A Formal Logic Framework for Receipt-freeness in Internet Voting Protocol

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

***Abstract*—The practical Internet voting protocols should have: privacy, completeness, soundness, unreusability, fairness, eligibility, and invariableness, universal verifiability, receipt-freeness, coercion-resistant. Receipt-freeness is a key property. Receipt-freeness means that the voter can't produce a receipt to prove that he votes a special ballot. Its purpose is to protect against vote buying. Formal method is an important tool to assess receipt-freeness of Internet voting protocols. In this paper we give a formal logic framework for receipt-freeness based on V. Kessler and H. Neumann logic. The framework is then applied to analyze receipt-freeness of two typical voting protocols: FOO and Meng Internet voting protocol.**

***Index Terms*—logic framework, internet voting protocol, formal method, receipt-freeness, protocol security, electronic government**

I. INTRODUCTION

With the popularization of Internet and advance of process of democracy of nation, a new voting system called Internet voting is introduced.

The secure and practical Internet voting protocols should have basic properties (privacy, completeness, soundness, unreusability, fairness, eligibility, and invariableness) and expanded properties (universal verifiability, receipt-freeness [1], coercion-resistant [2])

Receipt-freeness was introduced by Benaloh and Tuinstra in the paper "receipt-free secret-ballot elections" [1]. The voting protocols are receipt-freeness that means the voter can't produce a receipt to prove that he votes a special ballot. Its purpose is to protect against vote buying.

Benaloh and Tuinstra proposed a receipt-freeness protocol based on voting-booth, but Hirt and Sako in [4] point out that their protocol is not receipt-freeness.

A lot of Internet voting protocols have achieved receipt-freeness through ad hoc physical assumptions and trusted third parties, such as, one or two way untappable channels and/or anonymous or private channels [4,5,6,16]; third-party (trusted) honest verifiers [7]; smart cards [8]; tamper-resistant machines [9]; third party randomizers [10,11,12]; voting booths [1,13], special visual encryption tools [14], used deniable encryption [15].

Reliance on ad hoc physical assumptions or trusted third parties is problematic, because it undermines the security, flexibility, robustness, trustworthiness, and ease of use of an election scheme.

Formal method is the key to assess receipt-freeness of internet voting protocols. Many universal formal methods have been proposed to analyze security protocols. Owning to specialties of internet voting protocol, Delaune et al [17, 18] and Jonker and Vink [3] introduce a formal method for analyze receipt-freeness of internet voting protocol respectively.

In the definition of receipt proposed by H.L. Jonker and E.P. de Vink, I think it is worth discussing. Firstly, about "(R1) r can only have been generated by v" in [3], because in some voting protocol one part of receipt is generated by the authority, not generated by voter. Secondly, they give the following auxiliary receipt decomposition functions: "α: Rcpt →AT", which extracts the authentication term from a receipt. Authentication term should be the identification of voter. Thirdly the author does not prove the generic and uniform formalism that is right in their paper. Finally they use a special notation, it difficult to use and generalize it.

S. Delaune etc. also give the formal definition of receipt-freeness in the applied calculus. It mainly uses the observational equivalence in standard labelled bisimulation. But it does not define what a receipt consists of. A shortage of this formalism is that while it may be used to design a voting protocol with receipt-freeness, it offers little help to check receipts when these are present.

V. Kessler and H. Neumann logic [20] is a provable sound extension of AUTLOG in order to analyze the most important features of participants in electronic commerce protocols. In this paper we use V. Kessler and H. Neumann logic to construct a framework for receipt-freeness. Our approach focuses on establishing what can construct a receipt. This enables the identification of receipts, and provides a heuristic to take receipts into consideration in the early stages of designing a protocol. Our method is simple and it is easy to be generalized.

As is often done in protocol analysis, we assume the Dolev-Yao abstraction: cryptographic primitives are assumed to work perfectly, and the attacker controls the public channels. The attacker can see, intercept and insert

Corresponding author: Bo Meng, South-Center University for Nationalities. E-mail: mengscuec@gmail.com.

messages on a public channel, but can only encrypt, decrypt or sign messages for which he has the relevant key. In the case of both receipt-freeness, we assume that the vote buyer has all the capabilities of the attacker on the public channels.

We briefly overview the Kessler and H. Neumann logic in Section II. Next, in Section Ⅲ, we formalize receipt-freeness. In Section Ⅳ and Ⅴ, we illustrate our ideas in terms of the protocol by Fujioka Atshushi et al [23] and the protocol by Meng Bo [19]. Finally, we conclude in Section Ⅵ.

II. Overview of V. Kessler and H. Neumann logic

V. Kessler and H. Neumann logic is a provable sound extension of AUTLOG in order to analyze the most important features of participants in electronic commerce protocols. In this paper we use the V. Kessler and H. Neumann logic to construct the framework of rececipt-freeness in internet voting protocols.

In the following we only give the calculus rule. Syntax, Protocol Runs, Semantics of the Formulae etc. can be found in [20].In V. Kessler and H. Neumann logic calculus rules include inference rule, modalities, possession, recognizability, freshness, oldness, seeing, Saying, authentication and key confirmation, comprehension, equivalences, key derivation, and provability.

- Inference Rule

MP: $if\ \ \phi\ and\ (\phi \to \psi)\ then\ \psi$

M: $if\ \varphi\ \ is\ the\ theorem$
$then\ P\ believes\ \varphi\ \ is\ a\ theorem$

- Modalities

K: $P\ believes\ \varphi\ \wedge\ P\ believes\ (\varphi \to \psi)$
$\to P\ believes\ \psi$

4 $P\ believes\ \phi\ \to\ P\ believes\ P\ believes\ \ \phi$

5 $\neg p\ believes\ \phi$
$\to\ \ P\ believes\ \neg\ P\ believes\ \phi$

- Possession

H1 $P\ sees\ X\ \to\ \ P\ has\ X$

H2 $P\ has\ X_1 \wedge P\ has\ X_2 \wedge \cdots \wedge P\ \ has\ X_n$
$\to\ \ P\ \ has\ \ (X_1\ ,\ X_2\ \cdots X_n)$

H3 $P\ has\ X\ \to\ P\ has\ F(X)$

- Recognizability

R1 $P\ recognizes\ X_i$
$\to\ \ P\ recognizes\ \ (X_1\ ,\cdots, X_n)$

R2 $P\ recognizes\ X\ \wedge\ P\ has\ K^{-1}$
$\to\ P\ \ recognizes\ \ \ enc(K,X)$

R3 $P\ has\ X\ \ \to\ P\ recognizes\ h(X)$

R4 $P\ has\ \left(K^{+},X\right) \to\ P\ recognizes\ \sigma\left(K^{-1},X\right)$

- Freshness

F1 $fresh\ \ (X_i)\ \ \to\ \ fresh\ \left((X_1\ ,\cdots, X_n)\right)$

F2 $fresh\ \ (X) \to\ fresh\ \ \left(F(X)\right)$

- Oldness

O1 $old\ \ (t, X_1,\cdots, X_n)\ \ \to\ \ old\ \ (t\ ,\ X_i)$

O2 $old\ \ (t, F(X)) \to\ \ old\ \ (t, X)$

O3 $old(t, X) \wedge\ \ t \le t'\ \ \to\ \ old\ \ \left(t', X\right)$

- Seeing

SE1 $P\ sees\ \ (X_1,\cdots, X_n)\ \ \to\ \ \ P\ sees\ X_i$

SE2 $P\ sees\ \ (X)_k \wedge\ P\ has\ K^{-1} \to\ \ \ P\ sees\ X$

- Saying

NV $P\ said\ X\ \ \wedge\ fresh\ \ (X_i) \to\ \ P\ says\ X$

SA1 $P\ said\ \ (X_1,\cdots, X_n)\ \ \to\ \ P\ said\ X_i$

SA2 $P\ says\ \ \ (X_1,\cdots, X_n)\ \ \to\ \ P\ says\ X_i$

SA3 $P\ said\ \ h(X) \wedge \neg\ P\ sees\ \ h(X) \to P\ said\ X$

SA4 $P\ says\ \ h(X) \wedge \neg P\ sees\ \ h(X) \to P\ says\ X$

- Authentication and key Confirmation

A1 $R\ sees\ \ \ F(K,X) \wedge P \xleftrightarrow{K}$
$Q \wedge \neg P\ \ said\ F(K,X) \to Q\ \ said\ \ (K,X)$

A2 $R\ sees\ \ \ F(K^{-},X) \wedge \sigma \overset{K}{\mapsto} Q$
$\to Q\ \ \ said\ \ \ (K^{-},X)$

A3 $R\ sees\ F(K^{-},X) \wedge\ \ \sigma \overset{K}{\mapsto}_t Q \wedge old\left(t,\ F(K^{-},X)\right)$
$\to Q\ \ \ said\ \ \ (K^{-},X)$

- Comprehension

C $P\ \ \ sees\ \ \ X\ \ \wedge (\ X_P \equiv Y)$
$\to P\ \ believes\ \ P\ \ sees\ \ Y$

C1 $P\ \ \ recognizes\ \ \ X_i\ \ \to$
$(X_1\ ,\cdots, X_n)_P \equiv \left((X)_P\ \ ,\cdots,(X_n)_P\right)$

C2 $P\ \ \ recognizes\ \ \ X \wedge P\ \ has\ \ K^{-}$
$\to\ \ \ (enc(K,X))_P \equiv enc(K, X_P)$

C3 $P\ \ has\ \ \mathrm{X}\ \ \to\ \ \ (h(X))_P \equiv h(X_P)$

C5 $P\ \ \ has\ \ \ \left((K^{+}\ \ ,X)\right) \to$
$\left(\sigma\ \ (K^{-},X)\right)_P \equiv\ \ \left(\sigma(K^{-}\ \ ,X_P)\right)$

- Equivalences

E1 $X \equiv Y$

E2 $X \equiv Y \wedge Y \equiv Z \to X \equiv Z$

E3 $X \equiv Y \to F(X) \equiv F(Y)$

E4
$X_1 \equiv Y_1 \wedge \cdots \wedge X_n \equiv Y_n \to (X_1,\cdots, X_n) \equiv (Y_1,\cdots, Y_n)$

- Key Derivation

S $P \xleftrightarrow{K} Q \to Q \xleftrightarrow{K} P$

- Provability

P1 $P\ canprove\ \ \ (\phi \to \psi)\ \ to\ J\ \ until\ \ t$
$\to \begin{bmatrix} (P\ \ canprove\ \ \ \phi\ \ \ to\ J\ \ until\ \ \ t) \\ \to (P\ \ canprove\ \ \ \psi\ \ \ to\ J\ \ until\ \ t) \end{bmatrix}$

P2 $P\ \ has\ X \wedge\ \ (J\ \ sees\ \ \ X \to J\ \ believes\ \phi)$
$\to\ \ P\ \ canprove\ \ \ \phi\ \ to\ J$

$$\text{P3}\quad \begin{Bmatrix} P\ has\ \sigma(K^{-},X)\ \wedge\ P\ has\ \sigma(K^{+},X) \\ \wedge\ P\ canprove\left(\sigma \overset{K}{\mapsto}_{t} Q\right)\ to\ J \wedge (X_J\ \equiv Y) \end{Bmatrix}$$
$$\rightarrow P\ canprove\ \{Q\ \ said\ \ Y\}\ to\ J\ until\ t$$

$$\text{P4}\quad \begin{Bmatrix} P\ has\ \sigma(K^{-},X) \wedge\ P\ has\ \sigma(K^{+},X) \\ \wedge P\ canprove\ \left(\sigma \overset{K}{\mapsto}_{t} Q\right)\ to\ J\ \wedge (X_J \equiv Y) \wedge \\ P\ canprove\ old(t,\sigma(K^{-},X))\ to\ J \end{Bmatrix}$$
$$\rightarrow\ P\ canprove\ \{Q\ said\ \ Y\}\ to\ J\ until\ t$$

$$\text{P5}\quad \begin{Bmatrix} P\ canprove\ Q\ \ said\ \ h(X)\ to\ J\ until\ t \\ \wedge\ (J\ believes\ \neg Q\ \ sees\ h(X)) \end{Bmatrix}$$
$$\rightarrow P\ canprove\ \{Q\ \ said\ X\}\ to\ J\ until\ t$$

$$\text{P6}\quad \begin{Bmatrix} P\ canprove\{Q\ said(X_1,\cdots,X_n)\}to\ J\ until\ t \\ \rightarrow P\ \ canprove\ \{Q\ said\ (X_i)\}\ to\ J\ until\ t \end{Bmatrix}$$

III. Formalizing Receipt-Freeness

Intuitively, a receipt in the voting system is evidence that can be used to prove that a voter casts a special ballot for a candidate to the vote buyer. This means that a receipt has the following information:

(Information1) receipt includes the evidence that can prove itself identification to the third party, such as registration authority, voter buyer and so on.

(Information2) receipt includes the evidence that can prove that a voter votes a special ballot for a candidate.

(information3) receipt includes the evidence that can prove that special voter, not other voter, votes a special ballot.

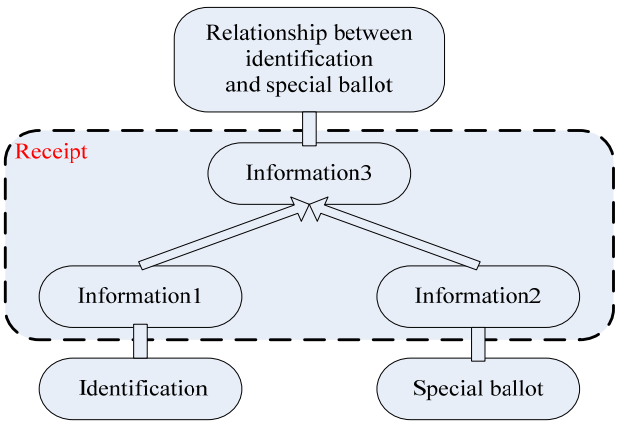

Figure 1. The structure of the information1, information2 and information3.

That means receipt should include Voter_ID (Information1), Ballot (Information2) and the relationship between Voter_ID and Ballot (Information3). Figure1 describes the structure of receipt.

In the following we give the definition of receipt based on V. Kessler and H. Neumann logic.

- Definition of receipt:

If a voting protocol has the following conditions, we said the voting protocol has receipt property.

Condition1:

$$\begin{Bmatrix} \text{voter buyer } believes \text{ voter buyer } canprove \\ \{\text{Authority } said \text{ Voter\_ID}\}\ to\ \text{J}\ until\ \text{t} \end{Bmatrix}$$

The condition1 shows that the voter has his legal identification, Voter_ID , that is issued by the legal authority, not by voter its self or other illegal party.

Condition2:

$$\begin{Bmatrix} \text{voter buyer } believes \text{ voter buyer } canprove \\ \{\text{voter } said \text{ Ballot}\}\ to\ \text{J}\ until\ \text{t} \end{Bmatrix}$$

The condition2 shows that the voter certainly votes a special ballot.

Condition3:

$$\begin{Bmatrix} \text{voter buyer } believes \text{ voter buyer } canprove \\ \begin{Bmatrix} \text{voter } said \text{ Relatioship between} \\ \text{Voter\_ID and Ballot} \end{Bmatrix} \\ to\ \text{J}\ until\ \text{t} \end{Bmatrix}$$

The condition3 shows that the voter who has the legal Voter_ID votes a special ballot, not other voter with Voter_ID votes a special ballot or the legal Voter_ID votes other ballot.

Proving rule P7:

$$\begin{Bmatrix} \begin{bmatrix} \text{voter buyer } believes \text{ voter buyer } canprove \\ \{\text{Authority } said \text{ Voter\_ID}\}\ to\ \text{J}\ until\ \text{t} \end{bmatrix} \\ \wedge \begin{bmatrix} \text{voter buyer } believes \text{ voter buyer } canprove \\ \{\text{voter } said \text{ Ballot}\}\ to\ \text{J}\ until\ \text{t} \end{bmatrix} \\ \wedge \begin{bmatrix} \text{voter buyer } believes \text{ voter buyer } canprove \\ \begin{Bmatrix} \text{voter } said \text{ Relatioship between} \\ \text{Voter\_ID and Ballot} \end{Bmatrix} \\ to\ \text{J}\ until\ \text{t} \end{bmatrix} \end{Bmatrix}$$
$$\rightarrow \text{voter buyer } believes \text{ voter buyer } canprove$$
$$\{\text{voter } said \text{ receipt}\}\ to\ \text{J}\ until\ \text{t}$$

The P7 rule shows that if the voter has a legal identification, Voter_ID , and can generate a special ballot ,and can prove the special ballot is voted by the voter who has the legal identification, Voter_ID , voter buyer can prove voter said or can generate the receipt, which means that the voting protocol has not the receipt-freeness property.

The advantage of the above generic formal framework is that it covers all receipts. We can get a receipt from a particular execution of a voting protocol, also referred to as a run. The public and private information exchanged and the transcripts of information in the computer of

voter during the protocol run can be considered a building block of an associated receipt.

Ⅳ. Application of FOO Voting Protocol

In this part we will present the voting scheme proposed by Fujioka, Okamoto and Ohta in 1992 [23]. FOO is a typical voting protocol. Many voting systems are developed based it, such as MIT EVOX voting system [21] ,Washington Sensus voting system [22].First, we give an informal description, that is used as a basis for an formal description that follows. Then we analyze receipt-freeness with the framework proposed in this paper. At last we point that the protocol is not receipt-freeness

A. *FOO Voting Protocol*

FOO voting protocol consists of two authorities: an administrator and a collector. The administrator is responsible for token issuing; the collector collects the votes and publishes the result of the election. The protocol is composed of initialization stage, registration stage, voting stage, and counting stage. Figure 2 describes the FOO voting protocol.

ID_i : the identification of the voter V_i

σ_i : the V_i's signature scheme

σ_A : the signature scheme of the administrator.

ξ : a secure bit-commitment using the random key k_i

.

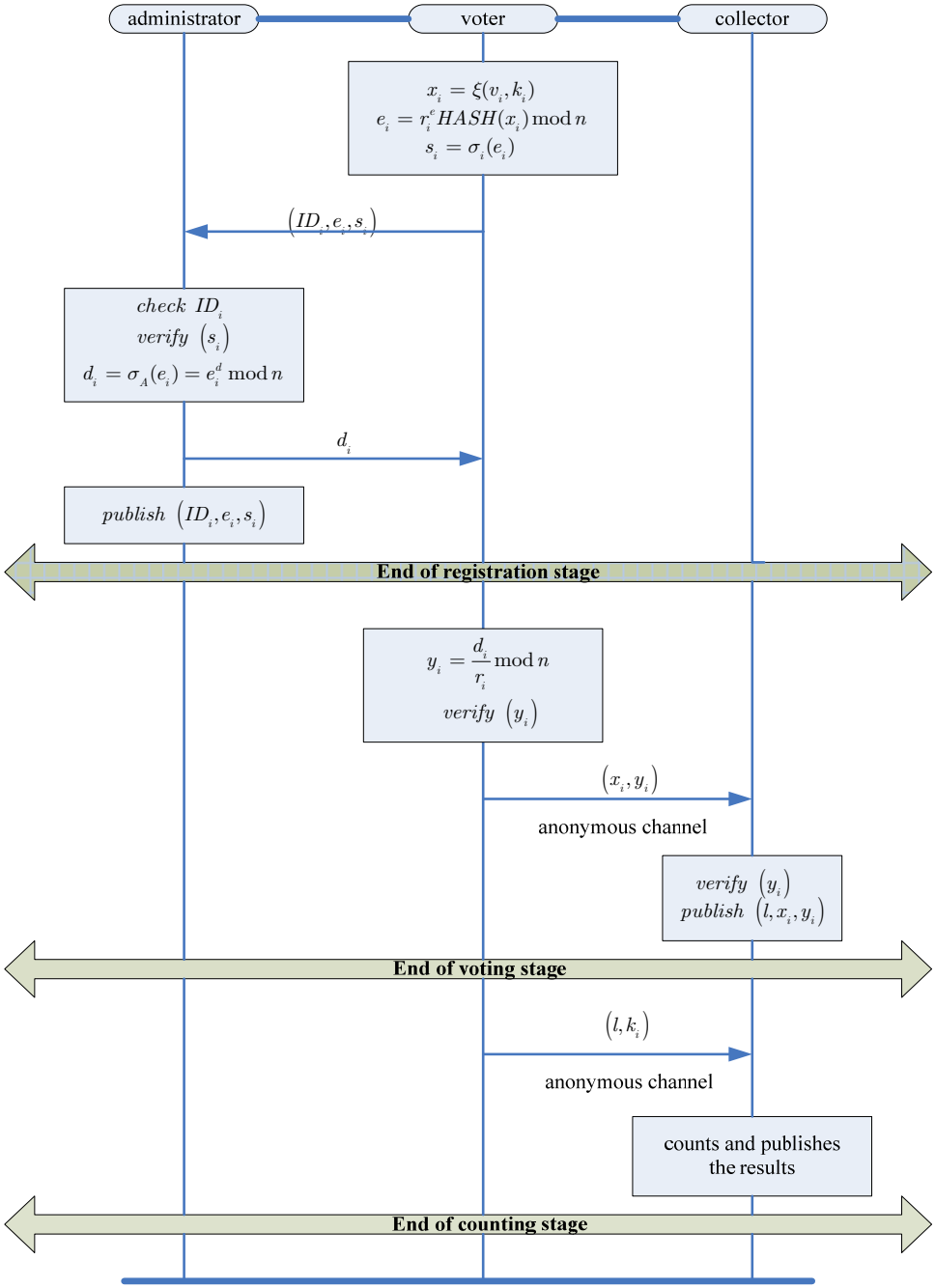

Figure 2. FOO voting protocol

- Initialization stage

Administrator generates and publishes the public key.

- Registration stage

V_i chooses his vote v_i and creates the ballot $x_i = \xi(v_i, k_i)$. V_i computes $e_i = r_i^e HASH(x_i) \bmod n$. V_i generates $s_i = \sigma_i(e_i)$ and sends (ID_i, e_i, s_i) to the administrator.

Administrator A receives (ID_i, e_i, s_i) and checks whether:

V_i has the right to vote; V_i has not yet applied for the signature;The signature s_i is valid.

If all these conditions are satisfied, then the administrator A generates $d_i = \sigma_A(e_i) = e_i^d \bmod n$ and sends it to the voter. If any of these conditions does not hold, the administrator rejects the signature.

At the end of the registration phase, the administrator announces the number of voters who where.

given the administrator's signature, and publishes the list (ID_i, e_i, s_i) .

- Voting stage

V_i retrieves the signature y_i of the ballot x_i by $y_i = \frac{d_i}{r_i} \bmod n$.

V_i checks that y_i is the administrator's signature of the x_i . If the check fails, he claims the disruption by showing that (x_i, y_i) is invalid.

V_i sends his token (x_i, y_i) anonymously to the collector.

The collector C checks the administrator's signature y_i of the ballot x_i . If the check succeeds, C enters (l, x_i, y_i) onto a list as an $l-th$ item.

- Counting stage

Counting stage consists of two phases: Opening and Counting.

Opening phase. When the election ends, the collector C publishes the list (l, x_i, y_i) . V_i then do the following:

V_i checks that the number of ballots in the list is equal to the number of voters. If the check fails,

voter claims this by revealing the token x_i, y_i and the blinding factor r_i .

V_i checks that his ballot is listed on the list. If his vote is not listed, then V_i claims this by revealing (x_i, y_i) , the valid ballot and its signature.

V_i sends (l, k_i) to C through anonymous channel.

Counting phase.

The collector C opens the commitment of the ballot x_i , retrieves the vote V_i , adds k_i and v_i to the list, and checks that the v_i is a valid vote.

C counts the votes and publishes the voting result.

B. *Informal Analysis of Rreceipt-freeness in FOO Voting Protocol*

In the registration stage, the voter chooses a r_i as the blind factor that only himself knows. ID_i is the identification of the voter V_i . $s_i = \sigma_i(e_i)$ is the digital signature of the voter V_i . Because (ID_i, e_i, s_i) are published by administrator, everybody can see it .So the voter can use the transcript of (ID_i, e_i, s_i) to prove to vote buyer that it is produced by him. So the transcript of (ID_i, e_i, s_i) can constitute a part of receipt

In the voting phase, V_i sends his token (x_i, y_i) anonymously to the collector. Because only voter V_i himself knows the blind factor r_i ,so the voter V_i can prove to the vote buyer that the $y_i = \frac{d_i}{r_i} \bmod n$ is produced by himself. So the transcripts of $x_i = \xi(v_i, k_i)$, $e_i = r_i^e HASH(x_i) \bmod n$ and (x_i, y_i) can be used to prove to the vote buyer that (ID_i, e_i, s_i) and (x_i, y_i) are corresponding relationship. So the transcript of production of (x_i, y_i) can be a part of receipt.

According to the protocol the (ID_i, e_i, s_i) , (l, x_i, y_i) , k_i and v_i are published by the authority, receipt is (ID_i, e_i, s_i) and (x_i, y_i)

C. *Formal Analysis of Receipt-freeness in FOO Voting Protocol*

According the previous informal result we give formal analysis of receipt-freeness. The receipt is (ID_i, e_i, s_i) and (x_i, y_i)

$$\text{receipt} = \begin{Bmatrix} ID_i \,||\, r_i^e HASH(\xi(v_i, k_i)) \bmod n \\ ||\, \sigma_i(r_i^e HASH(\xi(v_i, k_i)) \bmod n) \\ ||\, (\xi(v_i, k_i), \sigma_A(\xi(v_i, k_i)) \end{Bmatrix}$$

In order to proving that FOO voting protocol is receipt we need to prove that the following result:

$$\begin{bmatrix} \begin{bmatrix} \text{voter buyer } \textit{believes} \text{ voter buyer } \textit{canprove} \\ \{\text{Authority } \textit{said} \text{ Voter\_ID}\} \ \textit{to} \text{ J } \textit{until} \text{ t} \end{bmatrix} \\ \wedge \begin{bmatrix} \text{voter buyer } \textit{believes} \text{ voter buyer } \textit{canprove} \\ \{\text{voter } \textit{said} \text{ Ballot}\} \ \textit{to} \text{ J } \textit{until} \text{ t} \end{bmatrix} \\ \wedge \begin{bmatrix} \text{voter buyer } \textit{believes} \text{ voter buyer } \textit{canprove} \\ \begin{Bmatrix} \text{voter } \textit{said} \text{ Relatioship between} \\ \text{Voter\_ID and Ballot} \end{Bmatrix} \\ \textit{to} \text{ J } \textit{until} \text{ t} \end{bmatrix} \end{bmatrix}$$

$\rightarrow$ voter buyer *believes* voter buyer *canprove*

$\{$voter *said* receipt$\}$ *to* J *until* t

Owning to the space limitation, we only demonstrate the proving process of:

$$\begin{Bmatrix} \text{voter buyer believes voter buyer } canprove \\ \{\text{voter } said \text{ Ballot}\} \ to \text{ J } until \text{ t} \end{Bmatrix}$$

Our goal:

$$\begin{Bmatrix} \text{voter buyer believes voter buyer } canprove \\ \{\text{voter } said \text{ Ballot}\} \ to \text{ J } until \text{ t} \end{Bmatrix}$$

After an execution of the electronic payment protocol, voter buyer can get the messages of

$$\text{receipt} = \begin{Bmatrix} ID_i \ || \ r_i^e HASH(\xi(v_i,k_i)) \bmod n \ | \\ | \ \sigma_i(r_i^e HASH(\xi(v_i,k_i)) \bmod n) \\ || \ (\xi(v_i,k_i), \sigma_A(\xi(v_i,k_i)) \end{Bmatrix}, \text{ that is}$$

ID_i , $r_i^e HASH\left(\{v_i\}_{k_i}\right) \bmod n$, $\sigma\left(K_V^-, \left(r_i^e HASH\left(\{v_i\}_{k_i}\right) \bmod n\right)\right)$, $\{v_i\}_{k_i}$ $\sigma\left(K_A^-, \left(\{v_i\}_{k_i}\right)\right)$

- Prerequisites

M1: Voter has its public and private keys.

M2: All participants trust into the certification authority and believe that especially the judge shares this trust.

$$\text{P } sees \ Cert\left(Q, K_Q^+, \sigma, t\right) \rightarrow \text{P } believes \ \left\{\sigma \overset{K_Q}{\mapsto}_t \ Q\right\}$$

$$\text{P } believes \ \left(\text{J } sees \ Cert\left(Q, K_Q^+, \sigma, t\right)\right)$$

$$\rightarrow \text{P } believes \ \left\{\sigma \overset{K_Q}{\mapsto}_t \ Q\right\}$$

M3: The certificates are completely understood by everyone.

$$\left[Cert\left(P, K_P^+, \sigma, t\right)\right]_P \equiv Cert\left(P, K_P^+, \sigma, t\right)$$

vote buyer *believes*

$$\left[Cert\left(P, K_P^+, \sigma, t\right)\right]_P \equiv Cert\left(P, K_P^+, \sigma, t\right)$$

M4: Vote buyer can comprehend v_i and M believes J comprehends v_i as well.

$$\left(\{v_i\}_{k_i}\right)_{voter \ buyer} \equiv \{v_i\}_{k_i} ,$$

$$\text{vote buyer } believes \ \left(\{v_i\}_{k_i}\right)_J \equiv \{v_i\}_{k_i}$$

$$\text{vote buyer } recognizes \ \{v_i\}_{k_i} ,$$

$$\text{voter buyer } believes \text{ J } recognizes \ \{v_i\}_{k_i}$$

Neither vote buyer nor J need to understand the hash value $HASH\left(\{v_i\}_{k_i}\right)$ .We only assume voter buyer believes:

$$\left(\left(HASH\left(\{v_i\}_{k_i}\right)\right)_{voter \ buyer}\right)_J \equiv \left(HASH\left(\{v_i\}_{k_i}\right)\right)_{voter \ buyer}$$

M5: Vote buyer believes that no person signs forwarded messages that he doesn't understand. In addition vote buyer believes that J shares his belief.

vote buyer *believes*

$$\left\{\text{J } believes \ \neg\text{A } sees \ HASH\left(\{v_i\}_{k_i}\right)\right\}$$

$$\text{vote buyer } believes \ \neg\text{A } sees \ HASH\left(\{v_i\}_{k_i}\right)$$

- Verification

After the execution of the internet voting protocol, vote buyer can get the messages of ID_i , $r_i^e HASH\left(\{v_i\}_{k_i}\right) \bmod n$, $\sigma\left(K_V^-, \left(r_i^e HASH\left(\{v_i\}_{k_i}\right) \bmod n\right)\right)$, $\{v_i\}_{k_i}$ $\sigma\left(K_A^-, \left(\{v_i\}_{k_i}\right)\right)$

So we have:

vote buyer *sees*

$$\begin{Bmatrix} Cert\left(V, K_V^+, \sigma, t\right), ID_i, r_i^e HASH\left(\{v_i\}_{k_i}\right) \bmod n, \\ \sigma\left(K_V^-, \left(r_i^e HASH\left(\{v_i\}_{k_i}\right) \bmod n\right)\right), \\ \{v_i\}_{k_i}, \sigma\left(K_A^-, \left(\{v_i\}_{k_i}\right)\right) \end{Bmatrix} \quad (1)$$

$$(1), \text{SE1} \rightarrow \text{vote buyer } sees \ Cert\left(V, K_V^+, \sigma, t\right) \quad (2)$$

$$(2), \text{M3,C} \rightarrow \begin{Bmatrix} \text{vote buyer } believes \\ \text{vote buyer } sees \\ Cert\left(V, K_V^+, \sigma, t\right) \end{Bmatrix} \quad (3)$$

$$(3), \text{H1} \rightarrow \begin{Bmatrix} \text{vote buyer } believes \\ \text{vote buyer } has \ Cert\left(V, K_V^+, \sigma, t\right) \end{Bmatrix} \quad (4)$$

$$(4), \text{H2,K} \rightarrow \boxed{\begin{Bmatrix} \text{vote buyer } believes \\ \text{vote buyer } has \ K_V^+ \end{Bmatrix}} \quad (5)$$

$$(4), \text{M2,P2,K} \rightarrow \boxed{\begin{Bmatrix} \text{vote buyer } believes \\ \text{vote buyer } canprove \left\{\sigma \overset{K_V}{\mapsto} t \ V\right\} \end{Bmatrix}} \quad (6)$$

$$(1), \text{SE1} \rightarrow \text{vote buyer } sees \ \{v_i\}_{k_i} \quad (7)$$

$$(7), \text{M4,C} \rightarrow \begin{Bmatrix} \text{vote buyer } believes \\ \text{vote buyer } sees \ \{v_i\}_{k_i} \end{Bmatrix} \quad (8)$$

$$(8), \text{H1,K} \rightarrow \boxed{\left\{\text{vote buyer } believes \text{ voter } has \ \{v_i\}_{k_i}\right\}} \quad (9)$$

$$(1), \text{SE1} \rightarrow \text{ vote buyer } sees \ Cert\left(V, K_V^+, \sigma, t\right) \quad (10)$$

$$(10), \text{SE1} \rightarrow \text{vote buyer } sees \ K_V^+ \quad (11)$$

$$(11), \text{H1} \rightarrow \text{vote buyer } has \ K_V^+ \quad (12)$$

$$(7), \text{H1} \rightarrow \boxed{\text{vote buyer } has \ \{v_i\}_{k_i}} \quad (13)$$

$$(12),(13),\mathrm{M4,C5,E2,E4} \rightarrow \left\{\begin{array}{l}\left[\sigma\left(K_V^-,\left(r_i^e HASH\left(\{v_i\}_{k_i}\right)\bmod n\right)\right)\right]_{vote\ \mathrm{buyer}} \\ \equiv \sigma\left(K_V^-,\left(r_i^e HASH\left(\{v_i\}_{k_i}\right)\bmod n\right)\right)\end{array}\right\} \quad (14)$$

$$(1),\mathrm{SE1},(14),\mathrm{C} \rightarrow \left\{\begin{array}{l}\text{vote buyer } \textit{believes} \text{ vote buyer} \\ \textit{sees } \sigma\left(K_V^-,\left(r_i^e HASH\left(\{v_i\}_{k_i}\right)\bmod n\right)\right)\end{array}\right\} \quad (15)$$

$$(15),\mathrm{K,H1} \rightarrow \boxed{\left\{\begin{array}{l}\text{vote buyer } \textit{believes} \text{ vote buyer} \\ \textit{has } \sigma\left(K_V^-,\left(r_i^e HASH\left(\{v_i\}_{k_i}\right)\bmod n\right)\right)\end{array}\right\}} \quad (16)$$

$$(5),(6),(9),(16),\mathrm{M4,P3,K} \rightarrow \boxed{\left\{\begin{array}{l}\text{vote buyer } \textit{believes} \text{ vote buyer } \textit{canprove} \\ \left\{V \ \textit{said} \ \left(r_i^e HASH\left(\{v_i\}_{k_i}\right)\bmod n\right)\right\} \text{ to J until t}\end{array}\right\}} \quad (17)$$

$$(17),\mathrm{SA1} \rightarrow \left\{\begin{array}{l}\text{vote buyer } \textit{believes} \text{ vote buyer} \\ \textit{canprove}\left\{V \ \textit{said} \ \left(HASH\left(\{v_i\}_{k_i}\right)\right)\right\} \\ \text{to J until t}\end{array}\right\} \quad (18)$$

$$(18),\mathrm{M5,SA3} \rightarrow \left\{\begin{array}{l}\text{vote buyer } \textit{believes} \text{ vote buyer} \\ \textit{canprove } \left\{V \ \textit{said} \ \{v_i\}_{k_i}\right\} \\ \text{to J until t}\end{array}\right\} \quad (19)$$

So we can get:

$$\left\{\begin{array}{l}\text{voter buyer believes voter buyer } \textit{canprove} \\ \{\text{voter } \textit{said} \text{ Ballot}\} \ \textit{to} \text{ J } \textit{until} \text{ t}\end{array}\right\}$$

In the same way we can get the following result:

$$\left\{\begin{array}{l}\left\{\begin{array}{l}\text{voter buyer } \textit{believes} \text{ voter buyer } \textit{canprove} \\ \{\text{voter } \textit{said} \text{ Ballot}\} \ \textit{to} \text{ J } \textit{until} \text{ t}\end{array}\right\} \\ \left\{\begin{array}{l}\text{voter buyer } \textit{believes} \text{ voter buyer } \textit{canprove} \\ \left\{\begin{array}{l}\text{voter } \textit{said} \text{ Relatioship} \\ \text{between Voter\_ID and Ballot}\end{array}\right\} \textit{to} \text{ J } \textit{until} \text{ t}\end{array}\right\}\end{array}\right.$$

So according to P7, we can get he conclusions:

$$\left\{\begin{array}{l}\text{voter buyer } \textit{believes} \text{ voter buyer } \textit{canprove} \\ \{\text{voter } \textit{said} \text{ receipt}\} \ \textit{to} \text{ J } \textit{until} \text{ t}\end{array}\right\}$$

So FOO voting protocol is not receipt-freeness.

V Application of Meng Internet Voting Protocol

In this section we will present the voting scheme proposed by Meng Bo in 2007 [19]. First, we give an informal description, that is used as a basis for an formal description that follows. Then we analyze receipt-freeness with the framework proposed in this paper. At last we point that the protocol is receipt-freeness.

A. Meng Internet Voting Protocol

Meng Internet voting protocol is secure and practical and has the receipt-freeness and coercion-resistant. But it does not formally analyze receipt-freeness.

Meng Internet voting protocol accomplishes receipt-freeness by confidentiality of voter credential and designated verifier proof.

Meng Internet voting protocol consists of preparation phase, registration phase, voting phase and tallying phase.

In 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.

In registration phase firstly voter V_j generates the $ident_j$, then generates message4 and send it to the registration authority RA. RA receives the message and checks $ident_j$ that if it has registered. If voter has not registered, RA verifies $sign\left(ident_j, SK_{V_j}\right)$. If the verification is wrong, RA sends the error message to V_j, the protocol ends. If the verification is right, RA firstly generates $Proof_{V_j}^{A_i}$ based on non-interactive proofs of knowledge that two ciphertexts are encryption of the same plaintext with ElGamal cryptosystem. At last RA generates message5 and sends it to voter V_j through one –way anonymous channel. RA generates $\left(E^C\left(c_{i,j}\right)\right)SK_{A_i}$ and sends it to BB.

In voting phase V_j receives $Proof_{V_j}^{A_i}$ and verifies it through the method in [19]. If the result is right, V_j generates $E^V\left(C_J\right)+E^V\left(B_J^t\right)$ and send it to BB.

In tallying phase tallying authority TA tallies the ballot and publishes its results in BB.

B. Formal Analysis of Receipt-freeness in Meng Internet Voting Protocol

After an execution of the protocol the voter can send the message4-7 to vote buyer. Because the voter buyer can't know the authority' private key, he can't open the message4: $ENV_{PK_i}\left(SK_j\left(ident_j\right), ident_j, PK_j\right)$ and don't know the information $ident_j$.Owning to the voter can tell his relative private key to the voter buyer, so the voter buyer can open the message5: $ENV_{PK_j}\left(E^V\left(c_{i,j}\right), Proof_{V_j}^{A_i}\right)$ and get the information $E^V\left(c_{i,j}\right), Proof_{V_j}^{A_i}$.

After a run the vote buyer can get $E^V\left(c_{i,j}\right), Proof_{V_j}^{A_i}$ and $E^V\left(C_J\right)+E^V\left(B_J^t\right)$.The vote buyer wants to use

TABLE I. THE MESSAGE DATA STRUCTURE OF MENG INTERNET VOTING PROTOCOL [16]

Voting phase	message	message data structure
$Preparation\ phase$	$message_1$	$Public/private\ keys\ of\ authorities$
	$message_2$	$Public/private\ keys\ of\ voters$
	$message_3$	$AK \rightarrow BB : B^t, sign\left(B^t, PK_{AK}\right)$
$Registration\ phase$	$message_4$	$V_j \rightarrow RA : ENV_{PK_i}\left(SK_j\left(ident_j\right), ident_j, PK_j\right)$
	$message_5$	$RA \rightarrow V_j : ENV_{PK_j}\left(E^V\left(c_{i,j}\right), Proof_{V_j}^{A_i}\right)$
$Voting\ phase$	$message_6$	$V_j \rightarrow BB : E^V\left(C_J\right) + E^V\left(B_J^t\right)$
$Tallying\ phase$	$message_7$	$TA \rightarrow BB : tallyresult$

this information to construct a receipt.

Owning to ElGamal cryptosystem is used in the protocol and it is probabilistic encryption, the vote buyer can ask voter provide the transcripts of generating $E^V\left(C_J\right) + E^V\left(B_J^t\right)$ to decide whether it is created by voter. If the voter can provide the transcript, the voter is the creator of the $E^V\left(C_J\right) + E^V\left(B_J^t\right)$. $E^V\left(C_J\right)$ is Voter_ID and $E^V\left(B_J^t\right)$ is ballot. Then voter buyer can get:

$$\left\{\begin{array}{l}\text{voter buyer } believes \text{ voter buyer } canprove \\ \{\text{voter } said \text{ Ballot}\}\ to\ \text{J}\ until\ \text{t}\end{array}\right\}$$

$$\left\{\begin{array}{l}\text{voter buyer } believes \text{ voter buyer } canprove \\ \left\{\begin{array}{l}\text{voter } said \text{ Relatioship} \\ \text{between Voter\_ID and Ballot}\end{array}\right\}\ to\ \text{J}\ until\ \text{t}\end{array}\right\}$$

Next vote buyer must get:

$$\left\{\begin{array}{l}\text{voter buyer } canprove \\ \{\text{Authority } said \text{ Voter\_ID}\}\ to\ \text{J}\ until\ \text{t}\end{array}\right\}$$

$Proof_{V_j}^{A_i}$ is a proof that the $E^V\left(c_{i,j}\right)$ is generated by authority. Voter checks equality between credential got from authority and credential in BB by proof of knowledge that two ciphertexts are encryption of the same plaintext $Proof_{V_j}^{A_i}$. The other people cannot check owning to the specialty of designated verifier proof.

According to the specialty of designated verifier proof voter has the ability of generation of a false $Proof_{V_j}^{A_i}$. The vote buyer cannot check $Proof_{V_j}^{A_i}$ and cannot verify of $E^V\left(C_J\right)$.

So according to P7 we can't get:

$$\left\{\begin{array}{l}\text{voter buyer } believes \text{ voter buyer } canprove \\ \{\text{voter } said \text{ receipt}\}\ to\ \text{J}\ until\ \text{t}\end{array}\right\}$$

So Meng Internet voting protocol is receipt-freeness.

VI CONCLUSION

Formal method is an important tool to assess receipt-freeness of internet voting protocols We proposed a formal logic framework for receipt-freeness based on V. Kessler and H. Neumann logic. Our approach focuses on establishing what can construct a receipt. This enables the identification of receipts, and provides a heuristic to take receipts into consideration in the early stages of designing a protocol .Our method is simple and it is easy to be generalized.

Example of FOO voting protocol demonstrates that the protocol is not receipt-freeness. The receipt can be $\left(ID_i, e_i, s_i\right)$ and $\left(x_i, y_i\right)$. In order to make it receipt-freeness we can use tamper-resistant equipments such as usbkey, smart card and so on. Meng voting protocol is receipt-freeness.

In the future we will work on give a formal framework of the coercion-resistance, eligibility, fairness, university verification, privacy, completeness, soundness, unreusability, and invariableness with the formal method

REFERENCES

[1] Benaloh J,Tuinstra D.Receipt-free secret-ballot elections.In Proceedings of the 26th ACM Symposium on Theory of Computing.New York:ACM Press,1994,pp.544-553.

[2] Ari Juels , Markus Jakobsson. Coercion-resistant electronic elections, 2002. http://www.vote-auction.net/voteauction/165.pdf

[3] Hugo L. Jonker, Erik P. de Vink: Formalising Receipt-freeness. 476-488, Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, Bart Preneel (Eds.): Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings. Lecture Notes in Computer Science 4176 Springer 2006, pp. 476-488.

[4] Martin Hirt , Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In the proceeding of EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, LNCS 1807, 2000,pp. 539–556.

[5] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In the proceeding of 5th International Workshop on Security Protocols, Paris, France, LNCS 1361,April 07 - 09 1997,pp. 25–35.

[6] Kazue Sako , Joe Kilian. Receipt-free mix-type voting scheme. In the proceeding of International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Springer-Verlag, LNCS 921, 1995,pp.393–403.
[7] Youngcheon Lee , Kwangjo Kim. Receipt-free electronic voting through collaboration of voter and honest verifier, 2000. http://citeseer.nj.nec.com/lee00receiptfree.html.
[8] Emmanouil Magkos, et al. Receipt-freeness in large-scale elections without untappable channels. In the proceeding of I3E, 2001, pp. 683–694.
[9] Byoungcheon Lee , Kwangjo Kim. Receipt-free electronic voting scheme with a tamper resistant randomizer. In the proceeding of ICISC2002, Seoul, Korea, November 28-29, 2002, pp. 405–422.
[10] Olivier Baudron,et al. Practical multi-candidate election system. In the proceeding of the Twentieth Annual ACM Symposium on Principles of Distributed Computing, August 26-29, 2001, Newport, Rhode Island, USA. ACM, 2001,pp. 274–283.
[11] Josh C. Benaloh. Verifiable secret-ballot elections. PhD Thesis, Yale University, Department of Computer Science, 1987. Number 561.
[12] Aggelos Kiayias, Moti Yung. The vector-ballot e-voting approach. http://theory.lcs.mit.edu/~rivest/voting/papers/KiayiasYung-TheVectorBallotEVotingApproach.pdf
[13] Andrew Neff. Detecting malicious poll site voting clients, http://votehere.com/vhti/documentation/psclients.pdf.
[14] David chaum, Secret-Ballot Receipts:True Voter-Verifiable Elections, IEEE security and privacy, January-February 2004 (Vol. 2, No. 1),pp.38-47..
[15] Zuzana Rja¡¦skov´a, Electronic Voting Schemes, master thesies. Department of Computer Science Faculty of Mathematics, Physics and Informatics Comenius University, Bratislava, April 2002.
[16] Meng bo, zhang huanguo. Practical internet voting protocol without strong physical assumption, Wuhan University Journal of Natural Sciences, Volume 12, Number 1 / January 2007,pp.177-180.
[17] S. Delaune, S. Kremer, and M.D. Ryan. Receipt-freeness: Formal definition and fault attacks (extended abstract). In proceedings of the Workshop Frontiers in Electronic Elections, Milan, Italy, September 2005.
[18] S. Delaune, S. Kremer, and M.D. Ryan.Coercion-resistance and receipt-freeness in electronic voting In proceedings of 19th IEEE Computer Security Foundations Workshop, Venice, Italy, 5-7 July 2006 ,pp. 28-42.
[19] Bo Meng. An Internet Voting Protocol with Receipt-Free and Coercion-resistance, In proceedings of 7th IEEE International Conference on Computer and Information Technology, Aizu-Wakamatsu, Fukushima, Japan, 16-19 Oct. 2007,pp.721-726.
[20] Volker Kessler, Heike Neumann. A Sound Logic for Analysing Electronic Commerce Protocols. Proceedings of the 5th European Symposium on Research in Computer Security, September 16 - 18, 1998 . Lecture Notes In Computer Science; Vol. 1485,pp.345 – 360.
[21] EVOX Voting System,http://groups.csail.mit.edu/cis/voting/voting.html
[22] Lorrie Faith Cranor , Ron K. Cytron. Sensus: A Security-Conscious Electronic Polling System for the Internet, Proceedings of the Hawai`i International Conference on System Sciences, January 7-10, 1997, Wailea, Hawai`i, USA IEEE CS press,pp.561-570.
[23] Atshushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. a practical secret voting scheme for large scale elections. In the proceeding of Auscrypt ’92, Springer-Verlag, LNCS 718, 1992, pp. 244–251.

Bo Meng was born in 1974 He got his doctor degree from Wuhan University of Technology in 2003 in P.R.China; From 2004 to 2006, he work in Wuhan University as a postdoc in P.R.China.

Currently he is a Full Associate Professor of School of Computer, South-Center University for Nationalities in P.R.China.. He has authored/coauthored over 40 papers in International/National journals and conferences. His current research interests include information security, formal method, electronic commerce, internet voting, and protocol security.