a particular election period, such as a provisional key, voter-made or center-issued values. Since these parameters can help coercer/briber to calculate these mixed or encrypted intermediate values after acquiring, they will easily catch if voters conform to his/her instructions from comparing. The "major secret" of a voting scheme, such as the voting master key, which is used to sign the signature and represents voter, or the important credential of voting does not belong to the voting parameters (the clear definition of the major secret will be given in Level 5).

For instance, the form of ballot proposed by Liaw [11] and Carrollet al. mixes random parameters generated by the voter and prevents the coercer/briber from performing the verification behavior of Level 2. However, if all these parameters are obtained by the coercer/briber, a voter will not be able to lie and cast the ballot under their own volition.

Six electronic voting schemes can protect against Level 3 behavior. Sako et al. and Okamoto have developed electronic voting schemes [15] that transmit the most significant parameters needed in an election through the anonymous untappable channel. They are impossible for the coercer/briber to discover and obtain. The voters can cast their vote at will even though all other related values have been given to the coercer/briber.

Benaloh et al.'s scheme [3] provides a specific physical voting booth (as in a traditional election) for voting. Any parameters needed for the election are generated at the voting booth and the transmission processes are also completed at the voting booth. Therefore, it is impossible for the coercer/briber to ask voters for these critical values. A similar method is also used in the proposal by Fan and Sun [4].

Juels et al. proposed a scheme [8] that permits the voters to imitate a fake credential when voting to convince the coercer/briber that the voter complied with their instructions. Meanwhile, the voter actually utilizes an anonymous channel to cast the vote secretly using true credentials. This enables the scheme to prevent Level 3 behavior.

1.1.4 Level 4: Election Procedure Monitoring

One election usually divides its procedure into several phases, e.g. register, authentication, voting, and announcement. It may happen that the voters secretly transmit their volitions at the other phases (except voting time) through an anonymous or untappable channel which can not be detected, the Level 3 verification behavior done by the coercer/briber is thus resisted and a higher level behavior is needed. This higher level behavior is, "election procedure monitoring", Level 4. At this level, the coercer/briber observes the entire election processes. Any action performed and any related parameter generated by a voter are disclosed, such as sending the certificate, selecting a significant parameter, choosing the content of the ballot, using a key to encrypt the vote, and so on. Because most information is revealed, it is exceedingly hard to cheat and violate the coercer/briber. As mentioned in Level 3, the major secret is not part of the observed information in this level. The reason will explain in Level 5.

These schemes employ the untappable channel to send the voter's own will or specific values not withstanding this level of behavior [8, 15, 22, 24]. Both schemes published by Benaloh and Tuinstra [3] and Fan and Sun [4] resist it because they utilize the voting booths. Since any actions related to election (e.g., selecting important parameters, choosing the number

of candidates, encrypting the ballot), begin and end at the voting booth, it is impossible for the coercer/briber to monitor the voters and observe those values chosen by the voters. In addition, Chung and Wu proposed an e-voting system with passwords in 2012 [21] to distinguish whether a voter was bribed and coerced and to solve the substitutive coercive voting. Nevertheless, the scheme was based on the RSA public key algorithm, which required longer key to guarantee the security that the efficiency would be unfavorable in large-scale elections.

Wu et al. proposed a scheme to claim that the procedure monitoring behavior could be prevented. However, the significant long-term private key in their scheme needed to keep secret [25]. In 2017, Hsiao et al. [19] made the ballot content which could merely be inquired by the voter himself. This method was similar to using physical booths.

1.1.5 Level 5: Major Secret Revealing

Most cryptographic schemes, protocols, and electronic applications always own one significant value belongs to themselves such as the private key of one public-key crypto system, the signing key of a digital signature scheme, the share key of the authentication protocol, and the master key of the electronic commerce and government application. These secrets are usually the last line of defense. Once they are revealed, a malicious adversary may do anything that the secret's original owner can do, and the proposed security methods essentially become useless. We call it is "major secret", a kernel of one system that is not allowed to reveal.

Likewise, if an object obtained by others can vote in complete substitute for the voter in all election procedures, it is the major secret of an electronic voting scheme such as voting master key, and voting credential. If the secret is revealed to the coercer or briber, it does not matter what coercion/bribery prevention methods are in place. No-receipt, trap-door, bit-commitment, untappable channel, and physical voting booth, are proposed, but become meaningless since the secret allows the coercer/briber to perform all election procedures without the voter. This behavior is defined as Level 5.

All electronic voting schemes displayed in Table 2 below indicate that none of them is qualified for preventing against this Level 5 behavior. Surely, it does not mean that there is no any researcher who can present a practical method, which is qualified for preventing the behavior. Following the current tendency of well-developed technology of steganography, probably through combining the characteristic of indistinguishableness with the other related techniques, an approach might come true, by which a coercer/briber is allowed to join in voting in behalf of the voter even in case that he/she obtains the major secret, but actually he/she just unconsciously elects someone desirable by the voter. Such a concept is also one direction to address for us in the future.

Table 2. Levels of the existing e-voting schemes on coercer/briber behavior prevention

Scheme & Level \ Behavior		1	2	3	4	5
Fujioka, 1992 [2]	0	X	X	X	X	X
Mohanty and Majhi, 2010 [18]	0	X	X	X	X	X
Hwnag, Wen, Hwang, 2005 [6]	1	O	X	X	X	X
Chen, Jan-Chen, 2004 [7]	1	O	X	X	X	X
Lin, Hwang, Chang, 2003 [5]	2	O	O	X	X	X
Laiw, 2004 [11]	2	O	O	X	X	X
Juels, 2005 [8]	3	O	O	O	X	X
Li et al., 2008 [24]	3	O	O	O	X	X
Chung and Wu, 2009 [22]	3	O	O	O	X	X
Fan and Sun, 2006 [4]	4	O	O	O	O	X
Wu et al., 2014 [25]	4	O	O	O	O	X
Hsiao et al., 2017 [19]	4	O	O	O	O	X

1: Receipt Checking, 2:Intermediate Values Comparing
3: Parameters Acquiring, 4:Election Procedure Monitoring
5: Major Secret Revealing

1.1.6 Levels of the Existing E-voting Schemes on Coercer/briber Behavior Prevention

Based on the above discussion of the behaviors of the briber/coercer, the different levels of coercion/bribery prevention can be achieved by previously proposed electronic voting schemes and are investigated and categorized in Table 2. It provides the level information pertaining to whether or not the published e-voting schemes can prevent the five kinds of adverse verification behaviors. In this table, the notation "O" indicates that the designated published scheme can prevent that level of adverse verification behavior, and the notation "X" indicates that it cannot prevent that level of adverse verification behavior. Additionally, if a scheme can prevent at one level, it can also prevent all behavior levels below that since the information obtained in a higher level also involves the information obtained in the lower one.

1.1.7 Our Contributions

This study proposes a new electronic voting scheme that focuses on solving the bribery and coercion problems from level 1 to 4 mentioned above through the technique of blind signature with subliminal channel. In explicit terms, under the threat of violence/allurement of substance, voter can still pretend to obey the coercer/briber's orders, but secretly votes for his chosen candidate via the subliminal channel without being discovered. Besides, in order to prevent the coercer/bribery doing the subliminal-free channel counter attack, this study also suggests using the smart-card mechanism to protect the ballot. Thus,

at the end of the election, Arbitration Authentication Center (AAC) can easily and clearly identify the content of the implication ballot and determines which candidate the voter voted for.

1.2 Outline of the Paper

The rest of the paper is organized as follows. Section 2 introduces the techniques used in our scheme. Section 3 contains our proposed e-voting scheme including the entities, the process adopted, and detailed procedure; its security analysis is in Section 4. Future works is discussed in Section 5, where conclusions are also drawn.

2 Related Techniques

2.1 Blind signature

Blind signature indicates that signers can put valid signatures on the content of the message even though they cannot recognize it or they cannot locate their signatures on it whenever it is retrieved [17]. Due to its feature of anonymity, this technique of blind signature can be applied to e-voting [16], in which voters can conceal their own ballot information by means of obtaining a legal ballot signed blindly by the Election Center. This way, even if Tally Center announces publicly which candidate is voted for, the identity of the particular voter will never be discovered, and he/she can remain anonymous.

This paper mainly contributes to the research on bribery/coercion prevention. We propose the technique of subliminal channel so as to prevent the occurrences of coercion and bribery [10, 14]. Messages transmitted through subliminal channel to the designated receivers remain encrypted, which are different from signature messages. To be specific, messages that go through subliminal channel are hidden from all the people concerned except for the general signature messages that are intended for correctness verification. Thus, subliminal channel serves as a feasible method for voters to hide their voting volitions from coercers and bribers.

Regrettably, coercers and bribers may utilize the subliminal-free channel as a measure to counter attack the subliminal channel, stopping voters' transmission of voting volitions. In such a case, the smart-card mechanism is actuated as a precaution against the attack of subliminal-free channel so that subliminal channel can remain intact. Furthermore, the relations between voters and Tally Center can remain anonymous with another protective measure known as Mixnet technique. Mixnet technique functions as Mixer disturbs transmitted messages to such an extent that the disorganized orders of them are unable to be redeemed. This way, it is impossible to track the relations between the receiver (Tally Center) and its sender (Voter).

2.2 Mixnet

Chaum was the first person who proposed the idea of Mixnet [1] in 1981. The main function of Mixnet is to allow a set of senders to send their message anonymously. The structure composes of senders, receiver, and mixer. After senders send out the encrypted messages (using the public keys of receiver and mixer in order) to mixer, mixer uses its private key to decrypt the received messages and jumbles up the order of the messages, and then outputs them simultaneously. Thus, it prevents the receiver from determining the source of the message, as shown in Figure 1. Applied to electronic voting, mixer can mix up the IP addresses coming from different voters so that the Election Center on receiving the ballots shall not be able to identify the IP addresses pertaining to the ballots. Naturally, it cannot know which ballot belongs to which voter. In the era of fast developing science and technology, various types of Mixnet are being successively developed by scholars [9, 12]. Comparatively, depending on their needs, designers can choose a suitable type of Mixnet to apply in their e-voting scheme instead of being confined to that proposed by Chaum [1].

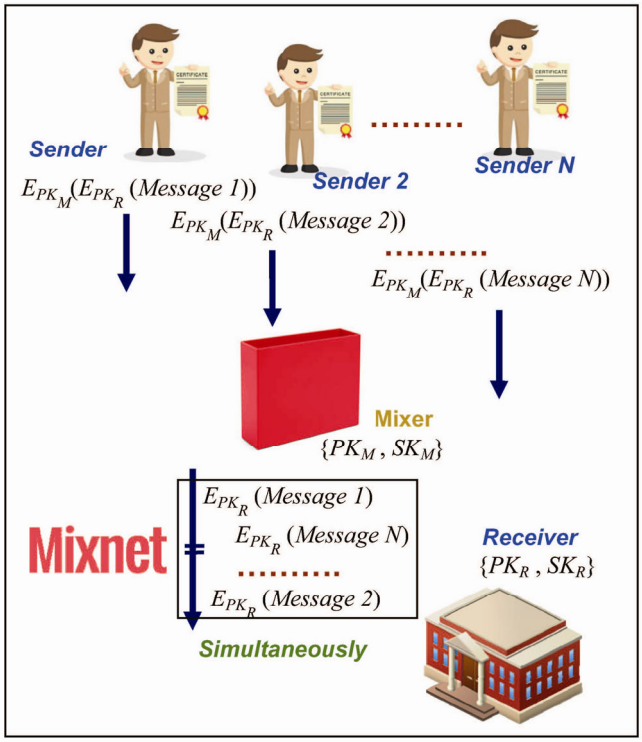

Figure 1. The process of transmission using mixer

3 Our Electronic Voting Scheme

There are three main components associated with our e-voting scheme: Arbitration Authentication Center, Tally Center, and voter. Arbitration Authentication Center (AAC) is the trustable third-party facility which

is responsible for certifying legality of voter, blind signing voter's ballot, and handling bribery and coercion problem. The Tally Center (TC) is responsible for confirming legal votes, checking double voting, and counting votes during the announcing of ballot phase. Voter is a person who has right to vote. Besides, in order to achieve the demand of anonymity, the voter communicates with TC via Mixnet as mentioned in Section 2.2.

Our e-voting process is constructed with four phases, authentication, voting, announcing, and off-line disputes phase. We would illustrate the overview of the process and the intention of some important parameters.

The main function of authentication phase, which is composed by step ***1*** and ***2*** in Figure 2, is authenticating legitimacy of voter and blind signing the content of voter's ballot. Therefore, there will be the interaction and communication between voter and AAC.

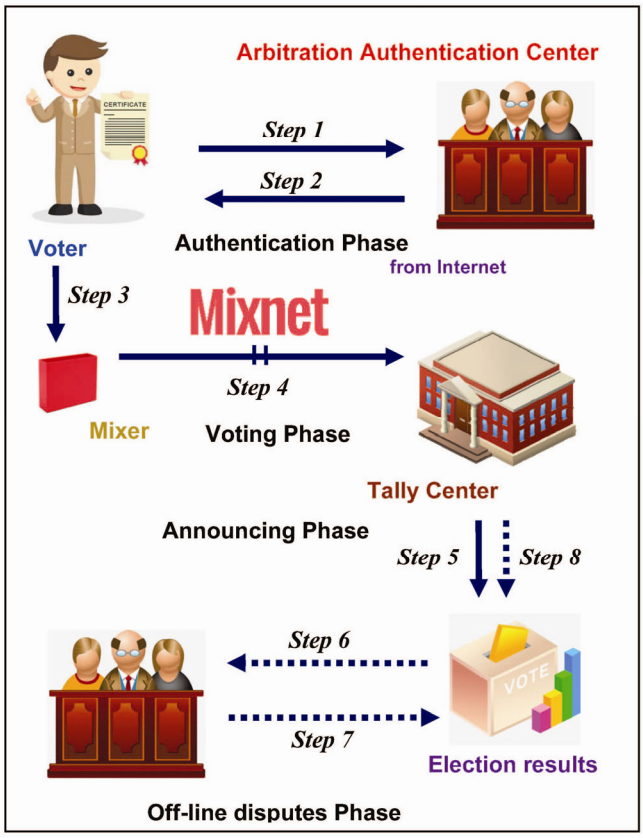

Figure 2. The structure of our E-voting scheme

First, AAC transmits the significant parameter T, which could help voters to generate the blind ballot e', to each voter. Continually, voter computes e' and its signature $Sig_v(e')$, and sends them with his/her certificate $Cert_v$ to AAC. After AAC receiving these information delivered by voter, it will confirm the validity of voter by $Cert_v$, and then generate the blind signature of ballot s'. After returning s, the authentication phase is completed.

3.1 The Notations of Our e-Voting Scheme

Before describing the detailed process of our scheme, we would define some notations which appear in the scheme:

p	a large prime (about 1024 bits)
q	a prime factor of p-1 (about 160 bits)
Z_p	set of integers modulo p
Z^*_p	multiplicative group of order q
g	generator of order q in Z^*_p
x_u	the private key of user u
y_u	the public key of user u, $y_u = g^{x_u} \bmod p$
x_v, y_v	the private key and public key of voter
x_{AAC}, y_{AAC}	the private key and public key of AAC
x_{TCS}, y_{TCS}	the short term private key and public key of TC; they expire within one election, meaning that a different key pair is assigned at each election
$Cert_v$	the public key certificate of voter issued by Certificate Authority
$E_u(m)$	the encrypted m by probability encryption method using user u's public key under asymmetric cryptosystem
$Sig_u(m)$	the digital signature of m which signed by user u's private key under asymmetric cryptosystem
$h(\cdot)$	a collision-resistant cryptographic hash function
$\|\|$	a concatenate notation
m	the content of ballot, each candidate has assigned an unique number to represent his/her identity
M	the set of m, $M=\{m_1, m_2, m_3,\ldots, m_n\}$, where n represents the number of all candidates
key	the session key used in subliminal channel shared with AAC and the designated voter, this key is pre-made by both private keys x_v and x_{AAC}, which equals $g^{x_{AAC}x_v} \bmod p = y_{AAC}^{x_v} \bmod p = y_v^{x_{AAC}} \bmod p$
m'	the subliminal message transmitted in subliminal channel

3.2 The Process of Our E-Voting Scheme

All voters and ACC would own a public and private key pairs (x_v, y_v) and (x_{AAC}, y_{AAC}) respectively at the beginning. On the other hand, TC would have a short-term public key y_{TCS} issued by the trust unit, named Election Certificate Authority. However, the short-term private key x_{TCS} is obtained by TC only after the voting period ends. Our e-voting scheme divides the process of election into four phases, authentication phase, voting phase, announcing phase, and off-line disputes phase.

Authentication phase

A1: AAC randomly chooses $t_v \in_R Z^*_p$, and embeds $T_v = g^{tv} \bmod p$ in smart card for each voter to compute the ballot with blind factor. Besides, AAC must publish a list of candidates' information, $M = \{m_1, m_2, \ldots, m_n\}$.

A2: Voter selects the desired candidate's number m from M and inputs it to the smart card. The card will

take the TC's short term public key y_{TCS} to encrypt m as the equation $E = E_{TCS}(m) \bmod p$ presented, and compute $R = T_v \cdot g^{a+b} y_{AAC}{}^{c} \bmod p$, $e = h(R \| E) \bmod q$, and $e' = e + c \bmod q$, where $a, b, c \in_R Z^*_p$, automatically. Finally the value of e', and its signature $Sig_v(e')$, which is signed by the embedded private key x_v, will be obtained from the outputs of the card.

A3: Voter sends his/her certificate $Cert_v$, e', $Sig_v(e')$ to AAC.

A4: AAC verifies the correctness of voter's certificate $Cert_v$, e', and $Sig_v(e')$. If one of them is incorrect, AAC will return the 'wrong' message to voter and stop authentication. Else, go to A5.

A5: AAC uses its private key x_{AAC} to sign the blind signature $s' = e' x_{AAC} + t_v \bmod q$.

A6: AAC returns s' to voter.

Voting phase

After receiving the value s', voter generates the legitimate signature of ballot and sends it with his/her ballot to TC.

V1: Voter utilizes the smart card to generates $s = s'+a+b \bmod q$, the legal signature of ballot.

V2: Voter sends the ballot $\{(s, e), E\}$ obtained form the smart card to TC via the Mixnet.

V3: After receiving $\{(s, e), E\}$ from voter, TC verifies the ballot by checking the equation $e \stackrel{?}{=} h(g^s y_{AAC}^{-e} \bmod p \| E)$.

If correct, the ballot $\{(s, e), E\}$ will be recorded to the database to avoid voter double voting; Otherwise, publish the error information with this ballot in the Bulletin Board.

V4: TC announces each value of ballot $\{(s, e), E\}$ in the Bulletin Board to show that voter's vote is indeed received.

Announcing phase

In this phase, TC counts the votes and announces the result of election.

N1: In order to prevent TC from knowing the immediate election result before announcing the ballots, TC gets its short term private key x_{TCS} from Election Certificate Authority after the voting time.

N2: TC decrypts each E using its short term private key x_{TCS} as $D_{TCS}(E)$ and obtains the content m.

N3: TC announces each corresponding s as a receipt for each voter at Bulletin Board.

Under no bribery and coercion condition, TC can announce the result of election as shown in Table 3. However, if voter hid true voting will in ballot by subliminal channel, AAC would discover them when it examines each s during the off-line disputes phase.

Table 3. The result of election

candidate 1	$\{ s_{v1}, s_{v2}, \ldots, s_{vx} \}$
candidate 2	$\{ s_{v3}, s_{v5}, \ldots, s_{vz} \}$
…	…
candidate N	$\{ s_{v6}, s_{v8}, \ldots, s_{vy} \}$

Off-line disputes phase

In this voting system, voter could use subliminal channel to disguise his/her true voting under bribery and coercive condition. When TC publishes the value of s in voting phase, AAC can examine it whether having subliminal message or not. The steps is shown as below:

D1: If voter wants to send the subliminal message m' to AAC, the value of $(a+b)$ must use the value of $[h(key)+ m']$ to substitute when he/she computed $R = T_v \cdot g^{a+b} y_{AAC}{}^{c} \bmod p$, and thus the value s would be equal to $s' + h(key)+ m' \bmod q$. Note that the m' will be inputted while voter keys in the special PIN to start the smart card as Section 2.3 shows.

D2: Before AAC examining each s, it needs to pre-compute the set of session key $\{key_i\}$, where i represents each different voter, and store them in its database.

D3: AAC computes each value of $[s_i' + h(key_i)] \bmod q$.

D4: AAC tries to add each likely candidate number as m' to $[s_i' + h(key_i)]$ seeing whether or not the value of $s_i' + h(key_i)+ m'$ equals s_i. If two values are the same, this means that the voter's true choice is m'. And original message m is involuntarily selection which is threatened by coercer or briber.

D5: AAC places the value of $h(h(key_i) + key_i)$ on the field of candidate which the voter had in mind, and places the value of s on the coercer/briber-appointed candidate. And this situation will cause the announced vote count to not match the actual vote count. The extra random values need to be placed on the other candidates (except for the candidates the coercer/briber had in mind), such that each candidate receives an additional virtual vote. Record the total number of virtual included in the final result.

D6: AAC returns the final election result to TC for announce.

3.3 Example for Off-line Disputes Phase

In Figure 4, there are three candidates in this election simulation with total 3,000 votes. We know that at the announcing phase, TC publishes all received s as mentioned above. Supposing that voter no. 7 had used subliminal channel to send his true voting-will, the candidate no. 3, for AAC, his vote, signature s_7, should be equal to $s_7' + h(key_7)+ 3$. In order to examine the hidden message s_7 successfully, the AAC needs to pre-compute two sets, including the set of session key $\{key_1, key_2, \ldots, key_{3000}\} = \{ y_{v1}{}^{xAAC}, y_{v2}{}^{xAAC}, \ldots, y_{v3000}{}^{xAAC} \}$ and the set $\{s_1' + h(key_1), s_2' + h(key_2), \ldots, s_{3000}' + h(key_{3000})\}$. So that the AAC can add each likely candidate number, e.g. 1, 2, and 3, to the value $s_7' + h(key_7)$ and then check which is equals to s_7. Certainly, the outcome shows that the voter no. 7 wants to vote for the candidate no. 3.

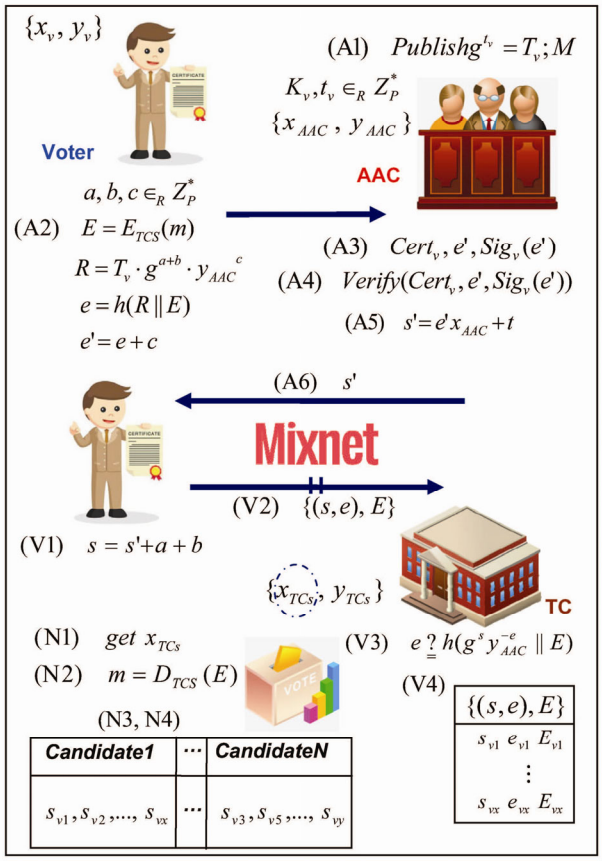

Figure 3. The first three phases of proposed e-voting scheme

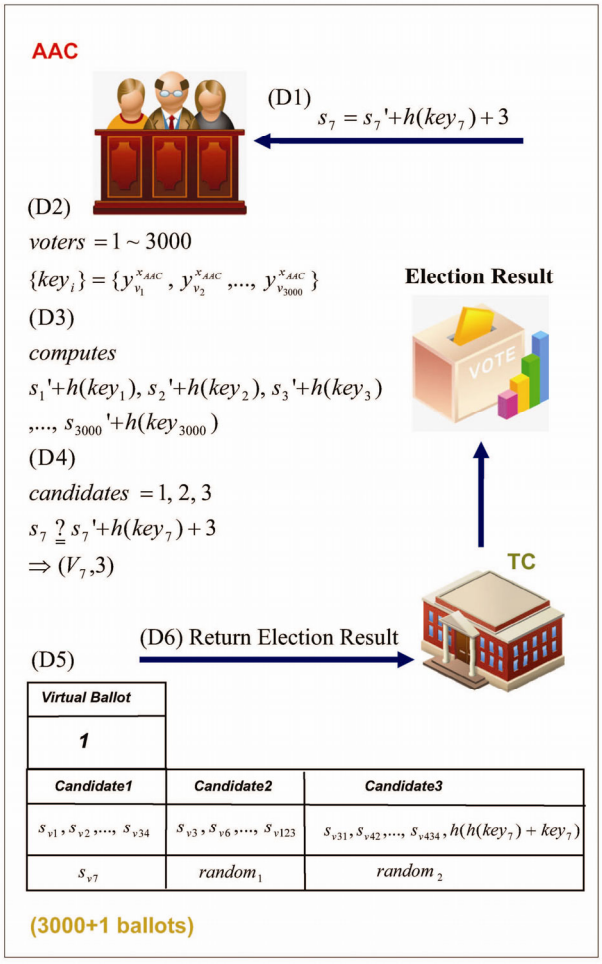

Figure 4. The example of the process of Off-line disputes phase

After that, surely the AAC has known of being coerced or bribed, and the candidate whom was told to vote for is candidate no. 1. Then, the AAC manipulates the result. Hence, $h(h(key_7)+key_7)$ shown for voter no. 7 is placed in the results of the candidate no. 3, and s_{v7} is placed in the results of the candidate no. 1. In addition, an extra random value is assigned to the other two candidates, to show that the three values: $random_1$, $random_2$, and s_{v7} are virtual votes. Finally, an announcement, that a virtual ballot was included in the votes is made; returns the final election result to TC.

4 Security Analysis

This e-voting scheme could satisfy the requirements of fairness, eligibility, uniqueness, anonymity, accuracy, mobility, verifiability, and uncoercibility. In particular, this system focuses on uncoercibility. In Section 4.8, we would explain how it could pass the bribery and coercive verification behaviors from Level 1 to 4 defined in Section 1.1 and offer the formal proof in detail.

4.1 Fairness

Fairness means the election result would not be revealed before the announcing phase. This requirement is essential for a fair election. If one e-voting scheme allows TC or voters to determine the immediate result, then anyone could possibly know whether the candidate he/she supported would win or lose the election. Hence, some people may attempt to influence other voters who have still not cast their ballot to vote for he/she wanted through threatens or lures.

In this scheme, we use probability encryption method to protect the content of vote and hence prevent this situation happening. The following equation appears in authentication phase:

$$E = E_{TCS}(m)$$

We apply the ElGamal encryption protocol [34] to encrypt vote message m, then E will be equal to $\{g^r, y_{TCS}{}^r \cdot m\}$. Because r is randomly chosen by each voter, no other people can know what the value is, and hence they are impossible to compute m by guessing r under the hard problem of Discrete Logarithm Problem (DLP). In addition, TC decrypts E must until the

announcing phase when it obtained its short private key x_{TCS} from Election Certificate. Therefore, no one can know or compute the immediate result from E easily. This meets the concept of fairness.

4.2 Eligibility

Eligibility means whoever owns legitimate right could participate in an election. While running the authentication phase of our scheme, each voter must send his/her certificate $Cert_v$ to AAC for verification, and these information are then required to be check including the correctness of signature, the validity of voter's public key, and some personal data such as serial number, identifier, issuer and etc. from the certificate. Therefore, if a person passes this phase, he/she is a legal voter undoubtedly.

4.3 Uniqueness

Uniqueness means one legal voter can vote only one time. The proposed scheme could achieve it with two reasons. One is that TC stores each ballot $\{(s, e), E\}$ in its database. Hence, if voter attempts to vote twice by sending the same $\{(s, e), E\}$ again, TC will discover by finding this value appear in the database. Another reason is the based blind signature cannot be forged by any selected message, i.e. if (s, e), E exists, then the (s', e''), E' would not be made by it as follows:

Assume the fake ballot $\{(s', e''), E'\}$ is existed, then the E' will be the message which selected by adversary A. e'' is made by E' and original signature (s, e) which equals $h(g^s y_{AAC}^{-e} \bmod p \,\|\, E') \bmod q$. And s' equals $s + e''x_{AAC} - ex_{AAC} \bmod q$. When this fake ballot $\{(s', e''), E'\}$ sends to TC, it can still pass the verification due to the reasons of:

$$
\begin{aligned}
& h(g^{s'} y_{AAC}^{-e''} \bmod p \,\|\, E') \\
=& h(g^{s+e''x_{AAC} - ex_{AAC}} g^{-e''x_{AAC}} \bmod p \,\|\, E') \\
=& h(g^{s - ex_{AAC}} \bmod p \,\|\, E') \\
=& h(g^{s} y_{AAC}^{-e} \bmod p \,\|\, E') \\
=& e''
\end{aligned}
$$

However, AAC will be impossible to be shared with A with the trusted private key. Once A tries to compute s'; this means he/she must get the AAC's private key x_{AAC} from its public key y_{AAC}; this is a contradiction with DLP problem. Consequently, we can say the adversary cannot forge the $\{(s', e''), E'\}$ from $\{(s, e), E\}$.

4.4 Anonymity

Anonymity means no entity can trace the relation between voter and his/her ballot. The entities include the other voters, TC, and AAC. We first consider the AAC, the possibility of its trace ability. Because of the unlink ability property of the blind signature which is used in this paper [23], even if the AAC can derive $c_i = e'_i - e$, $a_i + b_i = s - s'_i$, and $R_i = T_{vi} \cdot g^{ai+bi} y_{AAC}^{ci}$ from one published (s, e), E (where T_{vi}, e'_i, and s'_i are stored parameters in the AAC's database of each voter i). However, the AAC cannot determine which (R_i, c_i, a_i+b_i) corresponding to this (s, e), E, since all (R_i, c_i, a_i+b_i) of voter i can pass the verification $e \stackrel{?}{=} h(g^s y_{AAC}^{-e} \bmod p \,\|\, E)$ as following shows [29].

The computed (R_i, c_i, a_i+b_i) will make the equation $e \stackrel{?}{=} h(g^s y_{AAC}^{-e} \bmod p \,\|\, E)$ is always held:

$$
\begin{aligned}
& h(T_{vi} \cdot g^{ai+bi} y_{AAC}^{ci} \bmod p \,\|\, E) \\
=& h(T_{vi} \cdot g^{s-s'i} y_{AAC}^{e'i-e} \bmod p \,\|\, E) \\
=& h(T_{vi} \cdot g^{s-e'i x_{AAC} - tv_i} y_{AAC}^{e'i-e} \bmod p \,\|\, E) \\
=& h(g^{tv_i} \cdot g^{s-e'i x_{AAC} - tv_i} y_{AAC}^{e'i-e} \bmod p \,\|\, E) \\
=& h(g^{s-e'i x_{AAC}} y_{AAC}^{e'i-e} \bmod p \,\|\, E) \\
=& h(g^{s} y_{AAC}^{-e'i} y_{AAC}^{e'i-e} \bmod p \,\|\, E) \\
=& h(g^{s} y_{AAC}^{-e} \bmod p \,\|\, E) \\
=& e
\end{aligned}
$$

Hence, the probability that the AAC traces the relationship between voter and his/her ballot is zero.

We continually think about the TC, a center which is responsible for receiving and verifying the correctness of ballot. Because it does not recognize the sending IP address of the voter which has been jumbled up by mixer, it cannot distinguish a vote sending by certain voter.

Finally, we state that no voters can find out the related values form the two results that TC announces corresponding to the associated voter. The reason is that the published values are meaningless for tracing the relationship unless they voted voter voluntarily divulges the values to others that correspond to him/her.

4.5 Accuracy

Accuracy means no one can alter, remove, or duplicate the ballots. In this proposal, each voter can firstly make sure that his/her ballot $\{(s, e), E\}$ is indeed received by TC from the first announcement. Continually, after the election, voter can confirm the ballot has been counted by TC through the final announcement. Since each voter can double check his/her vote, therefore there is no opportunity for anyone to alter, remove, or duplicate the ballots.

4.6 Mobility

This scheme is designed to run on the current Internet. The voters only require basic equipment such as modem or Ethernet device for browsing the World Wide Web. Then, no matter where voters are, they can cast their ballots. Thus, this paper obtains the requirement of mobility.

4.7 Verifiability

Verifiability means that each voter can confirm his/her ballot whether it has been counted correctly or not. In this proposal, since the election results are announced by TC, voter can check ballot easily.

When all is said in done, each electronic voting scheme ought to underestimate certainty that this requirement is essentially achieved. In any case, it has a defect. If someone bribes or coerces voter to cast his/her vote for a designated candidate, he/she can easily determine whether a voter obeyed his/her order via the result of the election. In order to avoid this situation happening, some schemes only announce the total number of votes that each candidate obtained, but this causes the voter cannot check if his/her ballot counted or not. Strictly speaking, this method seems not to be taken as an excellent solution. Consequently, this proposal uses the way of virtual ballots to announce the election result which not only meets verifiability but also prevents bribery and coercion.

4.8 Uncoercibility

In brief, uncoercibility means the ability to prevent bribery and coercion. Specifically, the two unjust situations happen easily with electronic voting system; thus this security requirement is concerned more and more.

This study proposes a new e-voting system that can solve level 1 to 4 of bribery and coercion problems that mentioned in Section 1.1, i.e. four verification behaviors: receipt checking, intermediate values comparing, parameters acquiring, and election procedure monitoring. Though the technique of blind signature with subliminal channel and the major secret, the PIN of the smart card is kept secret. Besides, in order to prevent the subliminal-free channel from countering attack, this study also offers the smart-card mechanism as protection. Thus, we can successfully pass these deliberate verifications; The details are shown below:

4.8.1 Passing the "Receipt Checking" Verification

"Receipt checking" means voters must identify their will of vote by providing the election receipt to the coercer/briber. In this scheme, although the coercer/briber indeed could obtain the receipt. In fact, voter had used the subliminal channel to send his/her true voting will for AAC; hence we can say that the scheme prevents the "receipt checking" behavior certainly.

4.8.2 Passing the "Intermediate Values Comparing" Verification

"Intermediate values comparing" means the designated value for voters. Then, the coercer/briber would catch those values for comparing them with voters' expected values.

"Intermediate values comparing" means the designated value for voters. Then, the coercer/briber would catch those values for comparing them with voters' expected values. As mentioned in Section 4.8.1, voter is permitted to use the subliminal channel sending his/her true voting will for AAC secretly. Therefore, no matter what values the coercer or briber assigns, the verification result will always conform his/her anticipation.

4.8.3 Passing the "Parameters Acquiring" Verification

"Parameters acquiring" means voters offer the temporary parameters of ballot casting to coercer/briber for verifying the correctness of ballot. In this scheme, the smart card generates all the critical values related to voters' true voting will. In this case, coercer/briber would have no way to obtain the values. Therefore, it makes the coercer/briber hard to determine if the voter violates his/her order secretly from the offered ballot. The "parameters acquiring" verification behavior then lacks efficiency.

4.8.4 Passing the "Election Procedure Monitoring" Verification

"Election procedure monitoring" implies voters permit the coercer/briber to watch how a voter takes part in the race and throws the ticket, and in this manner to control every single basic esteem voters picked. Under this circumstance, to ensure that voter still can send his/her volition to AAC effectively, this plan depends on the inputted PIN of the smart card (the significant mystery) ought not be uncovered and shrewd card security machine to guarantee the subliminal channel can correspondence effectively and the without subliminal counter assault is futile. The reason is the estimation of $h(key)$ and subliminal message m' are created by the keen card. Indeed, even different qualities might be chosen by coercer or briber; be that as it may, the s unquestionably breaks even with $s'+ h(key)+m'$ that can not be modified. Subsequently, AAC can get the subliminal message completely. The "race technique observing" conduct will wind up noticeably unimportant in this plan.

4.8.5 Proof of the Uncoercibility Requirement

There are two investigations executed in this formal confirmation. The distinction between them is that one test has the non-unimportant likelihood ε to comprehend the Decisional Diffie-Hellman (DDH) issue (the definition will be portrayed later), and alternate does not. On the off chance that the coercer/briber can perceive that the voter did not take after his/her request really, there will exist a remarkable probability ε for taking care of DDH issue. What's more, that is a disagreement for the DDH issue.

Security Model

Before sealing the uncoercibility prerequisite, we initially characterize five capacities which are identified with our electronic voting plan, including

Authentication, BlindSign, Vote, Announce, and Verify. These capacities will be made out of the security model of our electronic voting plan and utilized as a part of two trials of the formal evidence.

Authentication phase: Two functions are involved in this phase.

Authentication ($Cert_v$, T_v, PK_{AAC}, $\underline{SC}$, n_C, PK_{TCS})→(e')

This capacity takes as info the testament of voter $Cert_v$, a parameter T_v, the public key of AAC PK_{AAC}, three irregular numbers a, b, c produced by the keen card $\underline{SC}$, the candidate number n_C, and the temporary public key of TC PK_{TCS}, and outputs a blind ballot e'. It will be performed by voter himself/herself.

BlindSign (e', t_v, SK_{AAC})→(s')

This function takes as input the blind ballot e', a secret parameter t_v, and the private key of AAC SK_{AAC}, and outputs a blind signature of the ballot s'. It will be done by AAC alone.

Voting phase: Only single function is included in this phase.

Vote (s', $\underline{SC}$, n_C, PK_{TCS})→(ballot)

This function takes as input the blind signature of ballot s', three arbitrary numbers created by smart card $\underline{SC}$, the candidate number n_C, and the impermanent public key of TC PK_{TCS}, and yields a tally of this election. This will be performed by voter himself/herself.

Announcing phase: Two functions are included in this phase.

Announce ($Ballot$, SK_{TCS})→($\boldsymbol{X}$, $\boldsymbol{R}$)

This function takes as input the voted ballot, and the temporary private key of TC SK_{TCS}, and after that yields the arrangement of each numbered vote $\boldsymbol{X}$, and the election result $\boldsymbol{R}$. This will be executed by TC.

Verify ($\boldsymbol{X}$, $\boldsymbol{R}$)→({0,1})

This function takes as information the arrangement of each counted ballot $\boldsymbol{X}$, and the election result $\boldsymbol{R}$. If one voter's vote is sure numbered, it will output "1", otherwise "0".

Assumptions

Three presumptions exist in this formal proof. One is the Decisional Diffie-Hellman (DDH) presumption. Another is the limitation of the private key. What's more, the other is the utilization of the smart-card protection mechanism for protecting some parameters.

Diffie-Hellman (DH) Parameter Generator

We let a randomized algorithm $\boldsymbol{g}$ to be a DH parameter generator. For any pair of primes p and q, where q divides p-1, we have the generator $\boldsymbol{g}$ from Z^*_p with order q, and thus, $<\boldsymbol{g}>= G$ is a q-order subgroup of Z^*_p.

Decisional Diffie-Hellman (DDH) Problem

Let $\boldsymbol{g}$ be a DH parameter generator. The challenger chooses a, b, $z \in_R Z^*_p$ and then flips a fair coin $b \in \{0,1\}$. If b = 1, it outputs (g, g^a, g^b, g^{ab}) to the adversary. Otherwise, it outputs (g, g^a, g^b, g^z). The adversary must output a guess b' for b.

Decisional Diffie-Hellman (DDH) Assumption

We suppose that there is an algorithm $\boldsymbol{B}$ said to have advantage $\varepsilon(k)$, where k is a polynomial time, in solving the DDH Problem if

$$|\Pr[\boldsymbol{B}(g,g^a,g^b,g^{ab})=0]-\Pr[\boldsymbol{B}(g,g^a,g^b,g^z)=0]| \geq \varepsilon(k)$$

The distribution in the left is referred as the Problem of DDH, and in the right as the Random of DDH. The DDH assumption is said to hold for g if any polynomial time algorithm has negligible advantage in solving the DDH problem of g.

The restriction of private key

The major secret of this scheme is the PIN of the smart card, since we can not reveal it, the embedded private key is also impossible to reveal by each member.

The use of the Smart-card Protection Mechanism

The three parameters a, b, and c, which are utilized to make the visually impaired mark of this e-voting plan, will be consequently created by the keen card. Along these lines, they are difficult to be acquired by the malevolent briber and coercer. Now, we consider the two experiments Experiment1 and Experiment2 to prove the security requirement of uncoercibility:

Theorem 1. Based on the DDH assumption, even the coercer/briber acquires the set of parameters ($Cert_v$, T_v, e', n_A, n_V), the probability that he/she knows the voter volition n_V counted in $\boldsymbol{R}$ is small than ε.

【Proof】

Experiment1 $\mathbf{Exp1}^{C/B-resist}_{ES,A,V}$ ($Cert_v$, T_v, $\underline{SC}$, n_A, n_V)

V←Controller(coercer/briber);
% coercer/briber controls voter
e'←Authentication ($Cert_v$, T_v, PK_{AAC}, $\underline{SC}$, n_A, PK_{TCS});
s'←BlindSign (e', t_v, SK_{AAC});
% coercer/briber controls the election processes
ballot←Vote (s', $\underline{SC}$, n_A, PK_{TCS});
session_key←MakeKey (PK_{AAC}, SK_V);
%voter gives session key to coercer/briber
$\boldsymbol{X}$, $\boldsymbol{R}$←Announce ($Ballot$, SK_{TCS});
% TC announce the result
If b = 1% voter flips the coin
  $\underline{SC}$←HideMsg (n_V, session_key);
  % voter hides the true will in smart card
If b = 0
  $\underline{SC}$←HideMsg (null, null);
  %voter no hides the true will in smart card
Verify ($\boldsymbol{X}$, $\boldsymbol{R}$);
%coercer/briber verifies the election result
  b'←Guess($\boldsymbol{X}$, $\boldsymbol{R}$, "b");
  % coercer/briber guesses the value of b
  If $b' = b$
    Output the value "1";
Else

Output the value "0"; % end the experiment

We input the five required components to begin the trial, including the endorsement of voter $Cert_v$, some parameters utilized as a part of this e-voting plan T_v and $\underline{SC}$, and the voter's and coercer's/briber's voting-will sn_V and n_A.

The function V←Controller (coercer/briber) showed up in here speaks to that the coercer/briber assumes an intense part in this examination. That is, he/she can control all actions of the election performed by the voter such as Authentication, Vote, and Verify. Besides, he/she can obtain the correct session_ key, which is produced by the function session_ key←MakeKey (PK_{AAC}, SK_V) and used to hide the voter's true voting-will n_V in subliminal channel, from the voter. Therefore the coercer/briber will have the enough information to judge whether the voter casts the ballot with his/her volition secretly or not.

The voter flips a fair coin $b \in \{0,1\}$ before the coercer/briber checks the election result. If b = 1, he/she will hide the true voting-will n_V and the session key in the smart card by the function $\underline{SC}$←HideMsg (n_V, session key). Otherwise he/she will hide nothing by another function $\underline{SC}$←HideMsg (null, null).

Finally, the coercer/briber guesses the value of b by determining if some value related to the session_key is announced in $\boldsymbol{X}$ and $\boldsymbol{R}$ as the function b'←Guess($\boldsymbol{X}$, $\boldsymbol{R}$, "b") presented. If the guessed value b'= b, the experiment will output the value "1", otherwise it will output the value "0".

Since the coercer/briber knows the correct session key, they will have the likelihood more than 0.5 to figure if the voter hides his/her own will n_V in smart-card. We can view this as the real attack on the DDH problem form by (g, g^{xv}, g^{xAAC}, $g^{xAAC\ xv}$), and have the probability which is equal to $|\Pr[b=b'] - \frac{1}{2}| \geq \varepsilon$ in taking care of this issue.

Presently, we hand our consideration over another test Experiment2. This experiment is similar to Experiment1. The distinction between them is that the session key utilized as a part of this test is an arbitrary number. It is made by the function session key←MakeKey (PK_{AAC}, z). The contents of the experiment are demonstrated below:

Experiment2 $\mathbf{Exp2}^{C/B-resist}_{ES,A,V}$ ($Cert_v$, T_v, $\underline{SC}$, n_A, n_V)

V←Controller(coercer/briber);
% coercer/briber controls voter
e'←Authentication ($Cert_v$, T_v, PK_{AAC}, $\underline{SC}$, n_A, PK_{TCS});
s'←BlindSign (e', t_v, SK_{AAC});
% coercer/briber controls the election processes
ballot←Vote (s', $\underline{SC}$, n_A, PK_{TCS});
session_key←MakeKey (PK_{AAC}, z);
%voter gives session key to coercer/briber
$\boldsymbol{X}$, $\boldsymbol{R}$←Announce ($Ballot$, SK_{TCS});
% TC announce the result
If b = 1% voter flips the coin
  $\underline{SC}$←HideMsg (n_V, session_key);
  % voter hides the true will in smart card
If b = 0
  $\underline{SC}$←HideMsg (null, null);
  %voter no hides the true will in smart card
Verify ($\boldsymbol{X}$, $\boldsymbol{R}$);
%coercer/briber verifies the election result
b'←Guess($\boldsymbol{X}$, $\boldsymbol{R}$, "b");
% coercer/briber guesses the value of b
If $b' = b$
  Output the value "1";
Else
  Output the value "0"; % end the experiment

The coercer/briber still can control all actions performed by the voter in this experiment. Be that as it may, it is hard for him/her to distinguish whether the voter hides n_V in smart card or not since the obtained session key is an irregular number. Therefore, the probability that he/she exactly guessed the value of b is equal to 0.5. At the end of the day, the coercer/briber can only figure the estimation of b randomly and does not have enough data possessed in the Experiment1 to guess.

We will obtain another DDH problem formed by (g, g^z, g^{xAAC}, g^{zxAAC}) and have the probability equal to $|\Pr[b=b'] - \frac{1}{2}| = 0$ to break it.

In this manner, we can finish up from these two investigations that the probability that the coercer/briber knows the voter hides the true voting-will n_V in smart card is non-negligible and equal to ε:

$$|\Pr[\boldsymbol{B}(g, g^{x_v}, g^{x_{AAC}}, g^{x_v x_{AAC}}) = 0] -$$

$$\Pr[\boldsymbol{B}(g, g^{z}, g^{x_{AAC}}, g^{z x_{AAC}}) = 0]| \geq |(\frac{1}{2} \pm \varepsilon) - \frac{1}{2}| = \varepsilon$$

This leads us having the non-negligible probability ε to break the DDH problem. We complete the proof of the Theorem 1.

4.9 Comparisons

Different schemes to resist bribery behavior have been analyzed in Chapter 2. This section would focus on the scheme being able to satisfy security requirements and the cost being high or low. The schemes published in past years are selected for the comparison.

Table 4 shows a comparison of security features between this scheme and nine proposed schemes, where the numbers 1 to 7 sequentially stand for Fairness, Eligibility, Uniqueness, Anonymity, Accuracy, Mobility, and Verifiability. The notation "O" stands for the scheme achieving the requirement. Besides, aiming at the complexity of computational

time, and the main security mathematical hard problem are compared in Table 5. It is discovered that election schemes require the technology of blind signature that the computational time would not appear large differences. It requires about 7-14 exponential times to complete one-time voting. Anonymous channel is applied to ordinary schemes, e.g. mixnet, public proxy server, or public key technology. A large amount of votes are collected and sent out together. It would have TC not be able to distinguish where the votes are from to ensure the characteristic of secret ballot. Untappable channel is used for some schemes to achieve such a characteristic, but would spend more costs. Furthermore, as described in Chapter II, it likes physical devices that the primary characteristic of mobility of e-voting would disappear. Based on different design principles for various schemes, the based mathematical hard problems would be distinct; however, most schemes are based on the common mathematical hard problems of RSA or DLP.

4.10 Applications

Being the feature of democratic society, election and voting are the process of decision-making behavior. The idea of democratic politics would be achieved by having the citizens who are qualified for voting elect competent candidates or leaders. The rapid development of technology and network application technology has the world constantly promoting electronization in the social transformation. The idea of e-voting is therefore derived.

E-voting schemes could be applied to various applications, including research foundations, shareholder meetings in a company, securities management agency, and mayor and council member election. When using an e-voting system, the voters do not have to arrive in the place for voting, but could simply log in the system through the smart phone, iPad, and notebook to complete voting. The votes are automatically counted and the results are verified that the election staff does not need to print the vote one by one, deal with the printing of election paper, and manually handle votes to effectively reduce voting costs and enhance economic benefits and effectiveness.

What is more, e-voting presents the advantage of mobility. Completing voting through network could overcome the restrictions on climate and region, enhance voting rate, and reduce the citizens' voting time and costs. The vote verification process would approach simplicity to shorten the time for voters waiting for long vote verification process and would enhance the correctness, completeness, and fairness.

5 Conclusion & Future works

In this paper, we first classify the coercer's/briber's behaviors into five levels according to the significance and amount of ballot information the coercer/briber can get hold of. Continually, the existing e-voting schemes are leveled according on these behaviors. Because the examined schemes achieved level 3 or 4 lose the mobility and convenience by using strong assumption or impractical physical equipments, we propose the electronic voting scheme which not only keeps these properties but resists coercion and bribery problems from Level 1 to 4 effectively.

The proposal cited the technique of blind signature with subliminal channel. In explicit terms, under the threat of violence/allurement of substance, voter can feint to obey the coercer/briber's orders, but secretly votes for his chosen candidate via the subliminal channel without being discovered. Besides, in order to withstand the coercer/bribery doing the subliminal-free channel counter attack, the scheme uses the smart-card mechanism to protect the ballot. Arbitration Authentication Center thus can easily and clearly identify the content of the implication ballot and determines which candidate the voter voted for.

Table 4. The security requirements comparison between 7 schemes

	1	2	3	4	5	6	7
Lin et al. Scheme (2003)	O	O			O	O	O
Fan et al. Scheme (2006)	O	O	O	O	O		O
Li et al. Scheme (2008)	O	O	O	O	O	O	O
Chung et al. Scheme (2012)	O	O	O	O	O	O	O
Wu et al. Scheme (2014)	O	O	O	O	O	O	O
Hsiao et al. Scheme (2017)	O	O	O	O	O	O	O
Proposed Scheme (2018)	O	O	O	O	O	O	O

1. Fairness; 2. Eligibility; 3. Uniqueness; 4. Anonymity; 5. Accuracy; 6. Mobility; 7. Verifiability.

Table 5. The cost comparison between 7 schemes

	Computational Complexity	Based Security Hard Problem
Lin et al. Scheme (2003)	14 Exponent	DLP & RSA
Fan et al. Scheme (2006)	7 Exponent	RSA
Li et al. Scheme (2008)	14 Exponent 4 Hash	DLP
Chung et al. Scheme (2012)	8 Exponent 2 Symmetric	RSA
Wu et al. Scheme (2014)	10 Exponent	DLP
Hsiao et al. Scheme (2017)	11 ECExponent 2 Symmetric	ECDLP
Proposed Scheme (2018)	10 Exponent	DLP

Since this scheme only achieve against the coercive and bribery problems from Level 1 to 4, which can not resist the level 5 behavior. Therefore, our future works will focus on "How to design a scheme to maintain the existing secure properties and prevent all levels of bribery and coercion behaviors".

Acknowledgements

This work was supported partially by the Ministry of Science and Technology of Republic of China under the Grants MOST 106-2622-E-029-005 -CC3 and 106-2221-E-029-005.

References

[1] D. L. Chaum, Untraceable Electronic Mail, Return Address and Digital Pseudonyms, *Communications of the Association for Computing Machinery*, Vol. 24, No. 2, pp. 84-88, February, 1981.

[2] A. Fujioka, T. Okamoto, K. Ohta, A Practical Secret Voting Scheme for Large Scale Elections, *Advances in Cryptology AUCRYPT' 92 Proceedings*. Springer-Verlag, Berlin, Heidelberg, 1992, pp. 244-251.

[3] J. Benaloh, D. Tuinstra, Receipt-Free Secret-Ballot Elections, *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, Montreal, Quebec, Canada, 1994, pp. 544-553.

[4] C. I. Fan, W. Z. Sun, Uncoercible Anonymous Electronic Voting, *Proceedings of the 2006 Joint Conference on Information Sciences*, Kaohsiung, Taiwan, 2006, pp. 721-725.

[5] I. C. Lin, M. S. Hwang, C. C. Chang, Security Enhancement for Anonymous Secure E-voting over a Network, *Computer Standards & Interfaces*, Vol. 25, No. 2, pp. 131-139, May, 2003.

[6] S. Y. Hwang, H. A. Wen, T. Hwang, On the Security Enhancement for Anonymous Secure E-voting over Computer Network, *Computer Standards & Interfaces*, Vol. 27, No. 2, pp. 163-168, January, 2005.

[7] Y. Y. Chen, J. K. Jan, C. L. Chen, The Design of a Secure Anonymous Internet Voting System, *Computer & Security*, Vol. 23, No. 4, pp. 330-337, June, 2004.

[8] A. Juels, D. Catalano, M. Jakobsson, Coercion-Resistant Electronic Elections, *WPES 2005 Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*, Alexandria, VA, 2005, pp. 61-70.

[9] M. Jakobsson, A Practical Mix, *Advances in Cryptology — EUROCRYPT'98 Lecture Notes in Computer Science*, Vol. 1403, Springer, Berlin, Heidelberg, 1998, pp. 448-461.

[10] A. K Awasthi, S. Lal, Proxy Blind Signature Scheme, *Transaction on Cryptology*, Vol. 2, No. 1, pp. 5-11, 2005.

[11] H. T. Liaw, A Secure Electronic Voting Protocol for General Elections, *Computes & Security*, Vol. 23, No. 2, pp. 107-119, March, 2004.

[12] M. R. Clarkson, A. C. Myers, Coercion-Resistant Remote Voting Using Decryption Mixes, *Workshop on Frontiers of Electronic Elections*, Milan, Italy, 2005.

[13] S. Weber, A *Coercion-Resistant Cryptographic Voting Protocol – Evaluation and Prototype Implementation*, Master Thesis, Darmstadt University of Technology, Darmstadt, Germany, 2006.

[14] L. C. Wu, Y. S. Yeh, T. S. Liu, Analysis of Sun et al.' Link ability Attack on Some Proxy Blind Signature Schemes, *Journal of Systems and Software*, Vol. 79, No. 2, pp. 176-179, February, 2006.

[15] T. Okamoto, Receipt-free Electronic Voting Schemes for Large Scale Elections, *Proceedings of Workshop on Security Protocols Lecture Notes in Computer Science*, Vol. 1361, Springer, Berlin, Heidelberg, 1997, pp. 25-35.

[16] M. S. Hwang, C. C. Lee, Y. C. Lai, An Untraceable Blind Signature Scheme, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E86-A, No. 7, pp. 1902-1906, July, 2003.

[17] Z. Tan, Z. Liu, C. Tang, Digital Proxy Blind Signature Schemes Based on DLP and ECDLP, *MM Research Preprints*, *No. 21, MMRC, AMSS, Academic*, Sinica, Beijing, 2002, pp. 212-217.

[18] S. Mohanty, B. Majhi, A Secure Multi Authority Electronic Voting Protocol Based on Blind Signature, *International Conference on Advances in Computer Engineering*, Bangalore, India, 2010, pp. 271-273, 21-22.

[19] T. C. Hsiao, Z. Y. Wu, C. H. Liu, Y. F. Chung, Electronic Voting Systems for Defending Free Will and Resisting Bribery and Coercion Based on Ring Anonymous Signcryption Scheme, *Advances in Mechanical Engineering*, Vol. 9, No. 1, pp. 1-9, 2017.

[20] D. Chaum, Elections with Unconditionally-secret Ballots and Disruption Equivalent to Beaking RSA, *Advances in Cryptology — EUROCRYPT '88 Lecture Notes in Computer Science*, Vol. 330, Springer, Berlin, Heidelberg, 1989, pp. 177-182.

[21] Y. F. Chung, Z. Y. Wu, Casting Ballots over Internet Connection Against Bribery and Coercion, *the Computer Journal*, Vol. 55, No. 10, pp. 1169-1179, 2012.

[22] Y. F. Chung, Z. Y. Wu, Approach to Designing Bribery-free and Coercion-free Electronic Voting Scheme, *Journal of Systems and Software*, Vol. 82, No. 12, pp. 2081-2090, December, 2009.

[23] O. Cetinkaya, A. Doganaksoy, Pseudo-Voter Identity (PVID) Scheme for E-voting Protocols, *The Second International Conference on Availability, Reliability and Security*, Vienna, Austria, 2007, pp. 1190-1196.

[24] C.-T. Li, M.-S. Hwang, C.-Y. Liu, An Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks, *Computer Communications*, Vol. 31, No. 10, pp. 2534-2540, 2008.

[25] Z. Y. Wu, J. C. Wu, S. C. Lin, An Electronic Voting Mechanism for Fighting Bribery and Coercion, *Journal of Network and Computer Applications*, Vol. 40, pp. 139-150, 2014.

Biographies

Zhen-Yu Wu received the Ph.D. degree in Computer Science from National Taiwan University in 2011. He is currently an Associate Professor with the Department of Information Management at National Penghu University of Science and Technology, Taiwan. His current interests focus on information security, cryptography, Internet of Things, and medical information.

Tzer-Shyong Chen received the Ph.D. in the Department of Electrical Engineering (Computer Science) at National Taiwan University, Taiwan. He is currently a professor in the Department of Information Management at Tunghai University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.

Yu-Fang Chung received the B.A. degree in English Language, Literature and Linguistics from Providence University in 1994, the M.S. degree from Dayeh University in 2003, and the Ph.D. degree from National Taiwan University in 2007, both in Computer Science, Taiwan. She is currently a professor in the Departments of Electronic Engineering and Information Management at Tunghai University, doing research, i.e., Information Security and Cryptography.

Kuo-Kuang Huang received the M.S. degree in engineering science from National Cheng Kung University and Ed.D from University of South Dakota. He is currently a Professor with the Department of Information Management at National Penghu University of Science and Technology, Taiwan. His research interests are in the areas of artificial intelligence, information security, Internet of Things, and distance education.