A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext

Bo Meng
School of Computer, South-Center University for Nationalities, Wuhan, China
Email: mengscuec@gmail.com

Abstract—**Internet voting protocol is the base of the Internet voting systems. Firstly, an improved proof protocol that two ciphertexts are encryption of the same plaintext is introduced. Secondly, a receipt-free and coercion-resistant Internet voting protocol based on the non-interactive deniable authentication protocol and an improved proof protocol that two ciphertexts are encryption of the same plaintext is developed. Thirdly, we analyze the proposed Internet voting protocol. The proposed Internet voting protocol has the properties of universal verifiability, receipt-freeness and coercion-resistance. At the same time the proposed protocol is with the weak physical assumption. Lastly, we compare security properties of the several typical Internet voting protocols with our present protocol.**

Index Terms—**security protocol, universal verifiability, receipt-freeness, coercion-resistance, physical assumption**

I. INTRODUCTION

With the progress of society and development of democracy of nation, the needs of the voting are more and more intense. Owning to the popularity of Internet, many transactions can be processed through Internet, so the people have the higher requirements of Internet voting. Internet voting protocol is the base of the Internet voting system.

Internet voting protocol can be classified into two classes based on if they need authority. One needs not authority, such as [1]. This kind of protocol is fewer. The other needs authority, which can be categorized by different technologies into three schemes.

The first is homomorphic scheme, such as [2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17]. The voter cooperates with the authorities in order to construct an encryption of his vote. Due to the homomorphic property, an encryption of the sum of the votes is obtained by multiplying the encrypted ballots of all voters. Finally, the result of the election is computed from the sum of the votes, which is jointly decrypted by the authorities. The purposes of homomorphic encryption method are protection of the voter's privacy and advancement of the efficacy of tally ballots. Generally the homomorphic encryption scheme is not receipt-free. The first voting protocol of this scheme was introduced by Benaloh[15]. Crameret et al. protocol [4] proposed by is representative.

The second is blind signature scheme, such as [18, 19, 20, 21, 22, 23, 24, 25]. Fujioka et al. protocol [20] is representative. Generally the blind signatures scheme is not receipt-free because the blinding factor is the receipt. The voter firstly obtains a token, a blindly signed message unknown to anyone except himself. Next, the voter sends his token together with his vote. These protocols require voter's participation in more rounds. Generally the protocols need two authorities. One is administrator which responsible for issuing the ballots and generating the blind signature of ballots. The other is collector which responsible for tallying the ballot and publish the result.

The third is mix net scheme, such as [8, 13, 26, 27, 28, 29, 30, 31, 32]. These protocols use the mix net to implement the privacy. The key idea of Mix nets is to permute and modify the sequence of objects in order to hide the correspondence between elements of original and final sequence. David Chaum introduced this idea in 1981 as a realization of anonymous channel. Internet voting protocols of mix net scheme use the mix net to mix the possible ballot and send done permutations secretly to the voter.

The secure and practical Internet voting protocol should have the following properties:

Basic properties: privacy, completeness, soundness, unreusability, fairness, eligibility, and invariableness.

Expanded properties: universal verifiability, receipt-freeness [2, 18], coercion-resistance [12]

- Universal verifiability: Any one can verify the fact that the election is fair and the published tally is correctly computed from the ballots that were correctly cast.
- Receipt-freeness: The voter can not produce a receipt to prove that he votes a special ballot. Its purpose is to protect against vote buying. Receipt-freeness was introduced by Benaloh and Tuinstra [2]. They proposed a receipt-free scheme based on the voting-booth. Hirt and

Sako [8] point out that their scheme is not receipt-freeness.

❁ Coercion-resistance [12]: A coercion-resistant voting protocol should offer not only receipt-freeness, but also defense against randomization, forced-abstention, and simulation attacks.

At present the hot point is how to realize universal verifiability, receipt-freeness and coercion-resistance with few assumption or constraints. There are three traditional methods: secure multi-party computation [42], deniable encryption [38] and designated verifier proof [10, 12, 40] to implement the receipt-freeness and coercion-resistance. According to our analysis we found that the three methods in Internet voting protocol have several problems. So in this paper we apply a new method: deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext to implement the receipt-freeness and coercion-resistance.

The main contributions of this paper are summarized as follows.

1. An improved proof protocol that two ciphertexts are encryption of the same plaintext is developed.

2. A receipt-free and coercion-resistant Internet voting protocol based on non-interactive deniable authentication protocol and an improved proof protocol that two ciphertexts are encryption of the same plaintext is introduced.

Organization of the paper: In Section II the related work is discussed. An improved proof protocol that two ciphertexts are encryption of the same plaintext is proposed in Section III. In Section IV a brief overview Meng non-interactive deniable authentication protocol that is used in the proposed Internet voting protocol is presented. In Section V the secure Internet voting protocol with receipt-freeness and coercion-resistance is proposed. Then we analyze the proposed protocol in Section VI.

II. RELATED WORK

In the past a lot of Internet voting protocols uses ad hoc physical assumption to accomplish receipt-freeness and coercion-resistance, Such as, one or two-way untappable channels and/or anonymous or private channels [5, 8, 12, 18, 26], third-party honest verifiers [35], smartcards [29], voting booth [2, 33], the third randomizer [5, 13, 34] ,tamper-resistant randomizer [9].

At present the hot point is how to realize universal verifiability, receipt-freeness and coercion-resistance with few physical assumptions. There are three traditional methods: secure multi-party computation [42], deniable encryption [38] and designated verifier proof [10, 12, 40] to implement the receipt-freeness and coercion-resistance.

Zhong et al. [42] use secure multi-party computation to implement the receipt-freeness. But in Zhong et al. protocol the voter need to involve the all phase, which is not comfortable for the voter's experience. At the same time it uses the secure channel to implement the receipt-freeness, which is a very strong physical assumption.

Rja¡¦skov´a [38] uses the deniable encryption to implement the receipt-freeness. Because deniable encryption is only process one bit in each run this method can not support the other voting ballot forms. Such as chose one from many, write in ballot.

Juels et al. [12] researched coercion-resistance firstly. Acquisti protocol[10] applies the idea of Juels et al. [12]. Juels et al. [12] and Acquisti [10] mainly applied the credential of voter and designated verifier proof to accomplish it. Voter can cheat the coercer by producing a false credential. Owning to designate verifier proof the coercer can not verify the proof.

The key idea of Juels [12] is that for the identity of a voter to remain hidden during the election process and for the validity of ballots instead to be checked blindly against a voter roll. When casting a ballot, a voter incorporates a concealed credential. This takes the form of a ciphertext on a secret value that is unique to the voter. The secret value is a kind of anonymous credential. To ensure that legitimate voters cast ballots, the tallying authority performs a blind comparison between hidden credentials and a list of encrypted credentials published by an election registrar alongside of the plaintext names of registered voters.

According to our analysis we found that it has the following problems: (1) can not prevent the "1009 attacks"; (2) do not defense against forced-abstention and simulation attacks ;(3) can not support write in ballot.

In Acquisti protocol [10] the election authorities provide shares of credentials to each voter, along with designated verifier proofs of each share's validity. Using homomorphic encryption, the voter assembles the shares and combines them with her own vote that is cast on a public bulletin board. All messages in the bulletin board can be decrypted by a coalition of the election authorities after the voting phase of the election is completed.

But according to our analysis of Acquisti protocol [10], we find that it has the following problems:

a. It is not invariableness.

In Acquisti protocol the voter can use per credential to vote many times. In other words the voter can use per credential to vote the same ballot many times and also can use per credential to vote different ballot many times. In the tallying phrase the author only deals with the status that the voter can use per credential to vote the same ballot many times. The other status that voter can use per credential to vote different ballot many times does not be considered. So on that status we use the search algorithm in the tallying phrase, the tally result may be different. So it is not property of invariableness. This is an important problem.

b. It is not receipt-freeness and coercion-resistance.

According to the definition of coercion-resistance we know that if an Internet protocol is not receipt-free, it is not coercion-resistant. So we firstly point that Acquisti protocol is not receipt-freeness.

In Acquisti protocol $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ is send by the authority through a trappable channel. That means the vote buyer can get $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ and know that it is

send by the authority. E^{v_j} represents RSA encryption under v_j's public key.

The voter can prove that $E^V\left(c_{i,j}\right), P_{v_j}$ is the decryption of $E^{v_j}\left(E^V\left(c_{i,j}\right), P_{v_j}\right)$ with the public key of v_j and the property of RSA encryption. $E^S\left(E^V\left(C_j + B_j^t\right)\right)$ is published on the bulletin board. Generally voter can successfully verify the designated verifier proof P_{v_j} of equality between $E^V\left(c_{i,j}\right)$ and the corresponding $E^C\left(c_{i,j}\right)$. So the voter can reveal how to generate the vote $E^S\left(E^V\left(C_j + B_j^t\right)\right)$ that is compatible with the receipt $E^S\left(E^V\left(C_j + B_j^t\right)\right)$ and $E^{v_j}\left(E^V\left(c_{i,j}\right), P_{v_j}\right)$. So Acquisti protocol is not receipt-freeness.

According to the definition of coercion-resistance Acquisti protocol is not coercion-resistance.

Meng protocol [40] is a practical and efficient Internet voting protocol with the secure properties and addresses the problems of Acquisti protocol. At the same time Meng protocol has the following specialties:(1)Have the properties of privacy, completeness, soundness, fairness, invariableness, universal verifiability, receipt-freeness and coercion-resistance;(2) Without of strong physical assumption;(3) Solve the problems that have not property of invariableness, can not prevent the "1009 attacks" and application of the tappable channel in Acquisti protocol.

In this paper we apply a new method, which is deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext, to implement receipt-freeness and coercion-resistance.

Deniable authentication protocol allow a sender to authenticate a message for a receiver, in a way that the receiver can not convince a third party that such authentication (or any authentication) ever took place. Deniable authentication has two characteristics that differ from traditional authentication:

1. Only the intended receiver can authenticate the true source of a given message.
2. The receiver can't prove the source of the message to a third party.

In the past the deniable authentication protocol has been studied. The deniable authentication protocol can be fall into two categories: interactive deniable authentication protocols and non-interactive deniable authentication protocols [41, 43, 44, 45, 46, 47, 48]. The interactive deniable authentication protocols are inefficient. Hence research on non-interactive deniable authentication protocols is the future direction. All the protocols [41, 43, 44, 45, 46, 47, 48] have not strong deniability. Meng non-interactive deniable authentication protocol [41] based on discrete logarithm problem has secure properties: completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack, and security of man-in-the-middle attack.

To our knowledge the research on the proof protocol that two ciphertexts are encryption of the same plaintext is at the beginning. Baudron et al. [5] proposed an interactive proof protocol based on paillier cryptosystem. Acquisti [10] applied the idea of Baudron et al and proposed an interactive proof protocol based on paillier cryptosystem with the condition p=2. Goulet et al.[11] proposed an interactive protocol based on ElGamal cryptosystem. But we found that Goulet et al' proof protocol is wrong. We give an improved proof protocol that two ciphertexts are encryption of the same plaintext.

So we use Meng non-interactive deniable authentication protocol and an improved proof protocol that two ciphertexts are encryption of the same plaintext to implement the receipt-freeness and coercion-resistance.

III. An Improved Proof Protocol That Two Ciphertexts Are Encryption of the Same Plaintext

To our knowledge the research on the proof protocol that two ciphertexts are encryption of the same plaintext is at the beginning. Baudron et al. [5] proposed an interactive proof protocol based on paillier cryptosystem. Acquisti [10] applied the idea of Baudron et al. and proposed an interactive proof protocol based on paillier cryptosystem with the condition p=2. Goulet et al. [11] proposed an interactive protocol based on ElGamal cryptosystem. But we found that Goulet et al.' proof protocol is wrong. In the following we address the problem of Goulet et al. and give an improved proof protocol that two ciphertexts are encryption of the same plaintext:

In the protocol we need two public and private keys: $(p, g, h_V), \alpha_V, h_V = g^{\alpha_V}$; $(p, g, h_C), \alpha_C, h_C = g^{\alpha_C}$,g is a generator of multiplicative $\mathbb{Z}_p^*$.

Prover proves to the verifier that $(x_V, y_V) = (g^{r_V}, h_V^{r_V} m)$ and $(x_C, y_C) = (g^{r_C}, h_C^{r_C} m)$ are the ciphertexts of the same m with the public key (p, g, h_V) and (p, g, h_C). At the same time prover does not tell verifier r_V, r_C.

- Prover computes:

$(x_V, y_V) = (g^{r_V}, h_V^{r_V} m), (x_C, y_C) = (g^{r_C}, h_C^{r_C} m)$

$r \in \mathbb{Z}_p, (x_1, y_1) = (g^r, h_V^r m), (x_2, y_2) = (g^r, h_C^r m)$

$a_1 = \frac{x_V}{x_1}, a_2 = \frac{x_1}{x_2}, a_3 = \frac{x_2}{x_C}$

$b_1 = \frac{y_V}{y_1}, b_2 = \frac{y_1}{y_2}, b_3 = \frac{y_2}{y_C}$

sends $(a_1, a_2, a_3, b_1, b_2, b_3)$ to verifier

- Verifier checks:

$a_1 a_2 a_3 \stackrel{?}{=} \frac{x_V}{x_C}, b_1 b_2 b_3 \stackrel{?}{=} \frac{y_V}{y_C}$

Verifier selects a random value c from $c \in \{0,1,2\}$ the set and sends c to the prover.

❁ Prover computes:

If: $\begin{cases} c=0,\ prove\ \log_g a_1 = \log_{h_V} b_1 \\ c=1,\ prove\ \log_g a_2 = \log_{\frac{h_V}{h_C}} b_2 \\ c=2, prove\ \log_g a_3 = \log_{h_C} b_3 \end{cases}$

sends to verifier.

If we repeat the above procedure z times, we see that a lying prover only succeeds with a probability of $\left(\frac{2}{3}\right)^Z$,which is a probability that shrinks quickly if we repeat enough times. Thus, the verifier can be sure with a large probability that the plaintext equivalence is true after a number of run of this proof.

IV. An Overview of Meng Non-Interactive Deniable Authentication Protocol

Meng non-interactive deniable authentication protocol is the secure and has properties: completeness, strong deniability, weak deniability, security of forgery attack, security of impersonate attack, security of compromising session secret attack, and security of man-in-the-middle attack.

❁ Strong deniability [49]: After execution of the deniable authentication protocol the sender can deny to have ever authenticated anything to receiver.

❁ Weak deniability [49]: The deniable authentication protocol is deniable. The receiver can prove to have spoken to the sender but not the content of what the sender authenticated in a way that the receiver can't convince a third party that such authentication.

Meng protocol supposes that the attacker can not monitor the communication between the sender and receiver in the non-interactive deniable authentication protocol.

Meng non-interactive deniable authentication protocol is briefly described as the following:

❁ Initialized phrase

The Authority chooses a large prime numbers p, and computes a random multiplicative generator element g in finite field of p elements: GF (p). Lastly he sends the g, p to the bullet board.

The sender picks a serial random numbers $r_i \in {}_U Z_{p-1}$ $S^i_{PR} = r_i \quad i = 1 \cdots\cdots l$, and computes his public key by $S^i_{PU} = g^{r_i} \pmod p \quad i = 1 \cdots\cdots l$ .Lastly, sender sends the S^i_{PU} to the bullet board.

The receiver picks a random numbers $x \in {}_U Z_{p-1}$ $R_{PR} = x$, and computes his public key by $R_{PU} = g^x \pmod p$ .Lastly, the sender sends the R_{PU} to the bullet board.

When finishing the initialized phrase the sender has serial public and private keys $\left(S^i_{PU}, S^i_{PR}\right)$, at the same time receiver has his public and private keys $\left(R_{PU}, R_{PR}\right)$

Hash (m) is a collision-free hash function with an input of m and output of q bits:q= Hash (m)

❁ Execution of protocol phrase

M is the message sent to the receiver.

Sender performs:

(1) Chooses randomly a public and private key $\left(S^t_{PU}, S^t_{PR}\right)$ .the private and public keys of each run of the propose protocol are different.

(2) Computes: $\delta = hash(m) S^t_{PR} \bmod q$ and forgets $\left(S^t_{PU}, S^t_{PR}\right)$ after a certain time. $k = \left(R_{PU}\right)^{\delta} \bmod p$ $hash\left(k \,||\, m\right) = MAC$ and sends $\left(S^t_{PU}, MAC, m\right)$ to the receiver.

Receiver computes:

(1) $k' = \left[\left(S^t_{PU}\right)^{hash(m)}\right]^{R_{PR}} \bmod p$

(2) Verifies $hash\left(k' \,||\, m\right) \stackrel{?}{=} MAC$ .if the result is true, the receiver accepts it. Otherwise the receiver rejects it.

The proof of security can be found in Ref. [41]

V. The Proposed Secure Internet Voting Protocol

The idea of the proposed secure Internet voting protocol with receipt-freeness and coercion-resistance is that: if everyone knows that the voter has the ability that generates the fake evidence, when the voter provides the evidence to the vote-buyer, the voter-buyer has not the ability to verify the evidence, so the vote-buyer does not give the money to the voter. So the proposed Internet voting protocol has receipt-freeness and against of and randomization attack.

How to make the voter to have ability that generates the fake evidence? Owning to the strong deniability of Meng non-interactive deniable authentication protocol we can use it to implement the ability.

The proposed Internet voting protocol applies the encryption technologies which include threshold ElGamal cryptosystem, mix net [27, 36], homomorphic encryption, Meng non-interactive deniable authentication protocol and the improved proof protocol that knowledge that two ciphertexts are encryption of the same plaintext.

A. The protocol

The proposed Internet voting protocol includes four phases: preparation phase, registration phase, voting phase and tallying phase.

❁ Notation definition

BB:bulletin board;

$A_i (i = 1, 2, \cdots, s)$: the ith authority;

$V_j (j = 1, 2, \cdots, l)$: the jth legal voter;

B^t : ballot voted t;

$c_{i,j}, j = 1, \cdots, l, i = 1, \cdots, d$: A_i creates the random number for V_j . It is the credential share of Vj.;

C_j : credential V_j ;

$PK^C, SK_i^C, VK^C, VK_i^C$: the threshold cryptosystem of A_i ,which is used to encrypt and decrypt $c_{i,j}$;

$PK^V, SK_i^V, VK^V, VK_i^V$: the threshold cryptosystem of A_i ,which is used to encrypt and decrypt B^t and $c_{i,j}$;

PK_i, SK_i : the public key and private key of A_i ,which is used when voter register;

PK_j, SK_j : the public key and private key of Vj;

$E^V(m)$: encrypt m with PK^V ;

$E^C(m)$: encrypt m with PK^C ;

$SK(m)$: sign m with private key SK ;

ϕ : mix operation;

$HASH(m)$: the value of HASH functions with m;

$ENV_{PK}(m)$: digital envelope of m with the public key PK ;

Identj: identification of V_j ;

$Proof_{V_j}^{A_i}$: the non-interactive deniable proof evidence of knowledge that and $E^V(c_{i,j})$ are encryption of the same $c_{i,j}$, which is produced by A_i for V_j .

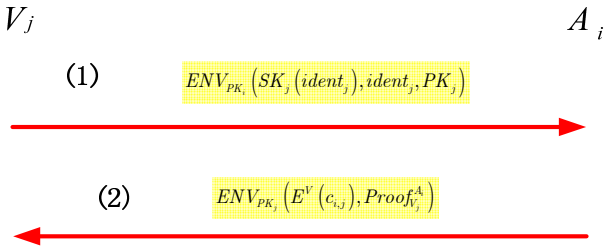

Figure 1. Registration phase.

❁ Preparation phase

Authorities and voters generate the public/private ElGamal keys. The private keys of voter and authorities are secret

Authorities generate the ballot B^t and send B^t and its digital signature to bulletin board denoted by BB.

❁ Registration phase

(1) Firstly voter V_j generates $ident_j$, secondly generates message $ENV_{PK_i}(SK_j(ident_j), ident_j, PK_j)$ and send it to the authority A_i . Authority A_i receives the message and uses its private key to open the digital envelope. Authority A_i checks $ident_j$ that if it has registered. If it has registered, Authority A_i sends the error message to V_j . The protocol ends. If it has not registered, Authority A_i verifies $SK_j(ident_j)$. If the verification is wrong, Authority A_i sends the error message to V_j , the protocol ends. If the verification is right, Authority A_i execute (2) step.

(2) Authority A_i firstly generates $E^V(c_{i,j})$, secondly generates $Proof_{V_j}^{A_i}$ based on Meng non-interactive deniable protocol and the improved proof protocol that knowledge that two ciphertexts are encryption of the same plaintext with ElGamal cryptosystem. Lastly Authority A_i generates $ENV_{PK_j}(E^V(c_{i,j}), Proof_{V_j}^{A_i})$. Authority A_i sends PK_j to other authorities. Other authorities generate $ENV_{PK_j}(E^V(c_{i,j}), Proof_{V_j}^{A_i})$ $(i=1,\cdots,i-1,i+1\cdots,s)$ at the same method. Authority A_i gets $ENV_{PK_j}(E^V(c_{i,j}), Proof_{V_j}^{A_i})$ $(i=1,\cdots,i-1,i+1\cdots,s)$ and sends $ENV_{PK_j}(E^V(c_{i,j}), Proof_{V_j}^{A_i})$ $(i=1,\cdots,i,\cdots,s)$ to voter V_j by anonymous channel. Authority A_i generates $(E^C(c_{i,j}))SK_{A_i}$, and sends $E^C(c_{i,j})$ and $(E^C(c_{i,j}))SK_{A_i}$ $(i=1,\cdots,i,\cdots,s)$ to BB. Voter V_j receives $Proof_{V_j}^{A_i}$ and verifies it. If it is right, V_j generates

$$\prod_{j=j,i=1,\cdots,s}(E^V(c_{i,j})) = E^V\left(\prod_{j=j,i=1,\cdots,s} c_{i,j}\right) \equiv E^V(C_J)$$

❁ Voting phase

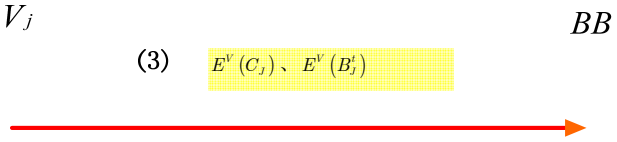

Figure 2. Voting phase

V_j chooses one ballot and generate $E^V(B_J^t)$ and send $E^V(C_J), E^V(B_J^t)$ to Table Ⅰ randomly in BB.

❁ Tallying phase

(1) According to the rules the authorities eliminate the duplicate $E^V(C_J)$ and its corresponding $E^V(B_J^t)$ in Table I. The results store in Table II.

(2) Authority mixes $E^C(C_J)$ in table III and $E^V(C_J), E^V(B_J^t)$ in table II. The corresponding results are $E^C(C_{\phi(J)})$ and $E^V(C_{\phi(J)})$, $E^V(B_{\phi(J)}^t)$. Authority stores $E^C(C_{\phi(J)})$ in Table IV and $E^V(C_{\phi(J)}), E^V(B_{\phi(J)}^t)$ in Table V.

(3) Authorities decrypt $E^C(C_{\phi(J)})$ in Table IV and $E^V(C_{\phi(J)})$ in Table V. In order to verify correctness of decryption by people, authority stores the proof of correctness of decryption in Table IV and Table V respectively.

(4) According to $C_{\phi(J)}$ in Table IV, authority finds $E^V\left(B^t_{\phi(J)}\right)$ in Table V which is corresponding to $C_{\phi(J)}$ that is equal to $C_{\phi(J)}$ in Table IV. Authority stores $E^V\left(B^t_{\phi(J)}\right)$ in Table VI.

(5) Authorities decrypt $E^V\left(B^t_{\phi(J)}\right)$ in Table VI and get $B^t_{\phi(J)}$. The proof of correctness of decryption is stored in Table VI.

(6) Authority tallies the ballot in Table VI and stores its results in Table VI.

TABLE I. BALLOTS BEFORE TALLYING

$E^V\left(C_J\right)$	$E^V\left(B^t_J\right)$

TABLE II. BALLOT ELIMINATED THE DUPLICATE $E^V\left(C_J\right)$ AND ITS CORRESPONDING $E^V\left(B^t_J\right)$

$E^V\left(C_J\right)$	$E^V\left(B^t_J\right)$

TABLE III. THE $E^C\left(C_J\right)$

$E^C\left(C_J\right)$

TABLE IV. THE $E^C\left(C_{\phi(J)}\right)$

$E^C\left(C_{\phi(J)}\right)$	Proof of correctness of decryption	$C_{\phi(J)}$

TABLE V. THE $E^V\left(C_{\phi(J)}\right)$ AND $E^V\left(B^t_{\phi(J)}\right)$

$E^V\left(C_{\phi(J)}\right)$	Proof of correctness of decryption	$C_{\phi(J)}$	$E^V\left(B^t_{\phi(J)}\right)$

TABLE VI. THE $E^V\left(B^t_{\phi(J)}\right)$

$E^V\left(B^t_{\phi(J)}\right)$	proof of correctness of decryption	$B^t_{\phi(J)}$

TABLE VII. THE RESULT TABLE

t	
1	
⋮	
t	

VI. PROPERTIES ANALYSIS

Owning to the space limitation we only analysis universal verifiability, receipt-freeness, coercion-resistance.

- Universal verifiability

Anyone can verify the tallying results according the message in BB. Each step in tallying phase is public and can be verified.

Voter can check that their ballot $E^V\left(C_J\right)$ and $E^V\left(B^t_J\right)$ do appear on BB. If voter does not vote repeatedly, his ballot must appear in table 2. After mixing, voter can not recognize its ballot. But voter can check correctness of the mix operation by proof provided by mix server.

Voter can check correctness of decryption of $E^C\left(C_{\phi(J)}\right)$ in table 4, $E^V\left(C_{\phi(J)}\right)$ in table 5 and $E^V\left(B^t_{\phi(J)}\right)$ in table 7 owning to threshold ElGamal cryptosystem.

So the proposed Internet voting protocol is universal verifiability.

- Receipt-freeness

The proposed Internet voting protocol accomplishes receipt-freeness by confidentiality of voter credential and the proposed deniable authentication protocol.

Voter checks equality between credential from authority and credential in BB by proof protocol that knowledge that two ciphertexts are encryption of the same plaintext $Proof^A_{V_j}$. Other peoples can not check owning to the specialty of the meng deniable authentication protocol. According to the Meng deniable authentication protocol voter has the ability of generation of a fake $Proof^A_{V_j}$. The vote-buyer can't check $ENV_{PK_j}\left(E^V\left(c_j\right), Proof^A_{V_j}\right)$ and can't verify $E^V\left(c_j\right)$. So the vote-buyer does not give the money to the voter.

So the protocol is receipt-freeness.

- Coercion-resistance

According to definition of coercion-resistance, firstly the protocol is receipt-freeness, and then prevents randomization attack, forced-abstention attack and simulation attack.

We have already analyzed that it is receipt-free. In the following we analyze that it can prevent randomization attack, Forced-abstention attack and simulation attack.

(1) Randomization attack

Voter wants to prevent randomization attack. He can generate a false credential to cheat coercer because coercer can not recognize it true or false. Then voter can use true credential to vote a ballot. So the protocol can prevent randomization attack.

(2) Forced-abstention attack

According to protocol coercer can not know if voter has registered based on BB and if voter has vote. So the protocol can prevent Forced-abstention attack.

(3) Simulation attack

Coercer can vote on voter behalf after getting private key of voter. But we suppose that the private key of voter is secret in our protocol. So the protocol can prevent simulation attack.

VII. CONCLUSION

Internet voting protocol is base of Internet voting system. In this paper Firstly, an improved proof protocol that two ciphertexts are encryption of the same plaintext is introduced. Secondly, a receipt-free and coercion-resistant Internet voting protocol based on non-interactive deniable authentication protocol and an improved proof protocol that two ciphertexts are encryption of the same plaintext is developed. Thirdly, we analyze the proposed Internet voting protocol. The proposed Internet voting protocol has the properties of universal verifiability, receipt-freeness and coercion-resistance and do not use the strong physical assumptions. Fourth, we compare security properties of Fujioka et al. [20], Cramer et al. [4], Juels et al. [12], Acquisti [10] protocols with our present protocol. Owning to the space limitation we only give the analyzed result described as in Table VIII.

In the future we will use the protocol analyzer ProVerif [50] based on the applied pi calculus to analyze the universal verifiability, receipt-freeness and coercion-resistance properties of the proposed Internet voting protocol. At the same time we will develop an Internet voting system based on our proposed protocol.

TABLE VIII. COMPARING SECURITY PROPERTIES OF THE EARLIER SEVERAL TYPICAL PROTOCOLS WITH OUR PRESENT PROTOCOL. THE MARK"**T**" REPRESENTS THE PROTOCOL HAS THE PROPERTY; THE MARK"**F**"REPRESENTS HAS NOT THE PROPERTY

Properties	Fujioka et al. [20]	Cramer et al. [4]	Juels et al. [12]	Acquisti. [10]	Our present
Privacy	**T**	**T**	**T**	**T**	**T**
Completeness	**T**	**T**	**T**	**T**	**T**
Soundness	**T**	**T**	**T**	**T**	**T**
Unreusability	**F**	**F**	**F**	**F**	**T**
Fairness	**T**	**T**	**T**	**T**	**T**
Eligibility	**T**	**F**	**F**	**F**	**T**
Invariableness	**T**	**T**	**T**	**F**	**T**
Universal verifiability	**T**	**T**	**T**	**T**	**T**
Receipt-freeness	**F**	**F**	**T**	**F**	**T**
Coercion-resistance	**F**	**F**	**F**	**F**	**T**
Homomorphic scheme	**F**	**T**	**F**	**T**	**T**
Blind signature scheme	**T**	**F**	**F**	**F**	**F**
Mix net scheme	**F**	**F**	**T**	**T**	**T**
Designated verifier proof	**F**	**F**	**T**	**T**	**F**
Deniable authentication protocol	**F**	**F**	**F**	**F**	**T**

REFERENCES

[1] R. A. DeMillo, N. A. Lynch, M. Merritt, "Cryptographic Protocols," In *Proceeding of 14th Annual ACM Symposium on Theory of Computing*, pp.383-400, 1982.

[2] Josh Benaloh and Dwight Tuinstra, "Receipt-free secret-ballot elections," In *Proceeding of STOC '94*, pp.544–553. 1994.

[3] Ronald Cramer, Matthew Franklin, Berry Schoenmakers, Moti Yung, "Multi-authority secret ballot elections with linear work," In *Proceeding of EUROCRYPT '96*, LNCS1070,pp.72–83,1996.

[4] Ronald Cramer, Rosario Gennaro, Berry Schoenmakers, "A secure and optimally efficient multi-authority election scheme," In *Proceeding of EUROCRYPT '97*, LNCS 1233, pp.103–118, 1997.

[5] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Guillaume Poupard, Jacques Stern, "Practical multi-candidate election system," In *Proceeding of PODC '01*, ACM, pp.274–283, 2001.

[6] Ivan Damg°ard and Mads Jurik, "A generalisation, a simplification and some applications of paillier'sprobabilistic public-key system," In *Proceeding of Public Key Cryptography '01*, LNCS 1992, pp.119–136, 2001.

[7] Ivan Damg°ard, Mads Jurik, Jesper Buus Nielsen, "A generalization of paillier's public-key system with applications to electronic voting," *http://www.daimi.au.dk/~ivan/GenPaillier_finaljour.ps*, 2003.

[8] Martin Hirt and Kazue Sako, "Efficient receipt-free voting based on homomorphic encryption," In *Proceeding of EUROCRYPT '00*, LNCS 1807,pp.539–556,2000.

[9] Byoungcheon Lee and Kwangjo Kim, "Receipt-free electronic voting scheme with a tamperresistant randomizer," In *Proceeding of ICISC2002*, pp.405–422,2002.

[10] Alessandro Acquisti, "Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots," *Technical Report 2004/105*, CMU-ISRI-04-116, 2004.

[11] Jonathan Goulet and Jeffrey Zitelli, "Surveying and Improving Electronic Voting Schemes,"*http://www.seas.upenn.edu/~cse400/CSE400_2004_2005/senior_design_projects_04_05.htm.*

[12] Ari Juels and Markus Jakobsson, "Coercion-resistant electronic elections," *http://www.vote-auction.net/VOTEAUCTION/165.pdf*,2002.

[13] Martin Hirt, "Multi-party computation: Efficient protocols, general adversaries, and voting," *PhD Thesis*, ETH Zurich, 2001.

[14] Ari Juels, Dario Catalano, Markus Jakobsson, "Coercion-resistant electronic elections," *http://www.rsasecurity.com/rsalabs/node.asp?id=2030* as of June 2005.

[15] Josh C. Benaloh,"Verifiable secret-ballot elections," *PhD Thesis*, Yale University, Department of Computer Science,. Number 561, 1987

[16] Kazue Sako and Joe Kilian, "Secure voting using partial compatible homomorphisms," In *Proceedings of CRYPTO'94*, LNCS 839, pp.248–259, 1994.

[17] David Chaum, "Secret-ballot receipts and transparent integrity,"*http://www.enhyper.com/content/SecretBallotReceipts.pdf*. 2002.

[18] Tatsuaki Okamoto, "Receipt-free electronic voting schemes for large scale elections," In *Proceeding of Security Protocols Workshop*, LNCS 1361, pp.25–35, 1997.

[19] David Chaum, "Elections with unconditionally- secret ballots and disruption equivalent to breaking rsa," In *Proceeding of EUROCRYPT '98*, LNCS 330, pp.177–182, 1988.

[20] Atshushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta, "a practical secret voting scheme for large scale elections," In *Proceeding of Auscrypt '92*, LNCS 718, pp.244–251,1992.

[21] Michael J. Radwin, "An untraceable, universally verifiable voting scheme," *http://www.radwin.org/michael/projects/voting.html*

[22] Wen-Sheng Juang, Chin-Laung Lei, Pei-Ling Yu, "A verifiable multi-authorities secret elections allowing abstaining from voting," Computer Journal 45(6),pp.672-682, 2002.

[23] Patrick Horster, Markus Michels, Holger Petersen, "Blind multisignature schemes and their relevance to electronic voting," In *Proceeding of 11th Annual Computer Security Applications Conference.* IEEE Press, pp149–156, 1995.

[24] Lorrie Cranor and Ron Cytron, "Sensus: A security-conscious electronic polling system for the Internet," In *Proceedings of the 30th Hawaii International Conference on System Sciences,* pp.561, 1997.

[25] Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, Tatsuaki Okamoto, "An improvement on a practical secret voting scheme," In *Proceedings of ISW '99,* pp.225–234, 1999.

[26] Kazue Sako and Joe Kilian, "Receipt-free mix-type voting scheme," In *Proceeding of EUROCRYPT '95*, LNCS 921,pp.393–403,1995.

[27] Choonsik Park, Kazutomo Itoh, Kaoru Kurosawa, "Efficient anonymous channel and all/nothing election scheme," In *Proceeding of Advances Cryptology - EUROCRYPT'93*, pp.248–259, 1993.

[28] Markus Jakobsson, Ari Juels, Ronald L. Rivest, Making mix nets robust for electronic voting by randomized partial checking, In *Proceeding of USENIX '02*, 2002,pp.339–353.

[29] Emmanouil Magkos, Mike Burmester,Vassilios Chrissikopoulos, "Receipt-freeness in large-scale elections without untappable channels," In *Proceeding of I3E*, pp.683–694,2001.

[30] Birgit Pfitzmann, "Breaking an efficient anonymous channel," In *Proceedings of EUROCRYPT '94*. LNCS 950, pp.332–340,1995.

[31] Markus Michels , Patrick Horster, "Some remarks on a receipt-free and universally verifiable mix-type voting scheme," In *Proceedings of ASIACRYPT '94*, LNCS 1163, pp.125–132,1996.

[32] Masayuki Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers," In *Proceedings of EUROCRYPT '98*, LNCS 1403, pp.437–447, 1998.

[33] Andrew Neff, "Detecting malicious poll site voting clients," *http://votehere.com/vhti/documentation/psclients.pdf*, 2003.

[34] Aggelos Kiayias and Moti Yung, "The vector-ballot e-voting approach," *http://theory.lcs.mit.edu/~rivest/voting/papers/KiayiasYung-TheVectorBallotEVotingApproach.pdf.*

[35] Byoungcheon Lee and Kwangjo Kim, "Receipt-free electronic voting through collaboration of voter and honest verifier," *http://citeseer.nj.nec.com/lee00receiptfree.html*, 2000.

[36] David Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, 24(2),pp. 84–88 , 1981.

[37] Markus Jakobsson, Kazue Sako, Russell Impagliazzo, "Designated verifier proofs and their applications," In *Proceeding of EUROCRYPT '96*, LNCS 1070, pp.143–154, 1996.

[38] Zuzana Rja¡¦skov´a, "Electronic Voting Schemes," *Master thesies,*omenius University, Bratislava, April 2002.

[39] G.R. Blakley, "Safeguarding cryptographic keys," In *Proceedings of AFIPS Conference*, 48, 1979, pp.313-317.

[40] Bo Meng, "An Internet Voting Protocol With Receipt-free and Coercion-resistant," In *Proceedings of IEEE 7th International Conference on Computer and Information Technology*, Japan, pp.721-726, October 16 to 19, 2007

[41] Bo Meng, "A Secure Non-Interactive Deniable Authentication Protocol with Strong Deniability Based on Discrete Logarithm Problem and its Application on Internet Voting Protocol," *Information Technology Journal* , 8(3),pp.302-309, 2009.

[42] Hong zhong, Liusheng Huang, Yonglong Luo, "A Multi-Candidate Electronic Voting Scheme Based on Secure Sum Protocol," *Journal of Computer Research and Development*, 43(8).pp.1405-1410,2006.

[43] Shao, Z., "Efficient deniable authentication protocol based on generalized ElGamal signature scheme," *Computer Standards & Interfaces* 26 (5),pp.449–454, 2004

[44] Lee,W.B., Wu,C.C., Tsaur, W.J., "A novel deniable authentication protocol using generalized ElGamal signature scheme," *Information Sciences*, 177(6), pp.1376-1381,15 March 2007.

[45] Lu, R., Cao, Z., "A new deniable authentication protocol from bilinear pairings," *Applied Mathematics and Computation* 168 (2) ,pp.954–961,2005

[46] Lu, R., Cao, Z.,. "Non-interactive deniable authentication protocol based on factoring," *Computer Standards & Interfaces* 27 (4) ,pp.401–405,2005.

[47] Qian, HF, Cao ZF, Wang LC, Xue QS, "Efficient Non-interactive Deniable Authentication Protocols", In *Proceeding of Fifth International Conference on Computer and Information Technology*, pp.673-679,2005.

[48] Shi, Y.and Li, J., "Identity-based deniable authentication protocol," *ELECTRONICS LETTERS*, 41(5),pp.241-242, 3rd March 2005.

[49] Raimondo, MD.and Gennaro, R, "New approaches for deniable authentication," In *Proceedings of the 12th ACM Conf. on Computer and Communications Security*. New York: ACM Press, pp.112−121, 2005.

[50] Bruno Blanchet, "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules," In *Proceedings of the 14th IEEE WCSF*, Canada, pp.82-96, June 11-13, 2001.

Bo Meng was born in 1974 in People's Republic of China. He received his M.S. degree in computer science and technology, Ph.D. degree in traffic information engineering and control from Wuhan University of Technology, at Wuhan, People's Republic of China, in 2000, 2003, respectively. From 2004 to 2006, he works in Wuhan University, People's Republic of China as Postdoctoral researcher in information security.

Currently he is an Associate Professor of school of computer, South-Center University for Nationalities, in People's Republic of China. He has authored/coauthored over 40 papers in International/National journals and conferences. His current research interests include electronic commerce, internet voting, and protocol security.