A Receipt-free Coercion-resistant Remote Internet Voting Protocol without Physical Assumptions through Deniable Encryption and Trapdoor Commitment Scheme

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

Zimao Li and Jun Qin
School of Computer, South-Center University for Nationalities, Wuhan, China
Email: {lizm@sdu.edu.cn, wrj_qj@hotmail.com}

***Abstract*—The secure remote Internet voting protocol play an important role in Internet voting system. The direction of development of remote Internet voting protocol is that implementation of receipt-freeness and coercion-resistance is from with strong physical assumptions to with weak physical assumptions. The final purpose is that receipt-freeness and coercion-resistance is implemented without physical assumptions. In this paper firstly, a receipt-free coercion-resistant remote Internet voting protocol based on MW deniable encryption scheme and BCP commitment scheme is developed. To our best knowledge the proposed remote Internet voting protocol, which has receipt-freeness and coercion-resistance, is the first remote Internet voting protocol implemented without physical assumptions. Secondly, we analyze receipt-freeness and coercion-resistance of the proposed remote Internet voting protocol. Finally, we compare security properties of several typical protocols with our present protocol.**

***Index Terms*—physical assumptions, remote Internet voting, deniable encryption, trapdoor commitment scheme, protocol security**

I. INTRODUCTION

With the progress of society and development of democracy of nation, people can use the election to express their opinions. Owning to the popularity of Internet and information technology, many traditional transactions are processed through Internet. People may want to use the personal computer at their home to vote in election, which is called remote Internet voting. Thus the secure remote Internet voting system plays an important role in remote Internet voting. The secure Internet voting protocol is the base of the remote Internet voting system.

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

- Basic properties: privacy, completeness, soundness, unreusability, fairness, eligibility, and invariableness.
- Expanded properties: universal verifiability, receipt-freeness[1,2], coercion-resistance [3]

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. Notion of receipt-freeness was introduced by Benaloh and Tuinstra [1]. They propose a receipt-free scheme with strong physical assumptions: voting-booth. Hirt and Sako in [4] point out that their scheme is not receipt-free.

Coercion-resistance: A coercion-resistant voting protocol should offer not only receipt-freeness, but also it can prevent randomization attack, forced-abstention attack and simulation attack.

The direction of development of remote Internet voting protocol is implementation of receipt-freeness and coercion-resistance without physical assumptions and constraints. The final purpose is that receipt-freeness and coercion-resistance is implemented without physical assumptions. People have developed a lot of Internet voting protocols with receipt-freeness and coercion-resistance. But according to our analysis we found that the weakest physical assumption among implementations of receipt-freeness and coercion-resistance is one way anonymous channel. To our best knowledge up to now the remote Internet voting protocol with receipt-freeness and coercion-resistance implemented without physical assumptions does not exist. Motivated by this in this paper we apply deniable encryption and trapdoor commitment scheme to implement the receipt-freeness and coercion-resistance in the remote Internet voting protocol without physical assumptions.

The main contributions of this paper are summarized as follows.

- A receipt-free coercion-resistant remote Internet voting protocol is introduced.

Corresponding author: Bo Meng, School of Computer, South-Center University for Nationalities, Wuhan, China, 430074

This work was supported by National Natural Science Foundation of China （ 60603008 ） and Natural Science Foundation of Hubei Province (2007ABA342)

© 2010 ACADEMY PUBLISHER
doi:10.4304/jsw.5.9.942-949

- Implemented receipt-freeness and coercion-resistance without physical assumptions and constraints
- Based on deniable encryption scheme and trapdoor commitment scheme.

Organization of the paper: In section II related works is discussed. The related cryptographic primitives are introduced in section III. In section IV the remote Internet voting protocol with receipt-freeness and coercion-resistance implemented without physical assumptions and constraints, is proposed. Then we analyze the proposed protocol in section V.

II .RELATED WORKS

The direction of development of remote Internet voting protocol is that implementation of receipt-freeness and coercion-resistance is from with strong physical assumptions to with weak physical assumptions. The final purpose is that receipt-freeness and coercion-resistance is implemented without physical assumptions [34].

In the past a lot of Internet voting protocols have used strong physical assumptions to accomplish receipt-freeness and coercion-resistance. For example, voting booth[1,5,6,7,8]; untappable private channel[9,10]; secret communication channel and smartcard[11]; visual cryptography[5,6]; tamper resistant randomizer[12]; secure channel[13];etc.

Several Internet voting protocols have been proposed with weak physical assumptions in recent years. To our best knowledge the weakest physical assumptions among implementations of receipt-freeness and coercion-resistance is one way anonymous channel.

Juels and Jakobsson [3] firstly address the problem of achieving receipt-freeness and coercion-resistance without "unpractical" assumptions, which does not require untappable channels, but instead assumes voter access to an anonymous channel at some point during the voting process. Later they give a new version [14].Their protocol is based on Plaintext Equivalence Test, mix net and zero knowledge proof. According to our analysis we find that it has the following problems: (1) do not defense against forced-abstention and simulation attacks ;(2) can not support write in ballot. Based on JCJ idea [14], Smith [15] points out JCJ scheme is not secure against 1009 attack and time stamping attack, and then proposes an improved coercion-resistant scheme with weak physical assumptions: anonymous channel. His scheme replaces the inefficient comparison mechanism of JCJ by a new one that computes the voting results in linear time. In addition, it includes an additional mix step in the tallying phase and uses timestamps. He performs a global blind comparison of ciphertexts instead of employing the costly plaintext equivalence test. But Ara´ujo and Traor´ [16] and Clarkson et al. [17] point out that the method is not secure: an adversary can use the ElGamal malleability to determine whether a coerced voter gave him a valid or a fake credential. Weber [18] and Weber et al. [19] also point out weaknesses on Smith's proposal and fixed the JCJ scheme and Smith scheme. Their protocol is with untappable private channel. Their method is based on the Shamir secret sharing [20] and Pedersen distributed key generation protocol [21]. Applying some of the JJ ideas [3], Acquisti [22] proposes a coercion-resistant receipt-free voting protocol with weak physical assumptions: an anonymous channel. Its idea is that election authorities provide shares of credentials to each voter, along with designated verifier proofs of each share's validity. Voter can cheat the coercer by producing a false credential. Owning to designate verifier proof the coercer can not verify the proof. Meng points out that it is not receipt-freeness and coercion-resistance in [23].

Rja¡¦skov´a [24] uses deniable encryption to implement the receipt-freeness. Because his 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.

Ara´ujo and Traor´ [16] present a coercion-resistant voting scheme that employs some of the JCJ ideas and that computes election results in linear time based on LRSW assumptions [25]. Their protocol is with weak physical assumptions: an anonymous channel.

Chen et al. [26] introduce the notion of linkable ring signature for designated verifiers and then use it to propose a new receipt-free electronic voting scheme. The voting scheme achieves receipt-freeness by allowing the voters to vote multi-times with weak physical assumptions: an anonymous channel.

Applying some of Acquisti ideas, Meng [23] presents a receipt-free 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. His protocol has receipt-freeness and coercion-resistance and it with weak physical assumptions: a one way anonymous channel between voter and authority. Meng [27] also proposes an Internet voting protocol applied designated verifier proof and proof of knowledge of two ciphertexts of the same plaintext based the same idea. The protocol also supposes there is a one way anonymous channel between voter and authority.

To our best knowledge up to now it does not exist that the remote Internet voting protocol with receipt-freeness and coercion-resistance implemented without physical assumptions.

Deniable encryption can be used against revealing information that the owner of the information may decrypt it in an alternative way to a different plaintext. Namely if this user opens all his inputs including the claimed encrypted message to a coercer, the coercer fails to prove the validity or invalidity of the opened message.

Motivated by this we apply deniable encryption scheme and trapdoor commitment scheme, to implement the receipt-freeness and coercion-resistance without physical assumptions.

III.RELATED CRYPTOGRAPHIC PRIMITIVES

In this section we introduce the related cryptographic primitives which are used to develop our proposed remote Internet voting protocol. These cryptographic

© 2010 ACADEMY PUBLISHER

primitives include BCP commitment scheme and MW deniable encryption scheme.

A. BCP Commitment Scheme

A trapdoor commitment scheme is a function with associated a pair of matching public and private keys. The main property we want from such a function is collision-resistance: unless one knows the trapdoor, it is infeasible to find two inputs that map to the same value. On the other hand, knowledge of the trapdoor suffices to find collisions easily. BCP commitment scheme [30] is based on BCP cryptosystem [30]. A trapdoor commitment scheme consists of key generation algorithm, commitment function, and collision-finding function.

❁ Key Generation

The key generation algorithm, on input a security parameter l produces a modulus N product of two safe primes of size $l/2$ together with a square h of maximal order in G. The public key is given by N and h. The factorization of the modulus is the private key (p,q).

❁ Committing a Message

To commit to a message $m \in \mathbb{Z}_N$ the sender chooses a random number $r \in_R \mathbb{Z}_{N\lambda(N)/2}$ and sets $B = C(r,m) = h^r (1+mN) \bmod N^2$, and sent (B,r,m) to the receiver.

❁ Collision-finding function

Now given a commitment $B = C(r,m) \in G$ together with the corresponding (r,m), knowing the factorization of the modulus, one can find collisions, for any message m' as follows $r' = r + (m-m')d\lambda(N) \bmod N\lambda(N)/2$. Thus the receiver can get $B = C(r,m) = C(r',m') \in G$.

B. MW Deniable Encryption Scheme

Deniable encryption can be used against revealing information that the owner of the information may decrypt it in an alternative way to a different plaintext. Namely if this user opens all his inputs including the claimed encrypted message to a coercer, the coercer fails to prove the validity or invalidity of the opened message. MW deniable encryption scheme [32] consists of preliminaries, encryption, decryption and dishonest opening phases.

❁ Preliminaries

The receiver chooses a random element $\alpha \in \mathbb{Z}^*_{N^2}$, and sets $g = \alpha^2 \bmod N^2$, publishes publicly (N,g). Then the sender gets (N,g) and chooses a random number $a \in [1, \mathrm{ord}(G)]$, computes $h = g^a \bmod N^2$ and publish publicly (g).The public key of the receiver is given by the triplet (N,g,h), while the corresponding secret key is private key (p,q). At the same time the sender can generates his public key (N,g,h) and private key a based on BCP cryptosystem. Finally he creates his private key a and public key $y = g^a \bmod p$ according to ElGamal cryptosystem [28, 29]. Because everyone can know the public key (N,g,h) of the sender, the receiver can get the sender' private key a owning to the knowledge of $h = g^a \bmod N^2$ and $N = p \times q$.

❁ Encryption

The sender choose random numbers $r_2 \in \langle g \rangle$, after that the sender generate the message $m \in \mathbb{Z}_N$, which will be sent to the receiver in deniable encryption scheme. The sender computes $B = C(r,m) = C(r_2,m) = h^{r_2}(1+mN) \bmod N^2$ based on BCP commitment scheme. Generating the fake message m', he can find $r_1 = r_2 + (m-m')d\lambda(N) \bmod N\lambda(N)/2$ which make $B = C(r_2,m) = C(r_1,m')$ .Then he computes $\left(\partial = g^{hash(r_2)} \bullet r_1, \wp = \left(y^{hash(r_2)} \bullet r_1^a\right) \bullet r_2\right)$ using ElGamal cryptosystem. $(\partial, \wp)$ is the ciphertext of r_2. Finally he sends $(\partial, \wp)$ and $B = C(r,m)$ to the receiver.

❁ Decryption

The receiver uses the private key (p,q) to recover $m = \left(D - 1 \bmod N^2 / N\right) \bullet \pi \left(\bmod N\right)$ based on BCP cryptosystem.

❁ Dishonest Opening

The receiver uses the private key a to recover the plaintext r_2 with $r_2 = \wp \bullet \partial^{-a} = \left(y^k \bullet r_1^x\right) \bullet r_2 \left(g_\bullet^{\ k} \bullet r_1\right)^{-a}$, then he can compute $hash(r_2)$, and gets $r_1 = \partial \bullet g_\bullet^{-hash(r_2)}$. The receiver computes $A_1 = g^{r_1} \bmod N^2$ and $A_2 = g^{r_2} \bmod N^2$ based on BCP cryptosystem, then he recovers $m_1 = \left(B \Big/ \left(A_1^{\ a}\right) - 1 \bmod N^2 \right) \Big/ N$ and $m_2 = \left(B \Big/ \left(A_2^{\ a}\right) - 1 \bmod N^2 \right) \Big/ N$ with the BCP decryption algorithm. If $m = m_1$ then $r = r_1$; If $m = m_2$ then $r = r_2$. According to the encryption algorithm, let $r = r_2$, at the same time, the receiver knows m , so he can get $m' = \left[\left(C(r,m) \Big/ h^r - 1 \right) \Big/ N \right] \bmod N^2$, which makes $B = C(r,m) = C(r_1,m')$. Thus if the receiver

© 2010 ACADEMY PUBLISHER

coerced he can provide the fake message m' to the coercer. The coercer can not verify the fake message.

IV. The Proposed Remote Internet voting protocol

A. Assumptions and Model

In proposed remote Internet voting protocol when coerced by the coercer the voter wants to lie about the decrypted message to a coercer and hence, escape coercion. On one hand, the voter is able to decrypt the correct message from the registration authority, on the other hand, all the information held by the voter when opened to a coercer, do not allow this coercer to verify the encrypted message ,or the coercer can not find the message is a fake message. Consequently, bribing or coercing the voter becomes useless from the very beginning.

The participants in our protocol consist of the voter, registration authority, tallying authority, coercer and briber. As usual, the registration authority and tallying authority can be beyond the reach of any coercer by introducing threshold encryption while the voter is possibly coerced or bribed.

The briber can bribe the voter and voter want to provide the evidence to prove that he vote a special ballot according to requirement of the briber. The briber has the ability to monitor the communication channels. The briber is a passive attacker.

The coercer has the power to approach the voter coercing him to reveal the decrypted message, the decryption key and all the parameters he used during decryption. In our proposed protocol, we assume that the coercer has the ability to eavesdrop all the communication channels.

In our proposed protocol we also assume that the channel between the voter and registration authority and the voter and bulletin board are tappable channel. That is mean everyone including briber and coercer can get the content on the channel.

B. The Idea of The Proposed Remote Internet Voting Protocol

The idea of the proposed Internet voting protocol with receipt-freeness and coercion-resistance is that: if everyone knows that the voter has the ability that generates the fake credential and the ballot, when the voter provides the evidence to the vote-buyer or briber or coercer, they has not the ability to verify the evidence, so the vote-buyer does not give the money to the voter. At the same time the voter can escape the coercion .So the proposed Internet voting protocol has receipt-freeness and coercion-resistance.

How to make the voter to have ability that generates the fake credential and the ballot with the condition the briber and coercer can eavesdrop the communication channel? Owning to the property of MW deniable encryption and BCP commitment scheme we can use it to implement the ability.

The proposed Internet voting protocol applies the encryption technologies which include ElGamal cryptosystem, threshold ElGamal cryptosystem, mix net, deniable encryption and BCP commitment scheme.

C. The Proposed Protocol

In order to express the idea clearly we suppose that there is only one registration authority and one tallying authority. The proposed remote Internet voting protocol includes four phases: preparation phase, registration phase, voting phase and tallying phase.

❁ Notation definition:

A_R : The registration authority;

A_T : The tallying authority;

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

B^t : Ballot voted t ;

$C_j\,(j=1,\cdots,l)$: A_R creates the random number for V_j . It is the credential of V_j ;

${}_{BCP}PU_R, {}_{BCP}PR_R$: The public key and private key of A_R based on BCP cryptosystem, which is used when voter register;

${}_{ElG}PU_R, {}_{ElG}PR_R$:The public key and private key of A_R based on ElGamal cryptosystem, which is used when voter register;

${}_{BCP}PU_T, {}_{BCP}PR_T$:The public key and private key of A_T based on BCP commitment scheme, which is used when voter vote;

${}_{BCP}PU_j, {}_{BCP}PR_j$:The public key and private key of V_j based on BCP cryptosystem;

${}_{ElG}PU_j, {}_{ElG}PR_j$:The public key and private key of V_j based on ElGamal cryptosystem;

$PR(m)$: Sign m with private key PR ;

$PU(m)$: Encrypt m with private key PU ;

ϕ : Self blinding operation;

$Identif_j$: Identification of V_j ;

❁ Preparation phase

The registration authority A_R chooses a random element $\alpha \in \mathbb{Z}^*_{N^2}$, and sets $g=\alpha^2 \bmod N^2$, publishes publicly (N,g) . Then the voter V_j gets (N,g) and chooses a random number $a \in [1, \mathrm{ord}(\mathrm{G})]$, computes $h=g^a \bmod N^2$ and publish publicly (g) .The public key of the registration authority A_R is given by the triplet ${}_{BCP}PU_R=(N,g,h)$, while the corresponding secret key is private key ${}_{BCP}PR_R(p,q)$. At the same time the voter V_j can generates his public key ${}_{BCP}PU_j=(N,g,h)$ and private key ${}_{BCP}PR_j=a$ based on BCP cryptosystem. Finally he also creates his private key ${}_{ElG}PR_j=a$ and public key ${}_{ElG}PU_j=y=g^a \bmod p$ according to ElGamal cryptosystem. Because everyone can know the public key ${}_{BCP}PU_R=(N,g,h)$ of

© 2010 ACADEMY PUBLISHER

registration authority A_R , the voter V_j can get the registration authority A_R ' private key ${}_{BCP}PR_j = a$ through the knowledge of $h = g^a \bmod N^2$ and $N = p \times q$. Finally the registration authority A_R generates his public key and private key ${}_{ElG}PU_R$, ${}_{ElG}PR_R$ based on ElGamal cryptosystem Registration authority A_R generates the ballot B^t and send B^t and its digital signature to bulletin board denoted by BB.

Tallying authority A_T generates his public key ${}_{BCP}PU_T = (N,h)$ and private key ${}_{BCP}PR_T = (p,q)$ according to BCP commitment scheme.

❁ Registration phase

(1) Firstly voter V_j generates the $Identif_j$, secondly produces message ${}_{EIG}PR_j\left(Identif_j\right) \| {}_{EIG}PU_j \| Identif_j$ and send it to registration authority A_R . Registration authority A_R receives the message and uses its private key to verify the digital signature. Registration authority A_R checks $Identif_j$ that whether he has registered or not. If he has registered, registration authority A_R sends the error message to V_j . The protocol ends. If he has not registered, registration authority A_R executes <2> step. Figure 1 describes the registration phase.

(2) According to requirements of MW deniable encryption scheme registration authority A_R produces $\begin{bmatrix} {}_{EIG}PR_R\left\{(\partial,\wp) \| B = C\left(r,C_j\right)\right\} \\ \| (\partial,\wp) \| B = C\left(r,C_j\right) \end{bmatrix}$, then send it to the voter by tappable channel.

(3). Registration authority A_R sends ${}_{EIG}PR_R\left({}_{EIG}PU_R\left(C_j\right)\right) \| {}_{EIG}PU_R\left(C_j\right)$ to BB in Table III.

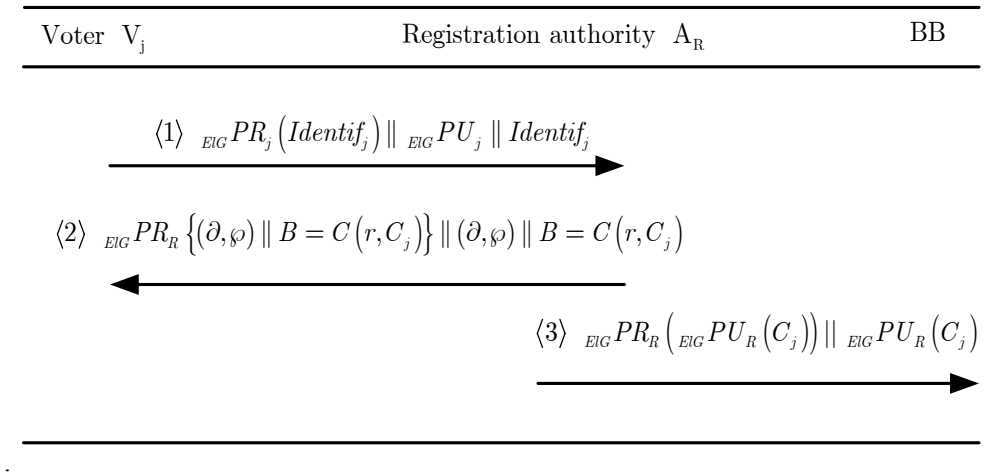

Figure 1. Registration phase

❁ Voting phase

Voter V_j chooses his favor ballot. Using tallying authority A_T 'public key ${}_{BCP}PU_T = (N,h)$ voter V_j generates $B_C = C\left(r_1,C_j\right) \| B_B = C\left(r_1,B_t\right)$ with BCP commitment scheme and sends it to Table I randomly in BB by a tappable channel.

❁ Tallying phase

(1) According to the rules the tallying authority eliminates the duplicate $B_C = C\left(r_1,C_j\right) \| B_B = C\left(r_1,B_t\right)$. The results are stored in Table II.

(2) Mixing Authority mixes $B_C = C\left(r_1,C_j\right) \| B_B = C\left(r_1,B_t\right)$ in Table II. The corresponding results are $\phi\left[B_C = C\left(r_1,C_j\right)\right] \| \phi\left[B_B = C\left(r_1,B_t\right)\right]$ and stored in Table IV and Table V.

(3) Tallying authority A_T decrypts $\phi\left[B_C = C\left(r_1,C_j\right) \| B_B = C\left(r_1,B_t\right)\right]$ in Table IV and Table V and gets C_j and B_t . At the same time he verifies ${}_{EIG}PR_R\left({}_{EIG}PU_R\left(C_j\right)\right) \| {}_{EIG}PU_R\left(C_j\right)$ and let registration authority A_R decrypt ${}_{EIG}PU_R\left(C_j\right)$ and gets C_j in Table III.

(4) Tallying authority A_T tallies the ballot and publishes the results.

TABLE I. BALLOTS BEFORE TALLYING

$B_C = C\left(r_1,C_j\right)$	$B_B = C\left(r_1,B_t\right)$

TABLE II. BALLOT ELIMINATED THE DUPLICATE

© 2010 ACADEMY PUBLISHER

$B_C = C(r_1, C_j)$	$B_B = C(r_1, B_t)$

TABLE III. THE ${}_{EIG}PR_R\left({}_{EIG}PU_R(C_j)\right) \| {}_{EIG}PU_R(C_j)$

${}_{EIG}PR_R\left({}_{EIG}PU_R(C_j)\right) \| {}_{EIG}PU_R(C_j)$	Proof	C_j

TABLE IV. E $\phi\left[B_C = C(r_1, C_j)\right]$

$\phi\left[B_C = C(r_1, C_j)\right]$	Proof	C_j

TABLE V. THE $\phi\left[B_B = C(r_1, B_t)\right]$

$\phi\left[B_B = C(r_1, B_t)\right]$	Proof	B_t

V. PROPERTIES ANALYSIS

Owning to the space limitation we only analysis receipt-freeness and coercion-resistance

A. Receipt-freeness

The proposed Internet voting protocol accomplishes receipt-freeness by MW deniable encryption scheme and BCP commitment scheme.

According to the proposed protocol, in registration phase the voter get the real credential, which can be verified by the voter himself through honest opening in MW deniable encryption scheme, from the registration authority. Applying the dishonest opening in MW deniable encryption scheme, the voter can generate a fake credential ${}_{fake}C_j$ to satisfy ${}_{EIG}PR_R\left\{(\partial, \wp) \| B = C(r, C_j)\right\} \| (\partial, \wp) \| B = C(r, C_j) = C({}_{fake}r, {}_{fake}C_j)$ which is used to cheat briber. Although the briber has the ability to monitor the communication channel between voter and registration authority, because the voter can provide the transcripts of $C({}_{fake}r, {}_{fake}C_j)$, the briber can verify it and can not find ${}_{fake}C_j$ is a fake credential. At the same time in voting phase the voter send the ballot and credential to BB by BCP commitment scheme. Own to the property of BCP commitment scheme the voter also can find collisions: $B_C = C(r_1, C_j) = C({}_{fake}r_1, {}_{fake}C_j) \| B_B = C(r_1, B_t) = C({}_{fake}r_1, {}_{fake}B_t)$ and provide the transcript of $B_C = C({}_{fake}r_1, {}_{fake}C_j) \| B_B = C({}_{fake}r_1, {}_{fake}B_t)$ which can be verified by the briber although the briber has the ability to eavesdrop the communication channel between voter and BB. In a word, the voter has the ability to produce the fake credential and ballot which can be verified by briber or voter buyer. So the vote buyer or briber does not give the money to the voter.

Hence the protocol is receipt-freeness.

B. Coercion-resistance

We have already analyzed that it is receipt-freeness in previous section. In the following we analyze that it can prevent randomization attack, forced-abstention attack and simulation attack.

(1) Randomization attack

The idea of Randomization attack is for an attacker to coerce a voter by requiring that she submit randomly composed balloting material. The effect of the attack is to nullify the choice of the voter.

We suppose that voter wants to prevent randomization attack. But after voting by coercer, the vote can vote his favorite ballot because the vote can vote several times according to the proposed protocol. So the protocol can prevent randomization attack.

(2) forced-abstention attack

This is an attack related to the previous one based on randomization. In this case, the attacker coerces a voter by demanding that she refrain from voting.

Because the coercer has the ability to eavesdrop the communication channel between the voter and registration authority, he can get ${}_{EIG}PR_R\left\{(\partial, \wp) \| B = C(r, C_j)\right\} \| (\partial, \wp) \| B = C(r, C_j)$ and ${}_{EIG}PR_j(Identif_j) \| {}_{EIG}PU_j \| Identif_j$, hence the current version of the proposed protocol is not against this attack. But we can use offline way in registration phase, thus according to protocol coercer can not know if voter has registered based on BB. In voting phase the coercer can get $B_C = C(r_1, C_j) \| B_B = C(r_1, B_t)$ by monitor the communications between the voter and BB. Owning to property of BCP commitment scheme the coercer can not identify the credential of the voter and find who vote the ballot. So the protocol can prevent forced-abstention attack.

(3) Simulation attack

Simulation attack is that an attacker coerces voters into divulging private keys or buying private keys from voters and then simulating these voters at will, i.e., voting on their behalf. Coercer can vote on voter behalf after getting private key of voter in our proposed protocol. But after voting by coercer, the vote can vote his favorite ballot because the vote can vote several times according to the proposed protocol. Hence the protocol can prevent simulation attack.

VI. CONCLUSION

Internet voting protocol is base of Internet voting system. In this paper firstly, a receipt-free coercion-resistant remote Internet voting protocol based on MW deniable encryption scheme and BCP commitment scheme is developed. The proposed protocol is the first remote Internet voting protocol, which has receipt-freeness and coercion-resistance and is implemented without physical assumptions. Secondly, we analyze receipt-freeness and coercion-resistance of the proposed remote Internet voting protocol. Thirdly, we compare security properties of several typical protocols with our

© 2010 ACADEMY PUBLISHER

present protocol. Owning to the space limitation we only give the result described in Table VI, Table VII, and Table VIII.

In the future we will use the protocol analyzer ProVerif [33] based on the applied pi calculus to analyze 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 VI. THE RESULT OF ANALYZING RECEIPT-FREENESS AND WHAT PHYSICAL ASSUMPTIONS ARE USED THE MARK"T" REPRESENTS THE PROTOCOL IS WITH PHYSICAL ASSUMPTIONS; THE MARK" ● " REPRESENTS THE PROTOCOL HAS THE PROPERTY; THE MARK" F" REPRESENTS THE PROTOCOL HAS NOT THE PROPERTY

		[1]	[4]	[9]	[11]	[5,6]	[26]	[12]	[22]
Physical assumptions	Voting booth	**T**				**T**			
	Untappable one-way channels		**T**						
	Untappable private channel			**T**					
	Secret communication channel				**T**				
	Smart card				**T**				
	Visual cryptography					**T**			
	Anonymous channel						**T**		**T**
	Tamper resistant randomizer							**T**	
	Randomizer		**T**						
	Tappable channel								**T**
Security	Receipt-freeness	F	●	●	●	●	●	●	●

TABLE VII. THE RESULT OF ANALYZING RECEIPT-FREENESS AND WHAT PHYSICAL ASSUMPTIONS ARE USED THE MARK"T" REPRESENTS THE PROTOCOL IS WITH PHYSICAL ASSUMPTIONS; THE MARK" ● " REPRESENTS THE PROTOCOL HAS THE PROPERTY

		[10]	[7]	[23]	[2]	[3,14]	[8]	our
Physical assumptions	Voting booth	**T**	**T**		**T**		**T**	
	Untappable private channel	**T**			**T**			
	Privacy commission members				**T**			
	Anonymous channel		**T**	**T**		**T**		
Security	Receipt-freeness	●	●	●	●	●	●	●

TABLE VIII. THE RESULT OF ANALYZING COERCION-RESISTANCE AND WHAT PHYSICAL ASSUMPTIONS ARE USED;THE MARK"T" REPRESENTS THE PROTOCOL IS WITH PHYSICAL ASSUMPTIONS; THE MARK" ● " REPRESENTS THE PROTOCOL HAS THE PROPERTY; THE MARK"**F**" REPRESENTS THE PROTOCOL HAS NOT THE PROPERTY

		[3]	[15]	[18,19]	[16]	[17]	[22]	[23]	[27]	our
Physical assumptions	Untappable private channel			**T**						
	Anonymous channel	**T**	**T**		**T**	**T**	**T**	**T**	**T**	
	Tappable channel						**T**			
Security	Coercion-resistance	**F**	**F**	●	●	**F**	**F**	●	●	●

REFERENCES

[1] J.Benaloh,D.Tuinstra, "Receipt-free secret-ballot elections," *In the proceeding of STOC '94*, pp.544–553, 1994.

[2] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," *In the proceeding of Security Protocols Workshop*, Springer-Verlag, LNCS 1361, pp.25–35, 1997.

[3] A.Juels, M. Jakobsson, "Coercion-resistant electronic elections," *http://www.vote-auction.net/VOTEAUCTION/165.pdf,*2002.

[4] M.Hirt,K.Sako, "Efficient receipt-free voting based on homomorphic encryption," *In the proceeding of EUROCRYPT '00*, Springer-Verlag, LNCS 1807, pp.539–556, 2000.

[5] D.Chaum, "Secret-ballot receipts and transparent integrity," Draft, *http://votingindustry.com/Tech_Corner/Chaum_article.pdf,* 2002.

[6] D.Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security and Privacy*, vol. 2, no. 1, pp. 38-47, Jan. 2004.

[7] C.I. Fan, W.Z. Sun, "An efficient multi-receipt mechanism for uncoercible anonymous electronic voting," *Mathematical and Computer Modeling*, Volume 48, Issues 9-10, pp.1611-1627, November 2008.

[8] A. Neff, "Detecting malicious poll site voting clients," *http://www.votehere.net/*,2003.

[9] K. Sako, J. Kilian, "Receipt-Free Mix-Type Voting Scheme, A practical solution to the implementation of a voting booth," *Advances in Cryptology — EUROCRYPT '95*, pp.393-403, 1995.

[10] T. Moran, M. Naor, "Receipt-Free Universally-Verifiable Voting with Everlasting Privacy*," Advances in Cryptology - CRYPTO 2006*, Volume 4117/2006.pp 373-392, 2006.

[11] O. Baudron, P.Fouque, D. Pointcheval, J. Stern, and G. Poupard, "Practical multi-candidate election system," *In Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing* (Newport, Rhode Island, United States). *PODC '01*. ACM, New York, NY, pp.274-283, 2001.

[12] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Providing Receipt-freeness in Mixnet-based Voting Protocols,"

© 2010 ACADEMY PUBLISHER

http://caislab.icu.ac.kr/Paper/paper_files/2003/ICISC03/mnvoting-final-icisc2003.pdf,2003.
[13] H.Zhong, L.S.Huang, and Y.L.Luo, "A Multi-Candidate Electronic Voting Scheme Based on Secure Sum Protocol," *Journal of Computer Research and Development*, 43(8).pp.1405-1410, 2006.
[14] A.Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," *In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (Alexandria, VA, USA, November 07 - 07, 2005). WPES '05*. ACM, New York, NY, pp.61-70, 2005.
[15] W.D. Smith, "New cryptographic voting scheme with best-known theoretical properties," *In Workshop on Frontiers in Electronic Elections (FEE 2005)*, Milan, Italy, *http://www.math.temple.edu/~wds/homepage/jcj.pdf*, September 2005.
[16] S.F.Ara´ujo, J.A.Traor´, "practical and secure coercion-resistant scheme for remote elections," *Frontiers of Electronic Voting, http://drops.dagstuhl.de/opus/volltexte/2008/1295/* ,2008
[17] M. Clarkson, S. Chong, and A.C.Myers, "Civitas: A Secure Remote Voting System," *Technical report, Cornell University Computing and Information Science Technology Report,* http://drops.dagstuhl.de/opus/volltexte/2008/1296/, May 2007.
[18] S. Weber, "A Coercion-Resistant Cryptographic Voting Protocol- Evaluation and Prototype Implementation," Darmstadt University of Technology, *http://www.cdc.informatik.tu-darmstadt.de/reports/reports/StefanWeber.diplom.pdf*, 2006.
[19] S.G.Weber, R.Araujo, and J. Buchmann, "On Coercion-Resistant Electronic Elections with Linear Work," *In Proceedings of the Second international Conference on Availability, Reliability and Security* (April 10 - 13, 2007). *ARES*. IEEE Computer Society, Washington, DC, pp.908-916, 2007.
[20] A. Shamir, "How to share a secret," *Common.* ACM 22, 11, pp.612-613, Nov. 1979.
[21] T. P. Pedersen, "A threshold cryptosystem without a trusted party (extended abstract)," *In Advances in Cryptology - EUROCRYPT 91*, volume 547 of LNCS, pp. 522-526, April 1991.
[22] A.Acquisti, "Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots," *Technical Report 2004/105*, International Association for Cryptologic Research, May 2, 2004, and Carnegie Mellon Institute for Software Research International, CMU-ISRI-04-116, *http://www.heinz.cmu.edu/~acquisti/papers/acquisti-electronic_voting.pdf*, 2004.
[23] B. Meng, "A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext. Journal of Networks," 4(5), pp.370-377, 2009
[24] Z. Rja¡¦skov´a, "Electronic Voting Schemes," Master thesies. Department of Computer Science Faculty of Mathematics, Physics and Informatics Comenius University, Bratislava, April 2002.
[25] J. Camenisch , A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," *Advances in Cryptology – CRYPTO 2004,*pp56–72,2004.
[26] G. Chen, C. Wu, W. Han, X. Chen, H. Lee, and K. Kim, "A New Receipt-Free Voting Scheme Based on Linkable Ring Signature for Designated Verifiers," *In Proceedings of the 2008 international Conference on Embedded Software and Systems Symposia* - Volume 00 (July 29 - 31, 2008). ICESSSYMPOSIA. IEEE Computer Society, Washington, DC, pp.18-23, 2008.
[27] B. Meng, "An Internet Voting Protocol with Receipt-Free and Coercion-Resistant," *In Proceedings of the 7th IEEE international Conference on Computer and information Technology* (October 16 - 19, 2007). CIT. IEEE Computer Society, Washington, DC, pp.721-726, 2007.
[28] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," In: Blakely, G.R., Chaum, D. (eds.) *CRYPTO 1984*. LNCS, vol. 196, pp. 10–18, Springer, Heidelberg, 1985.
[29] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory* 31(4), pp, 469–472, 1985.
[30] E.Bresson, D. Catalano,and D. Pointcheval, "A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications". In: Laih CS, ed. *Aciacrypt 2003*. LNCS 2894, Berlin: Springer-Verlag, pp.37-54, 2003.
[31] M. Klonowski, P. Kubiak, and M. Kutyłowsk, "Practical Deniable Encryption," *SOFSEM 2008: Theory and Practice of Computer Science,34th Conference on Current Trends in Theory and Practice of Computer Science*, Nový Smokovec, Slovakia, January 19-25, 2008.,pp599-609, 2008.
[32] B.Meng, J.Q.Wang, "An Efficient Receiver Deniable Encryption Scheme and Its Applications" (accepted).
[33] B. 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.
[34] B.Meng, "A Critical Review of Receipt-Freeness and Coercion-Resistance," Information Technology Journal, 8(7), pp.934-964, 2009.

Bo Meng was born in 1974 in P.R.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, P.R.China, in 2000, 2003, respectively. From 2004 to 2006, he works in Wuhan University, P.R.China as Postdoctoral researcher in information security.

Currently he is an Associate Professor in school of computer, South-Center University for Nationalities, P.R.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.

Zimao Li was born in 1974. He received his B.S. degree in Mathematics in 1996, M.Eng degree in Computer Science in 1999, both from Shandong University, P.R.China, and Ph.D degree in Computer Science from City University of Hong Kong, Hong Kong, in 2002.

He is currently an Associate Professor in the School of Computer Science, South-Center University for Nationalities, P.R. China. His research interests are design and analysis of algorithms, complexity theory and computational biology.

Jun Qin was born in 1968 in P.R.China. She received her M.S. degree in computer science in 1995 from Huazhong University of Science and Technology, and Ph.D. degree in computer software theory in 2005 from Wuhan University, respectively, at Wuhan, P.R.China, in 2006; she worked in Wisconsin University, U.S.A. as an international visiting scholar in information security.

Currently she is a Professor of school of computer, South-Center University for Nationalities, P.R.China. She has authored/coauthored over 50 papers in International/National journals and conferences. Her current research interests include electronic commerce security, intelligent algorithm.

© 2010 ACADEMY PUBLISHER