http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 7 (8): 1133-1140, 2008
ISSN 1812-5638

Formal Analysis of Key Properties in the Internet Voting Protocol Using Applied Pi Calculus

Bo Meng
School of Computer, South-Center University for Nationalities,
Wuhan, 430074, Hubei, People's Republic of China

Abstract: The internet voting protocols is the core part of the internet voting system. In order to put the internet voting protocols into practice they should have several key properties, such as privacy, completeness, soundness, unreusability, fairness, eligibility and invariableness, universal verifiability, receipt-freeness and coercion-resistance. Formal method is an important tool to assess these properties. But most of these properties are analyzed with informal method. The applied pi calculus can be used to model and verify the security protocols, such as internet voting protocol. In this study, firstly, privacy and coercion-resistance properties are researched. Then a typical internet voting protocol is modeled with applied pi calculus. Thirdly privacy and coercion-resistance of the typical internet voting protocol are analyzed with applied pi calculus. According to the result of analysis the typical internet voting protocol has privacy and coercion-resistance properties.

Key words: Internet voting protocol, privacy, coercion-resistance, formal method

INTRODUCTION

With the popularization of Internet and advance of process of democracy of nation, a new voting system called Internet voting is introduced. The internet voting protocol is the core part of the internet voting system. 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 (Benaloh and Tuinstra, 1994), coercion-resistance (Juels and Jakobsson, 2002; Juels *et al*., 2005).

Privacy describes the fact that a particular voted in a particular way is not revealed to anyone. Its purpose aims to guarantee that the link between a given voter and his vote remains hidden. Anonymity and privacy properties have been successfully studied.

However, research on privacy in the field of voting protocols is rather subtle. While generally most security properties should hold against many dishonest participants and authorities coalitions.

To ensure privacy we need to hide the link between the voter and the vote and not the voter or the vote itself. Coercion-resistance is introduced by Juels and Jakobsson (2002) and should offers not only receipt-free, but also defense against randomization, forced-abstention and simulation attacks.

Research on coercion-resistance is at the beginning. It is firstly researched by Juels and Jakobsson (2002) and Acquisti (2004), which mainly applied the credential of voter and designated verifier proof to accomplish it. Voter can cheat the coercer by producing a false credential. Owning to designate verifier proof the coercer cannot verify the proof.

Recently internet voting protocols (Acquisti, 2004; Juels *et al*., 2005; Meng, 2007) were proposed without the strong physical assumptions. Meng (2007) is the improvement of the protocols (Acquisti, 2004; Juels *et al*., 2005) which applies the idea and addresses the problems of protocols (Acquisti, 2004; Juels *et al*., 2005).

Meng protocol is a practical and efficient internet voting protocol and doesn't use strong physical assumptions in the implementation of these properties. This is the trend of advance in Internet voting protocol. But Meng (2007) does not analyze privacy and coercion-resistance with formal methods.

Formal method is the key tool to assess properties of internet voting protocols. Many universal formal methods have been proposed to analyze security protocols. Owning to specialties of internet voting protocol, Delaune (2006) introduced a formal model for analyzing privacy, receipt-freeness and coercion-resistance of internet voting protocol. Kremer and Ryan (2005) have used the applied pi calculus to analyze the protocol (Fujioka *et al*., 1992). Lee *et al*. (2004) protocol is analyzed by Ryan *et al*. (2006) with applied pi calculus.

The purpose of the study is to use DKR model (Delaune *et al*., 2006) to analyze privacy and coercion-resistance in Meng protocol.

PRIVACY AND COERCION-RESISTANCE IN DKR MODEL

In DKR model, it uses the applied pi calculus to formalize the privacy and coercion-resistance of internet voting protocol. Privacy is formalized as an observational equivalence. Coercion-resistance is expressed in terms of adaptive simulation and labeled bisimilarity. In the following we describe the definition of privacy and coercion-resistance. The other contents of DKR model can be found (Delaune *et al*., 2006).

DKR point out the informal and formal definition of privacy:

- **Informal definition of privacy:** The system cannot reveal how a particular voter voted
- **Formal definition of privacy:** A voting protocol respects privacy, if:

$$S\left[V_A\left\{{}^{a}/_{v}\right\} \mid V_B\left\{{}^{b}/_{v}\right\}\right] \approx_l S\left[V_A\left\{{}^{b}/_{v}\right\} \mid V_B\left\{{}^{c}/_{v}\right\}\right]$$

The idea is that if the attacker can't find if arbitrary honest voters V_A and V_B exchange their votes, then in general he can't know anything about how V_A (or V_B) voted. We can find that this definition is robust even in situations where the result of the election is such that the votes of V_A and V_B are necessarily revealed.

At the same time DKR give the informal and formal definition of coercion-resistance:

- **Informal definition of coercion-resistance:** A voter cannot cooperate with a coercer to prove to him that she voted in a certain way

The coercer has not only the ability that gets the information from observing the election process but also the ability that can interact with the voter.

The coercer can be an active attacker.

- **Formal definition of coercion-resistance:** A voting protocol is coercion-resistance if there have a closed extended process V' and a strict evaluation context C such that:

$$S\left[V_A\left\{{}^{c}/_{v}\right\}^{c_1,c_2} \mid V_B\left\{{}^{\alpha}/_{v}\right\}\right] \leq_\alpha S\left[V' \mid V_B\left\{{}^{x}/_{v}\right\}\right]$$

$$vc_1,c_2.C\left[V_A\left\{{}^{c}/_{v}\right\}^{c_1,c_2}\right] \approx_l V_A\left\{{}^{c}/_{v}\right\}^{chc}$$

$$vc_1,c_2.C[V']^{\setminus out(chc,\cdot)} \approx_l V_A\left\{{}^{\alpha}/_{v}\right\}$$

The ideas of this definition is that whenever the coercer requests a given vote on the left-hand side then V_B can change his vote according to the right-hand side and counterbalance the outcome. However, we need to avoid the case where $V' = V_A\{{}^{c}/_{v}\}^{c_1,c_2}$ letting V_B vote α. Therefore we require that when we apply a context C, intuitively the coercer, requesting $V_A\{{}^{c}/_{v}\}^{c_1,c_2}$ to vote c, V' in the same context votes α. There may be circumstances where V' may need not to cast a vote that is not α.

THE SIMPLIFIED VERSION OF MENG PROTOCOL

Meng protocol is secure and practical with related properties. But it does not formally analyze these properties. Here we describe the simplified version in Fig. 1 in order to concentrate on the key aspect on privacy and coercion-resistance.

Meng 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 it 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 verifies $ident_j$ that if it has registered. If voter has not registered, RA verifies $sign(ident_j, SK_{V_j})$. If the verification is wrong, RA sends the error message to V_j, the protocol ends. If the verification is right, RA generates $Proof_{V_j}^{RF}$

$$\text{Preparation phase}\begin{cases}\text{message}_1 & AK \rightarrow \text{RAandTA}: PK^C, SK^C, PK^V, SK^V, PK_{RA}, SK_{RA}\\ \text{message}_2 & AK \rightarrow V_j: PK_{V_j}, SK_{V_j}\\ \text{message}_3 & AK \rightarrow BB: B^t, sign\left(B^t, PK_{AK}\right)\end{cases}$$

$$\text{Registration phase}\begin{cases}\text{message}_4 & V_j \rightarrow RA: penc\left(\left(sign\left(ident_j, SK_{V_j}\right) \| ident_j\right), PK_{RA}\right)\\ \text{message}_6 & RA \rightarrow V_j: penc\left(\left(penc\left(C_j, PK^V\right) \| proof_{V_j}^{RA}\right), PK_{V_j}\right)\end{cases}$$

$$\text{Voting phase}\ \left\{\text{message}_8 \quad V_j \rightarrow BB: penc\left(C_j, PK^V\right) \| penc\left(B_J, PK^V\right)\right.$$

$$\text{Tallying phase}\ \left\{\text{message}_7 \quad TA \rightarrow BB: \text{tallyresult}\right.$$

Fig. 1: Simplified version of Meng protocol

based on non-interactive proofs of knowledge that two ciphertexts are encryption of the same plaintext with ElGamal crypto system. At last RA generates message 5 and sends it to voter V_j through one-way anonymous channel. At the same time RA creates penc (C_J, PK^C) and send it to BB.

In voting phase V_j receives $proof_{v_j}^{RA}$ and verifies it. If the result is right, V_j generates penc (C_j, PK^V)‖penc(B_j, PK^V) and send it to BB.

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

MODELING MENG SIMPLIFIED PROTOCOL WITH APPLIED PI CALCULUS

We use the applied pi calculus (Abadi and Fournet, 2001) to model Meng simplified protocol. Figure 2 describes the functions and Fig. 3 describes the equational theory in Meng simplified protocol.

We model cryptography in a Dolev-Yao style as being perfect. Digital signature is modeled as being signature with message recovery, i.e., the signature itself contains the signed message which can be extracted using the checksign function.

The main process is modeled in Fig. 4. In this model the main process consists of preparation process, registration process, voting process and tallying process (Fig. 4). At the same time it sets up private channels. These processes are described in detail in the following parts.

The preparation process is modeled in Fig. 5. In the model authority AK generates the public/private ElGamal keys. The private keys of voter and RA and TA are sent by secure channel. RA generates uotechoice(t) and sends it to BB.

Where, x is a fresh free variable value.

The registration process can be modeled in Fig. 6. In this model voter V_j creates:

$$\text{penc}\left(\begin{pmatrix}\text{sign}(\text{ident}_j, SRK_{v_j})\,\|\,\text{ident}_j\end{pmatrix}, \\ PUK_{RA}\right)$$

and sends it to RA. RA verifies sign ($ident_j$, SRK_{v_j}) If the verification is true, RA generates:

$$\text{penc}\left(\begin{pmatrix}\text{penc}(C_j, PUK^V), proof_{v_j}^{RA}\end{pmatrix}, \\ PUK_{v_j}\right)$$

and sends it to V_j through one-way anonymous channel. At the same time RA generates penc (C_j, PK^C) and sends it to BB.

$$\begin{aligned}
&\text{Fun pdec}(x,y) && (*\text{decrypt x with the key y}*)\\
&\text{Fun penc}(x,y) && (*\text{encrypt x with the key y}*)\\
&\text{Fun hash}(m) && \begin{pmatrix}*\text{hash function with}\\ \text{the input is m}*\end{pmatrix}\\
&\text{Fun sign}(x,y) && (*\text{sign x with the key y}*)\\
&\text{Fun checkproof}(x) && (*\text{check proof x}*)\\
&\text{Fun checksign}(x,y) && \begin{pmatrix}*\text{verify the signature x}\\ \text{with the key y}*\end{pmatrix}\\
&\text{Fun projectioni}(x) && \begin{pmatrix}*\text{select the ith field}\\ \text{in formatted message in x}*\end{pmatrix}
\end{aligned}$$

Fig. 2: Functions in Meng simplified protocol

$$\begin{aligned}
&\text{Equation pdec}(\text{penc}(x,SK),PK) = x\\
&\text{Equation pdec}(\text{penc}(x,PK),SK) = x\\
&\text{Equation checkproof}\left(proof_{v_j}^{RA}\right) = \text{ok}\\
&\text{Equation checksign}(\text{sign}(x,SK),PK) = \text{true}\\
&\text{Equation penc}(x,y)\otimes\text{penc}(z,y) = \text{penc}(x+z,y)\\
&\text{Equation projectioni}(x_1,x_2,\cdots,x_t) = x_i
\end{aligned}$$

Fig. 3: Equational theory in Meng simplified protocol

$$\begin{aligned}
&\text{Main process} =\\
&(*\text{private channels}*)\\
&\text{v skcch. v skvch. v skrach. v skv}_j\text{ch. v skakch. v ch2}\\
&\begin{pmatrix}\text{preparation process}\,|\,\text{registration process}\\ |\ \text{voting process}\,|\,\text{tallying process}\end{pmatrix}
\end{aligned}$$

Fig. 4: Main process

$$\begin{aligned}
&\text{let preparation process} =\\
&\nu\ SK^C.\nu\ SK^V.\nu\ SK^{RA}.\nu\ SK_{v_j}.\nu\ SK_{AK}\quad (*\text{private keys}*)\\
&\text{out}(pkcch,PK^C).\ \text{out}(pkvch,PK^V).\ \text{out}(pkrach,PK^{RA}).\\
&\text{out}(pkv_j\text{ch},PK_{v_j}).\ \text{out}(pkakch,PK_{AK})\quad (*\text{sending public keys}*)\\
&\text{out}(skcch,SK^C).\text{out}(skvch,SK^V).\text{out}(skrach,SK^{RA}).\\
&\text{out}(skv_j\text{ch},SK_{v_j}).\text{out}(skakch,SK_{AK})\quad (*\text{sending private keys}*)\\
&\text{in}(pkakch,PUK_{AK})\quad (*\text{receiving public key}*)\\
&\text{let } B^t\,\|\,\text{sign}(B^t,PUK_{AK}) = \text{votechoice}(t)\ \text{in}\\
&\text{out}(bbch,\text{votechoice}(t))\qquad (*\text{sending votechoice(t) to BB}*)
\end{aligned}$$

Fig. 5: Preparation process

The voting process is described in Fig. 7. In the model V_j receives the m5 and decrypt m5 with the private key SRK_{v_j} to recover encrypt (C_J, PUK^V)‖ $ndupproof_{v_j}^{RA}$. Then V_j uses the projection function to extract $ndupproof_{v_j}^{RA}$, which is the evidence that prove that the

$$
\begin{aligned}
&\text{let registration process} = \\
&\quad \text{in}\left(\text{pkv}_j\text{ch},\text{PUK}_{v_j}\right).\ \text{in}\left(\text{skv}_j\text{ch},\text{SRK}_{v_j}\right) \quad (\text{*receive } V_j \text{ public and private keys*}) \\
&\quad \text{in}\left(\text{pkrach},\text{PUK}_{RA}\right).\ \text{in}\left(\text{skrach},\text{SRK}_{RA}\right) \quad (\text{*receive RA public and private keys*}) \\
&\quad \text{in}\left(\text{pkvch},\text{PUK}^{V}\right).\ \ \text{in}\left(\text{pkcch},\text{PUK}^{C}\right) \\
&\quad \text{phase1} \\
&\quad \text{let penc}\left(\left(\text{sign}\left(\text{ident}_j,\text{SRK}_{v_j}\right)\|\,\text{ident}_j\right),\text{PUK}_{RA}\right) = \text{m1 in} \\
&\quad \text{out}\left(\text{ch1},\text{m1}\right).\quad \text{in}\left(\text{ch1},\text{m2}\right) \\
&\quad \text{let pdec}\left(\text{m2},\text{SRK}_{RA}\right) = \text{m3 in} \\
&\quad \text{if checksign}\left(\text{m3},\text{PUK}_{v_j}\right) = \text{true then} \quad (\text{*check signature *}) \\
&\qquad \left\{\begin{array}{l} \text{let penc}\left(\left(\text{penc}\left(C_j,\text{PUK}^{V}\right),\text{proof}_{v_j}^{RA}\right),\text{PUK}_{v_j}\right) = \text{m4 in} \\ \text{out}\left(\text{ch2},\text{m4}\right).\text{out}\left(\text{ch3},\text{penc}\left(C_J,\text{PUK}^{C}\right)\right) \end{array}\right\}
\end{aligned}
$$

Fig. 6: Registration process

$$
\begin{aligned}
&\text{let voting process} = \\
&\quad \text{in}\left(\text{ch2},\text{m5}\right).\text{in}\left(\text{skv}_j\text{ch},\text{SRK}_{v_j}\right).\text{in}\left(\text{pkvch},\text{PUK}^{V}\right) \\
&\quad \text{phase1} \\
&\quad \text{let pdec}\left(\text{m5},\text{SRK}_{v_j}\right) = \text{encrypt}\left(C_J,\text{PUK}^{V}\right)\|\,\text{ndvpproof}_{v_j}^{RA} \text{ in} \\
&\quad \text{let encrypt}\left(C_J,\text{PUK}^{V}\right)\|\,\text{ndvpproof}_{v_j}^{RA} = \text{m6 in} \\
&\quad \text{let projection2}\left(\text{m6}\right) = \text{ndvpproof}_{v_j}^{RA} \text{ in} \\
&\quad \text{if checkproof}\left(\text{ndvpproof}_{v_j}^{RA}\right) = \text{true then} \\
&\qquad \left\{\begin{array}{l} \text{let projection1}\left(\text{m6}\right) = \text{encrypt}\left(C_J,\text{PUK}^{V}\right) \text{ in} \\ \text{let penc}\left(C_J,\text{PUK}^{V}\right)\|\,\text{penc}\left(B_J,\text{PUK}^{V}\right) = \text{ballot in} \\ \text{out}\left(\text{ballotch},\text{ballot}\right) \quad (\text{*sending ballot to BB*}) \end{array}\right\}
\end{aligned}
$$

Fig. 7: Voting process

$$
\begin{aligned}
&\text{let tallying process} = \\
&\quad \text{in}\left(\text{ballot},\text{bbballot}\right) \quad (\text{*receive ballot *}) \\
&\quad \text{phase1} \\
&\quad \text{let projection1}\left(\text{bbballot}\right) = \text{encrypt}\left(C_j,\text{PUK}^{V}\right) \text{ in} \\
&\quad \text{let projection2}\left(\text{bbballot}\right) = \text{encrypt}\left(B_J,\text{PUK}^{V}\right) \text{ in} \\
&\quad \text{let encrypt}\left(C_j,\text{PUK}^{V}\right)\otimes\text{encrypt}\left(B_j,\text{PUK}^{V}\right) = \text{encrypt}\left(C_j+B_j,\text{PUK}^{V}\right) \text{ in} \\
&\quad \text{in}\left(\text{bbch},\text{vote}\right) \\
&\quad \text{in}\left(\text{ch3},\text{encrypt}\left(C_J,\text{PUK}^{C}\right)\right) \\
&\quad \text{let encrypt}\left(C_J,\text{PUK}^{C}\right)\otimes\text{encrypt}\left(C_J,\text{PUK}^{C}\right) \\
&\quad = \text{encrypt}\left(C_J+B_t,\text{PUK}^{C}\right) \text{ in} \\
&\quad \text{let tallying}\left(\begin{array}{l}\text{encrypt}\left(C_j+B_j,\text{PUK}^{V}\right),\\ \text{encrypt}\left(C_J+B_t,\text{PUK}^{C}\right)\end{array}\right) = \text{tallyresult in} \\
&\quad \text{phase2} \\
&\quad \text{out}\left(\text{resultch},\text{tallyresult}\right)
\end{aligned}
$$

Fig. 8: Tallying process

encrypt (C_J, PUK^V) and penc (C_J, PUK^V) are ciphertext of the same plaintext C_J. $Ndupproof_{V_j}^{RA}$ is a non-interactive designated verifier proof. The V_j verifies the proof $ndupproof_{V_j}^{RA}$. If the result is true V_j uses projection functions to get encrypt (C_J, PUK^V) from m6. Finally it creates ballot penc (C_J, PUK^V)‖penc (B_J, PUK^V) and sends it to BB

The tallying process is modeled in Fig. 8. In the model the BB receives the ballot bbballot, then uses the projection function to extract encrypt (C_j, PUK^V) and encrypt (B_j, PUK^V). Finally TA tally based the homomorphic encryption property and publishes the results in BB.

ANALYSIS OF PRIVACY WITH DKR MODEL

We do not give full formal proofs here owning to multifarious procedure and the space the limitation. According the DKR model, in order to prove privacy, we need to show:

$$S\left[V_A\left\{a/v\right\} \mid V_B\left\{b/v\right\}\right] \approx_1 S\left[V_A\left\{b/v\right\} \mid V_B\left\{c/v\right\}\right]$$

According to the definition of privacy, in order to get the proof of privacy, we need to suppose that at least two voters are honest. We denote the voters V_1 and V_2 and their votes ballotuoter 1 and ballotuoter 2, respectively. We say that a voting protocol respects privacy whenever a process where, V_1 votes ballotuoter 1 and V_2 votes ballotuoter 2 is observationally equivalent to a process where, V_1 votes ballotuoter 2 and V_2 votes ballotuoter 1.

The processes modeling the two voters are shown in Fig. 9.

The proof can be sketched as follows. The only difference between:

$$(\text{voting process})\left[\text{ballotvoter1}/V_1, \text{ballotvoter2}/V_2\right]$$

and

$$(\text{voting process})\left[\text{ballotvoter2}/V_1, \text{ballotvoter1}/V_2\right]$$

lies in the two voter processes. We therefore first show that:

$$P = (\text{voting process1} \mid \text{voting process2})\left[\text{ballotvoter1}/V_1, \text{ballotvoter2}/V_2\right]$$

$$\approx_1$$

$$Q = (\text{voting process1} \mid \text{voting process2})\left[\text{ballotvoter2}/V_1, \text{ballotvoter1}/V_2\right]$$

$$P \xrightarrow{vx_1.out(ch,x_1)} \left(P_1 \mid \left\{\text{penc}\left(C_J\text{voter1},PUK^V\right) \| \text{penc}\left(B_J\text{voter1},PUK^V\right)/x_1\right\}\right)$$

$$\xrightarrow{vx_2.out(ch,x_2)} \begin{pmatrix} P_2 \mid \left\{\text{penc}\left(C_J\text{voter1},PUK^V\right) \| \text{penc}\left(B_J\text{voter1},PUK^V\right)/x_1\right\} \\ \mid \left\{\text{penc}\left(C_J\text{voter2},PUK^V\right) \| \text{penc}\left(B_J\text{voter2},PUK^V\right)/x_2\right\} \end{pmatrix}$$

Similarly

$$Q \xrightarrow{vx_1.out(ch,x_1)} \left(Q_1 \mid \left\{\text{penc}\left(C_J\text{voter2},PUK^V\right) \| \text{penc}\left(B_J\text{voter2},PUK^V\right)/x_1\right\}\right)$$

$$\xrightarrow{vx_2.out(ch,x_2)} \begin{pmatrix} Q_2 \mid \left\{\text{penc}\left(C_J\text{voter2},PUK^V\right) \| \text{penc}\left(B_J\text{voter2},PUK^V\right)/x_1\right\} \\ \mid \left\{\text{penc}\left(C_J\text{voter1},PUK^V\right) \| \text{penc}\left(B_J\text{voter1},PUK^V\right)/x_2\right\} \end{pmatrix}$$

$$
\begin{aligned}
&(*\ \text{voter1}\ *)\\
&\text{let voting process1} =\\
&\quad \text{in}(\text{ch2},\text{m5voter1}).\text{in}(\text{skv}_j\text{ch},\text{SRK}_{v_j}).\text{in}(\text{pkvch},\text{PUK}^{v})\\
&\quad \text{phase1}\\
&\quad \text{let pdec}(\text{m5voter1},\text{SRK}_{v_j}) = \text{encrypt}(\text{C}_j\text{voter1},\text{PUK}^{v}) \,\|\, \text{ndvpproof}_{v_j}^{RA}\text{voter1 in}\\
&\quad \text{let encrypt}(\text{C}_j\text{voter1},\text{PUK}^{v}) \,\|\, \text{ndvpproof}_{v_j}^{RA}\text{voter1} = \text{m6voter1 in}\\
&\quad \text{let projection2}(\text{m6voter1}) = \text{ndvpproof}_{v_j}^{RA}\text{voter1 in}\\
&\quad \text{if checkproof}(\text{ndvpproof}_{v_j}^{RA}\text{voter1}) = \text{true then}\\
&\quad\quad \left\{\begin{array}{l}
\text{let projection1}(\text{m6voter1}) = \text{encrypt}(\text{C}_j\text{voter1},\text{PUK}^{v}) \text{ in}\\
\text{let penc}(\text{C}_j\text{voter1},\text{PUK}^{v}) \,\|\, \text{penc}(\text{B}_j\text{voter1},\text{PUK}^{v}) = \text{ballotvoter1 in}\\
\text{phase1}\\
\text{out}(\text{ballotch},\text{ballotvoter1}) \qquad (*\text{sending ballot to BB}*)
\end{array}\right.\\
&(*\ \text{voter2}\ *)\\
&\text{let voting process2} =\\
&\quad \text{in}(\text{ch2},\text{m5voter2}).\text{in}(\text{skv}_j\text{ch},\text{SRK}_{v_j}).\text{in}(\text{pkvch},\text{PUK}^{v})\\
&\quad \text{phase1}\\
&\quad \text{let pdec}(\text{m5voter2},\text{SRK}_{v_j}) = \text{encrypt}(\text{C}_j\text{voter2},\text{PUK}^{v}) \,\|\, \text{ndvpproof}_{v_j}^{RA}\text{voter2 in}\\
&\quad \text{let encrypt}(\text{C}_j\text{voter2},\text{PUK}^{v}) \,\|\, \text{ndvpproof}_{v_j}^{RA}\text{voter2} = \text{m6voter2 in}\\
&\quad \text{let projection2}(\text{m6voter2}) = \text{ndvpproof}_{v_j}^{RA}\text{voter2 in}\\
&\quad \text{if checkproof}(\text{ndvpproof}_{v_j}^{RA}\text{voter2}) = \text{true then}\\
&\quad\quad \left\{\begin{array}{l}
\text{let projection1}(\text{m6voter2}) = \text{encrypt}(\text{C}_j\text{voter2},\text{PUK}^{v}) \text{ in}\\
\text{let penc}(\text{C}_j\text{voter2},\text{PUK}^{v}) \,\|\, \text{penc}(\text{B}_j\text{voter2},\text{PUK}^{v}) = \text{ballotvoter2 in}\\
\text{phase1}\\
\text{out}(\text{ballotch},\text{ballotvoter2}) \qquad (*\ \text{sending ballot to BB}\ *)
\end{array}\right.
\end{aligned}
$$

Fig. 9: Two voters for analyzing privacy property

Note that the use of phase is the key to hold privacy in the protocol. The phrase is a global synchronization command. The process first executes all instructions of a given phase before moving to the nest phase. When we omit the synchronization after the registration phase with the administrator, privacy is violated.

ANALYSIS OF COERCION-RESISTANCE WITH DKR MODEL

We also do not give full formal proofs here owning to multifarious procedure and the space the limitation. According to the DKR model, in order to prove concerion-resistance, we need to show:

$$
\begin{aligned}
&S\left[V_A\left\{{}^{c}/_{v}\right\}^{c_1,c_2} \mid V_B\left\{{}^{\alpha}/_{v}\right\}\right] \leq_{\alpha} S\left[V' \mid V_B\left\{{}^{x}/_{v}\right\}\right]\\
&vc_1,c_2.C\left[V_A\left\{{}^{c}/_{v}\right\}^{c_1,c_2}\right] \approx_1 V_A\left\{{}^{c}/_{v}\right\}^{chc}\\
&vc_1,c_2.C\left[V'\right]^{\backslash out(chc,\bullet)} \approx_1 V_A\left\{{}^{\alpha}/_{v}\right\}
\end{aligned}
$$

We only introduce the ideas on how to construct the voting process' and context C.

For coercion-resistance the coercer can provides the inputs for the messages and make voter to send it out to BB. If the coercer prepares messages corresponding to a given vote, voter can fake the scripts and know that voter will counterbalance the outcome, by adaptively choosing the same vote. The possible voting process' and the possible context C required for the definition of coercion resistance are shown in Fig. 10 and 11.

The idea is that voting process' to use fake C_j to vote a and sent the $\text{fakendupproof}_{v_j}^{RA}$ to the context C, it is the coercer and attacker. outputting scripts $\text{fakendupproof}_{v_j}^{RA}$ to the coercer. Voting process' prepares all outputs as if he uses a C_J voting c. The context C can't find the truth. The context C creates its own vote and send it to voting process'. The key part is that, using his private key, the voter

$$
\begin{aligned}
&\text{let voting process}'= \\
&\quad \nu\, \text{fake}C_J. \\
&\quad \text{in}\left(\text{pkv}_j\text{ch}, \text{PUK}_{v_j}\right).\ \text{in}\left(\text{pkvch}, \text{PUK}^V\right). \\
&\quad \text{out}\left(\text{cpkv}_j\text{ch}, \text{PUK}_{v_j}\right).\text{out}\left(\text{cpkvch}, \text{PUK}^V\right) \\
&\quad \text{let penc}\left(\left(\text{penc}\left(\text{fake}C_J, \text{PUK}^V\right), \text{fakeproof}_{V_j}^{RA}\right), \text{PUK}_{V_j}\right) = \text{fakem4 in} \\
&\quad \text{let pdec}\left(\text{fakem4}, \text{SRK}_{V_j}\right) = \text{encrypt}\left(\text{fake}C_J, \text{PUK}^V\right) \| \text{fakendvpproof}_{V_j}^{RA} \text{ in} \\
&\quad \text{let encrypt}\left(\text{fake}C_J, \text{PUK}^V\right) \| \text{fakendvpproof}_{V_j}^{RA} = \text{fakem5 in} \\
&\quad \text{out}\left(\text{fakech}, \text{fakem5}\right) \\
&\quad \text{let projection2}\left(\text{fakem5}\right) = \text{fakendvpproof}_{V_j}^{RA} \text{ in} \\
&\quad \text{if checkproof}\left(\text{fakendvpproof}_{V_j}^{RA}\right) = \text{true then} \quad (*\text{check fake proof}*) \\
&\quad \left\{\begin{array}{l} \text{let projection1}\left(\text{m5}\right) = \text{encrypt}\left(\text{fake}C_J, \text{PUK}^V\right) \text{ in} \\ \text{let penc}\left(\text{fake}C_J, \text{PUK}^V\right) \| \text{penc}\left(B_J, \text{PUK}^V\right) = \text{fakeballot in} \\ \text{out}\left(\text{ballotch}, \text{fakeballot}\right) \quad (*\text{send fake ballot to BB}*) \end{array}\right\} \\
&\quad \text{in}\left(\text{efakech}, \text{cm6}\right) \quad (*\text{receive cm6 }*) \\
&\quad \text{let projection2}\left(\text{em6}\right) = \text{cfakendvpproof}_{V_j}^{RA} \text{ in} \\
&\quad \text{if checkproof}\left(\text{cfakendvpproof}_{V_j}^{RA}\right) = \text{true then} \quad (*\text{check fake proof}*) \\
&\quad \left\{\begin{array}{l} \text{let projection1}\left(\text{em6}\right) = \text{encrypt}\left(\text{cfake}C_J, \text{cPUK}^V\right) \text{ in} \\ \text{in}\left(\text{cchoicech}, \text{cvote}\right) \\ \text{let encrypt}\left(\text{cfake}C_J, \text{cPUK}^V\right) \| \text{penc}\left(\text{ccB}_J, \text{ccPUK}^V\right) = \text{cfakeballot in} \\ \text{out}\left(\text{cballotch}, \text{cfakeballot}\right) \quad (*\text{send fake ballot to BB}*) \end{array}\right\}
\end{aligned}
$$

Fig. 10: Voting process

$$
\begin{aligned}
&\text{let context } C = \\
&\quad \text{in}\left(\text{fakech}, \text{fakem6}\right) .\text{in}\left(\text{cpkv}_j\text{ch}, \text{cPUK}_{v_j}\right).\text{in}\left(\text{cpkvch}, \text{cPUK}^V\right) \\
&\quad \text{let projection2}\left(\text{fakem6}\right) = \text{cfakendvpproof}_{V_j}^{RA} \text{ in} \\
&\quad \text{if checkproof}\left(\text{cfakendvpproof}_{V_j}^{RA}\right) = \text{true then} \quad (*\text{check fake proof}*) \\
&\quad \left\{\begin{array}{l} \text{let penc}\left(\text{cB}_J, \text{cPUK}^V\right) = \text{cchoice in} \\ \text{out}\left(\text{cchoicech}, \text{cchoice}\right) \quad (*\text{send context choice}*) \\ \text{out}\left(\text{efakech}, \text{fakem6}\right) \end{array}\right\}
\end{aligned}
$$

Fig. 11: Context C: attacker

provides a $\text{fakendupproof}_{V_j}^{RA}$, proving that $\text{fake}C_J$ is legal credential of voter V_j, which make the coercer believe that he can use it to vote its special ballot.

CONCLUSION

The secure and practical Internet voting protocols should have privacy, completeness, soundness, unreusability, fairness, eligibility and invariableness, universal verifiability, receipt-freeness and coercion-resistance. Firstly, we talk about the privacy and coercion-resistance. Secondly, a typical internet voting protocol is modeled with applied pi calculus. Finally the typical protocol with DKR privacy and coercion-resistance formal model is analyzed. The result shows that the protocol has the privacy and coercion-resistance properties.

In the future we will work on analysis of the eligibility, fairness, university verification, completeness, soundness, unreusability and invariableness with the applied pi calculus.

NOTATIONS

+	:	Addition operator
⊗	:	Multiplication operator in homomorphic encryption
‖	:	Concatenation
l	:	The no. Of the voters in the election
V_j	:	The jth legal voter (j = 1, 2, ..,*l*)
B^t	:	The ba;;ot which the voter vote the tth candatite
AK	:	Authority for generating the keys of TA, RA and voter
TA	:	The registration authority
BB	:	Bullion board
C_j	:	RA creates the secret number for V_j' credential
PK^C	:	The public key of RA and TA
SK^C	:	The private key of RA and TA
PK^V	:	The public key of RA and TA
SK^V	:	The private key of RA and TA
PK_{RA}	:	The public key of RA, the public key is used when the voter register
SK_{RA}	:	The private key of RA, the private key is used when the voter register
PK_{AK}	:	The public key of AK
SK_{AK}	:	The private key of AK
PK_{v_j}	:	The public key of voter V_j
SK_{v_j}	:	The private key of voter V_j
$Proof_{v_j}^{RA}$	:	The non-interactive designated verifier proof of knowledge that penc(C_j, PK^V) and penc (C_j, PK^C) are the ciphertext of C_j, which is generated by RA for V_j
$ident_j$	:	The identification of voter V_j

REFERENCES

Abadi, M. and C. Fournet, 2001. Mobile values, new names and secure communication. Proceeding of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, 2001, London, UK., pp: 104-115.

Acquisti, A., 2004. Receipt-free homomorphic elections and write-in voter verified ballot. CMU-ISRI-04-116, 2004, Carnegie Mellon Institute for Software Research International. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-electronic_voting.pdf.

Benaloh, J. and D. Tuinstra, 1994. Receipt-free secret-ballot elections. Proceeding of the 26th Annual ACM Symposium on Theory of Computing, May 23-25, Montréal, Québec, Canada, pp: 544-553.

Delaune, S., S. Kremer and M.D. Ryan, 2006. Coercion-resistance and receipt-freeness in electronic voting protocol. Proceedings of 19th IEEE Computer Security Foundations Workshop, July 2006, Venice, Italy, pp: 28-42.

Fujioka, A., T. Okamoto and K. Ohta, 1992. A practical secret voting scheme for large-scale elections. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, December 13-16, Springer-Verlag, London, UK., pp: 244-251.

Juels, A. and M. Jakobsson, 2002. Coercion-resistance electronic elections. RSA Laboratories, Bedford, MA 01730, USA. http://www.vote-auction.net/VOTEAUCTION/165.pdf.

Juels, A., D. Catalano and M. Jakobsson, 2005. Coercion-resistance electronic elections Proceeding of the 2005 ACM Workshop on Privacy in the Electronic Society, November 7-7, Alexandria, VA., USA., pp: 61-70.

Kremer, S. and M.D. Ryan, 2005. Analysis of an electronic voting protocol in the applied Pi calculus. Lecture Notes Comput. Sci., 3444: 186-200.

Lee, B., C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yood, 2004. Providing receipt-freeness in mixnet based voting protocols. Proceeding of the 6th International Conference on Information Security and Cryptology, November 27-28, Springer Berlin/Heidelberg, UK., pp: 1-14.

Meng, B., 2007. An internet voting protocol with receipt-free and coercion-resistant. Proceedings of 7th IEEE International Conference on Computer and Information Technology, October 16-19, IEEE Computer Society, Washington DC, USA., pp: 721-726.

Ryan, K.M. and S.S. Delaune, 2006. Verifying properties of electronic voting protocols. Proceedings of IAVoSS Workshop on Trustworthy Elections, 2006, Robinson College, Cambridge, UK., pp: 1-8.