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 (60803008) and Natural Science Foundation of Hubei Province (2007ABA342)
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 weak physical assumptions to 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 smart card[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 with "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’jo and Traoré [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 coerced by producing a false credential. Owning to designate verifier proof the coerced can not verify the proof. Meng points out that it is not receipt-freeness and coercion-resistance in [23].

Rjas’kov’a [24] uses denial encryption to implement the receipt-freeness. Because his denial 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’jo and Traoré [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 denial 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
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 \( 1/2 \) 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 \((p, q)\). At the same time the sender 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 \(y = g^a \mod p\) 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’s private key \(a\) owning to the knowledge of \(h = g^a \mod N\) and \(N = p \times q\).

Encryption

The sender choose random numbers \(r_{2} \in \{g\}\), 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 \(B = C(r_m) = C(r_{2}m) = h^m (1 + mN) \mod N^2\) based on BCP commitment scheme. Generating the fake message \(m^*\) , he can find \(r_1 = r_2 + (m - m^*) \frac{d\lambda(N)}{\lambda(N)} \mod N\lambda(N)/2\) which make \(B = C(r_{2}m) = C(r_{1}m^*)\). Then he computes \((\bar{\sigma} = g^\text{hash}(r_1) \cdot r_1, \bar{\varphi} = y^{\text{hash}(r_1)} \cdot r_1^* \cdot r_2)\) using ElGamal cryptosystem. \((\bar{\sigma}, \bar{\varphi})\) is the ciphertext of \(r_2\). Finally he sends \((\bar{\sigma}, \bar{\varphi})\) and \(B = C(r_m)\) to the receiver.

Decryption

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

Dishonest Opening

The receiver uses the private key \(a\) to recover the plaintext \(r_2\) with \(r_2 = \bar{\varphi} \cdot \bar{\sigma}^{-a} = (y^a \cdot r_1^a) \cdot r_2^a \cdot g^a \cdot r_1 \). Then he can compute \(\text{hash}(r_1)\), and gets \(r_1 = \bar{\sigma} \cdot g^{-\text{hash}(r_1)}\).

The receiver computes \(A_1 = g^a \mod N^2\) and \(A_2 = g^a \mod N^2\) based on BCP cryptosystem, then he recovers \(m_1 = \left(B/(A_1)^{-1} \mod N^2\right)/N\) and \(m_2 = \left(B/(A_2)^{-1} \mod N^2\right)/N\) 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 \(m = \left[\left(C(r_m)/h^{-1}\right) \mod N^2\right]\) which makes \(B = C(r_m) = C(r_1m^*)\). Thus if the receiver
coerced he can provide the fake message $m'$ to the coercer. The coercer cannot 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 cannot 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 coercer can bribe the voter and voter want to provide the evidence to prove that he vote a special ballot according to requirement of the coercer. 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 duration. 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;
  $V_j (j = 1, 2, \ldots, l)$: The $j$th legal voter;
  $B^i$: Ballot voted $t$;
  $C_j (j = 1, 2, \ldots, l)$: $A_R$ creates the random number for $V_j$.

It is the credential of $V_j$:

$\text{bcp PU} \times \text{BCP PR}_R$: The public key and private key of $A_R$ based on BCP cryptosystem, which is used when voter register;

$\text{elG PU} \times \text{elG PR}_R$: The public key and private key of $A_R$ based on ElGamal cryptosystem, which is used when voter register;

$\text{bcp PU} \times \text{BCP PR}_T$: The public key and private key of $A_T$ based on BCP commitment scheme, which is used when voter vote;

$\text{elG PU} \times \text{elG PR}_T$: The public key and private key of $V_j$ based on BCP cryptosystem;

$\text{elG PU} \times \text{elG PR}_R$: The public key and private key of $V_j$ based on ElGamal cryptosystem;

$\text{pr (m)}$: Sign $m$ with private key $\text{PR}$;

$\text{PU (m)}$: Encrypt $m$ with private key $\text{PU}$;

$\phi$: Self blinding operation;

$\text{Identification of } V_j$: Identification of $V_j$.

- Preparation phase

The registration authority $A_R$ chooses a random element $a \in Z_{n^2}^*$, and sets $g = a^2 \mod n^2$, publishes publicly $(N, g)$. Then the voter $V_j$ gets $(N, g)$ and chooses a random number $a \in \left[1, \text{ord}(G)\right]$, computes $h = g^a \mod n^2$ and publish publicly $(g)$. The public key of the registration authority $A_R$ is given by the triplet $\text{bcp PU}_R = (N, g, h)$, while the corresponding secret key is private key $\text{bcp PR}_R = (p, q)$. At the same time the voter $V_j$ can generates his public key $\text{bcp PU}_j = (N, g, h)$ and private key $\text{bcp PR}_j = a$ based on BCP cryptosystem. Finally he also creates his private key $\text{elG PR}_j = a$ and public key $\text{elG PU}_j = y = g^a \mod p$ according to ElGamal cryptosystem. Because everyone can know the public key $\text{bcp PU}_R = (N, g, h)$ of
registration authority $A_R$, the voter $V_j$ can get the registration authority $A_R$’s private key $b_{CP} PR_j = a$ through the knowledge of $h = g^a \mod N^2$ and $N = p \times q$. Finally the registration authority $A_R$ generates his public key and private key $e_{EG} PU_R, e_{EG} PR_R$ based on ElGamal cryptosystem. Registration authority $A_R$ generates the ballot $B'$ and send $B'$ and its digital signature to bulletin board denoted by BB.

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

**Registration phase**

1. Firstly voter $V_j$ generates the $Identif_j$, secondly produces message $e_{EG} PR_R(Identif_j) \parallel e_{EG} PU_j \parallel Identif_j$ 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 $e_{EG} PR_R \{ (\partial, \varphi) \parallel B = C(r, C_j) \}$, then send it to the voter by tappable channel.

3. Registration authority $A_R$ sends $e_{EG} PR_R \{ e_{EG} PU_R(C_j) \} \parallel e_{EG} PU_R(C_j)$ to BB in Table III.

**Voting phase**

Voter $V_j$ chooses his favor ballot. Using tallying authority $A_T$’s public key $b_{CP} PU_T = (N, h)$ voter $V_j$ generates $B_c = C(r, C_j) \parallel B_b = C(r, B_j)$ 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 $B_c = C(r, C_j) \parallel B_b = C(r, B_j)$ in Table I and Table II. At the same time he verifies $e_{EG} PR_R \{ e_{EG} PU_R(C_j) \} \parallel e_{EG} PU_R(C_j)$ and let registration authority $A_R$ decrypt $e_{EG} PU_R(C_j)$ and gets $C_j$ in Table III.

2. Tallying authority $A_T$ decrypts $\phi(B_c = C(r, C_j) \parallel B_b = C(r, B_j))$ in Table IV and Table V and gets $C_j$ and $B_j$. The corresponding results are $\phi(B_c = C(r, C_j))$ and $\phi(B_b = C(r, B_j))$ and stored in Table IV and Table V.

3. Tallying authority $A_T$ tallies the ballot and publishes the results.
TABLE III. THE $e_{GR}PR_{eGR}(e_{GR}PU_{eGR}(C_j)) || e_{GR}PU_{eGR}(C_j) \quad \text{Proof} \quad C_j$

TABLE IV. $\phi[B_c = C(r_1, C_j)] \quad \text{Proof} \quad C_j$

TABLE V. $\phi[B_b = C(r_1, B_j)] \quad \text{Proof} \quad B_j$

V. PROPERTIES ANALYSIS

Owing 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 to satisfy

$$e_{GR}PR_{eGR}\{\phi, \psi\} || B = C(r, C_j) \quad \text{Proof} \quad C_j$$

which is used to cheat briber. Although the briber has the ability to monitor the communication channel between voter and registration authority, the voter can provide the transcripts of $C_{\text{fake}, \text{fake}, C_j}$, the briber can verify it and can not find $\text{fake}, C_j$ 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: $B_c = C(r_1, C_j) = C_{\text{fake}, r_1, \text{fake}, C_j}$ and provide the transcript of $B_c = C_{\text{fake}, r_1, \text{fake}, C_j} || B_b = C_{\text{fake}, r_1, \text{fake}, B_j}$ 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 coercer a voter by requiring that she submit randomly composed ballot 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 $e_{GR}PR_{eGR}\{\phi, \psi\} || B = C(r, C_j) \quad \text{Proof} \quad C_j$ and $e_{GR}PR_{eGR}\{\text{Identify} \} || e_{GR}PU_{eGR} \quad \text{Identify} \}$, 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 $B_c = C(r_1, C_j) || B_b = C(r_1, B_j)$ 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
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 VIII.** THE RESULT OF ANALYZING RECEIPT-FREENESS AND WHAT PHYSICAL ASSUMPTIONS ARE USED THE MARK “T” REPRESENTS THE PROTOCOL IS WITH PHYSICAL ASSUMPTIONS; THE MARK “F” **•** REPRESENTS THE PROTOCOL HAS THE PROPERTY; THE MARK “F” X **x** REPRESENTS THE PROTOCOL HAS NOT THE PROPERTY

<table>
<thead>
<tr>
<th>Physical assumptions</th>
<th>[1] [4] [9] [11] [5,6] [26] [12] [22]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voting booth</td>
<td>T</td>
</tr>
<tr>
<td>Untapparable one-way channel</td>
<td>T</td>
</tr>
<tr>
<td>Untapparable private channel</td>
<td>T</td>
</tr>
<tr>
<td>Secret communication channel</td>
<td>T</td>
</tr>
<tr>
<td>Smart card</td>
<td>T</td>
</tr>
<tr>
<td>Visual cryptography</td>
<td>T</td>
</tr>
<tr>
<td>Anonymous channel</td>
<td>T</td>
</tr>
<tr>
<td>Tamper resistant randomizer</td>
<td>T</td>
</tr>
<tr>
<td>Randomizer</td>
<td>T</td>
</tr>
<tr>
<td>Tappable channel</td>
<td>T</td>
</tr>
<tr>
<td>Security</td>
<td>F • • • • • • •</td>
</tr>
</tbody>
</table>

**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 “F” **•** REPRESENTS THE PROTOCOL HAS THE PROPERTY

<table>
<thead>
<tr>
<th>Physical assumptions</th>
<th>[10] [7] [23] [2] [3,14] [8] our</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voting booth</td>
<td>T T T T T T</td>
</tr>
<tr>
<td>Untapparable private channel</td>
<td>T T</td>
</tr>
<tr>
<td>Privacy commission members</td>
<td>T T</td>
</tr>
<tr>
<td>Anonymous channel</td>
<td>T T T T T T</td>
</tr>
<tr>
<td>Security</td>
<td>• • • • • •</td>
</tr>
</tbody>
</table>

**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 “F” **•** REPRESENTS THE PROTOCOL HAS THE PROPERTY; THE MARK “F” X **x** REPRESENTS THE PROTOCOL HAS NOT THE PROPERTY

<table>
<thead>
<tr>
<th>Physical assumptions</th>
<th>[3] [15] [18,19] [16] [17] [22] [23] [27] our</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untapparable private channel</td>
<td>T T T T T T T</td>
</tr>
<tr>
<td>Anonymous channel</td>
<td>T T T T T T T</td>
</tr>
<tr>
<td>Tappable channel</td>
<td>T T T T T T T</td>
</tr>
<tr>
<td>Security</td>
<td>F F F F F F F F F F F F F F F F F</td>
</tr>
</tbody>
</table>

REFERENCES

http://caiab.ici.ac.kr/Paper/paper_files/2003/ICISC03/mnnvot


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. degrees 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.