A Coercion-Resistant Internet Voting Protocol

Bo Meng
School of Computer, South-Center University For Nationalities
Wuhan, Hubei, P.R.China 430074
mengbo@263.net.cn

Abstract

Internet voting protocol is the core of the Internet voting systems. People are focusing on the implementation of coercion-resistant. A coercion-resistant protocol achieves not only receipt-free but also defense against randomization, forced-abstention, and simulation. In this paper, we present an Internet voting protocol that achieves coercion-resistant with few physical assumptions based on designated verifier Proof and proof of knowledge that two ciphertexts are encryption of the same plaintext. In the last we prove that the protocol is invariableness, receipt-free and coercion-resistant.

1. Introduction

With the popularization of Internet, a new voting scheme called Internet voting is introduced. Internet voting is that voting done by using a computer to cast a ballot over the Internet. Internet voting can be classified four types: remote Internet voting, kiosk Internet voting, polling places Internet voting, and precinct Internet voting. Unless otherwise indicated, when we say Internet voting we mean remote Internet voting.

Internet voting protocols is the key of the Internet voting system. Internet voting protocol can be classified into two types according as if they need authority. One type needs not authority, such as [1]. This kind of protocols is fewer. The other type needs authority, which can be categorized by different technologies into three schemes: homomorphic encryption scheme, blind signature scheme, Mix net scheme.

Homomorphic encryption schemes [2~17] mainly use the homomorphic encryption technology. The voter cooperates with the authorities in order to construct an encryption of his vote. Due to homomorphic property, an encryption of the sum of the votes is obtained by multiplying the encrypted votes of all voters. Finally, the result of the election is computed from the sum of the votes, which is jointly decrypted by the authorities. The purposes of homomorphic encryption method are protection of the voter's privacy and advancement of the efficacy of tallying ballots. Generally the homomorphic encryption scheme is not receipt-free

The blind signature is mainly used in blind signatures schemes [18~25]. The voter firstly obtains a token, a blindly signed message unknown to anyone except himself. Next, the voter sends his token together with his vote anonymously. These protocols require voter's participation in more rounds. The blind signatures scheme is not receipt-free because the blinding factor can be used to construct receipt.

Mix net schemes [8,13,26~,32] base on Mix net that is to permute and modify the sequence of objects in order to hide the correspondence between elements of original and final sequence. It can be used to implement anonymous channel.

The practical Internet voting protocols should have the following properties:

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

Expanded properties: universal verifiability, receipt-free [2,18], coercion-resistant [12]

People are focusing on the implementation of these properties. At present the hot point are how to realize coercion-resistant with few assumptions and constraints.

A lot of protocols use ad hoc physical assumption or the trusted third party to accomplish receipt-free and coercion-resistant properties. For example, one- or two-way untappable channels and/or anonymous or private channels, in [5,8,12,18,26]; third-party (trusted) honest verifiers, in [35]; smart cards, in [29]; voting booth, in [2,33]; the third randomizer, in [5,13,34]; tamper-resistant randomizer, in [9]; deniable encryption, such as [38,40]

* Foundation item: Supported by the Foundation of South-Center University for Nationalities (YZZ06026)

Second International Conference on Systems and Networks Communications (ICSNC 2007)
0-7695-2938-0/07 $25.00 © 2007 IEEE

Acquisti present a protocol in [10] that is better in the implementation of the expanded prosperities. It doesn't use strong physical assumption. Acquisti protocol mainly applied designated verifier proof to accomplish it. Voter can cheat the coercer by producing a false credential. Owning to designate verifier proof the coercer can't verify the proof. But according to our analysis of Acquisti protocol, we find that it has the following problems:

a. It is not invariableness.

In acquisti protocol the voter can use per credential to vote many times. In other words the voter can use per credential to vote the same ballot many times and also can use per credential to vote different ballot many times. In the tallying phrase the author only think about the status that the voter uses per credential to vote the same ballot many times. The other status doesn't be considered in Acquisti protocol. On that status the voter uses per credential to vote different ballot many times we use the search algorithm in the tallying phrase, the tally result may be different. So it is not invariableness. This is an important problem.

b. It is not receipt-free and coercion-resistant.

According to the definition of coercion-resistant we know that if Internet protocol is not receipt-free, it is not coercion-resistant. So we first point that the acquisti protocol is not receipt-free.

In acquisti protocol $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ is send by the authority through a tappable channel. That means the vote buyer can get $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ and know that it is send by the authority. E^{v_j} represents RSA cryptosystem under v_j's public key.

The voter can prove that $E^V\left(c_{i,j}\right),P_{v_j}$ is the decryption of $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ to the vote buyer with the public key of v_j and the property of RSA encryption.

$E^S\left(E^V\left(C_j+B_j^t\right)\right)$ is published on the bulletin board in acquisti protocol.

Generally voter can successfully verifies the designated verifier proof P_{v_j} of equality between $E^V\left(c_{i,j}\right)$ and the corresponding $E^C\left(c_{i,j}\right)$.

So the voter can reveal how to generate the ballot $E^S\left(E^V\left(C_j+B_j^t\right)\right)$, which means that voter can provide the transcript of production of $E^S\left(E^V\left(C_j+B_j^t\right)\right)$ to vote buyer. The transcript of production of $E^S\left(E^V\left(C_j+B_j^t\right)\right)$, $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ and $E^V\left(c_{i,j}\right),P_{v_j}$ can be constructed a receipt.

So acquisti protocol is not receipt-free.

According to the definition of coercion-resistant the acquisti protocol is not coercion-resistant.

In this paper we present an Internet voting protocol that achieves coercion-resistant with few physical assumptions.

2. The proposed Internet voting protocol

In order to solve these problems we propose a new Internet voting protocol, which has the following specialties: privacy, completeness, soundness, fairness, invariableness, universal verifiability, receipt-free and coercion-resistant with few physical constraints

The proposed Internet voting protocol applies the Encryption technologies which include threshold ElGamal cryptosystem, Mix net [27,36], homomorphic encryption, proof of knowledge that two ciphertexts are encryption of the same plaintext [5,10,11], designated verifier Proof of knowledge for equality of discrete logarithms [11].

We assume that the private key is private. There is a one-way anonymous channel from authorities to the voters in preparation phase.

Our proposed Internet voting protocol consists of preparation phase, voting phase and tallying phase.

- **Preparation phase**

Authority A_i creates L random numbers c, representing shares of credentials, for each eligible voter v_j. We represent each share as $c_{i,j}$, with $j=1\cdots\cdots l$ for each A_i. For each $c_{i,j}$, A_i performs

two operations: first, it encrypts $c_{i,j}$ using PK^C and appropriate secret randomization, signs the resulting ciphertext with SK_i^C, and publishes it on BB on a row publicly reserved for the shares of credential of voter v_j:

$$\left(E^C\left(c_{i,j}\right)\right)SK_{A_i}$$

SK_{A_i} represents the signature of authority A_i

Second, A_i also encrypts $c_{i,j}$ using PK^V and appropriate secret randomization, without signing it, but attaching to it a designated verifier proof P_{v_j} of equality of plaintexts $E^C\left(c_{i,j}\right)$ and $E^V\left(c_{i,j}\right)$. The proof is designated to be verifiable only by v_j. A_i encrypts this second message with v_j 's public key and sends it v_j through an one- way anonymous channel:

$$E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$$

E^{v_j} represents RSA encryption under v_j 's public key.

◆ **Voting phase**

For each encrypted share of credential she receives, v_j verifies the designated verifier proof of equality between $E^V\left(c_{i,j}\right)$ and the corresponding $E^C\left(c_{i,j}\right)$ that has been signed and published in her reserved area of BB. Upon successful verification, she multiplies together the shares $E^V\left(c_{i,j}\right)$

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

:

Where with C_j ψwe define the sum of the various shares of credentials .The voter then chooses the ballot-shares $E^V(b_1^t),\cdots,E^V(b_s^t)$, which correspond to her vote choice t from the list of permissible ballot published on the board. Then v_j generates:

$$E^V(C_J)E^V\left(B_j^t\right)=E^V\left(\sum_{i=1,\cdots,s}c_{i,j}+\sum_{i=1,\cdots,s}b_{i,j}^t\right)\equiv E^V(C_J+B_J^t)$$

$$\psi$$

and sends $E^S\left(E^V(C_J+B_J^t)\right)$ to the bulletin-board.

◆ **Tallying phase**

After the voting the authority computing:

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

Then, it mixes all $E^C\left(C_J\right)$, for $J=1\cdots\cdots l$, by re-encrypting (and self-blinding) the original ciphertexts using the credentials public parameters, PK^C.

Authority removes the repeated ballot.

Authority decrypts

$$E^S\left(E^V(C_J+B_J^t)\right)\ J=1,\cdots,l,\cdots,x$$

with SK_i^S, VK^S, VK_i^S. ←Authority then mixes the resulting ciphertexts, by re-encrypting (and self-blinding) the original ciphertexts using the vote's public parameters, PK^V.

Authority thus obtains two lists:

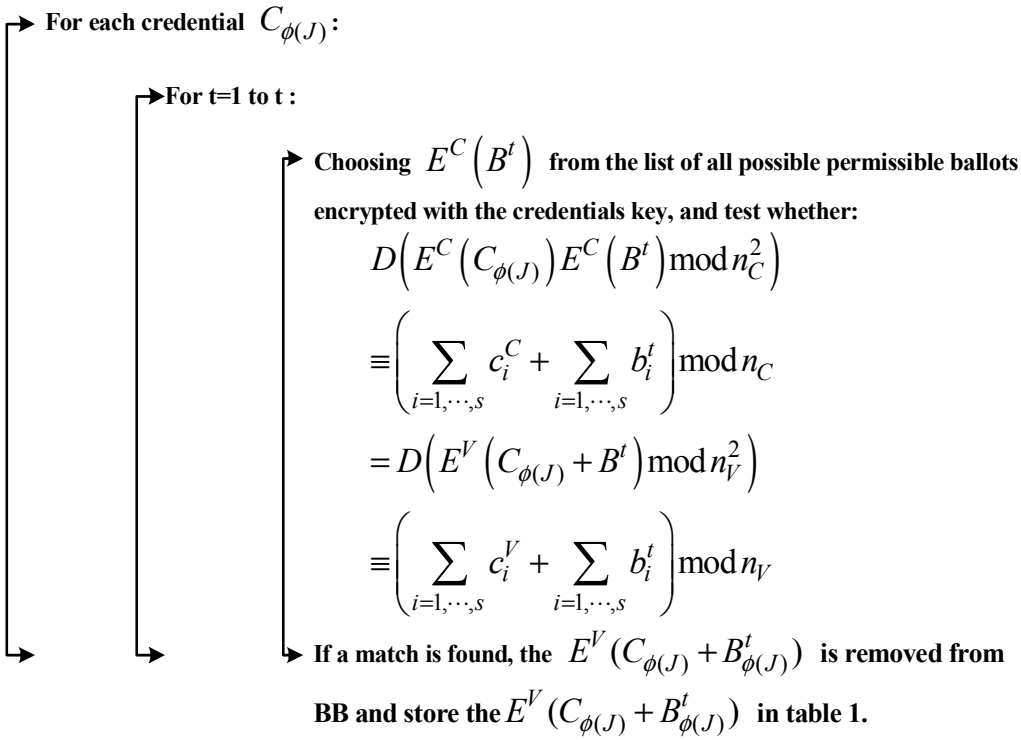
$E^C\left(C_{\phi(J)}\right)$ and $E^V(C_{\phi(J)}+B_{\phi(J)}^t)$ on BB.

Authority also obtains the encrypted ballots $E^C\left(B^t\right)$.

Finally execute the following search algorithm:

1. Choosing a credential $C_{\phi(J)}$ from the list $E^C\left(C_{\phi(J)}\right)$

2.



3. If finding that a $C_{\phi(J)}$ match several $E^V(C_{\phi(J)}+B^t_{\phi(J)})$, then according to the rules we can choose one $E^V(C_{\phi(J)}+B^t_{\phi(J)})$ as a valid ballot and $E^V(C_{\phi(J)}+B^t_{\phi(J)})$'corresponding ***t*** is counted in the tally result, the credential $C_{\phi(J)}$ is removed from the list of valid credentials.

4. The algorithm restarts from 1 with a different $C_{\phi(J)}$.

5. When all credentials $C_{\phi(J)}$ have been considered, the tallying is complete.

3. Properties analysis of the proposed Internet voting protocol

Owning to the space limitation we only analyze invariableness, receipt-free, coercion-resistant

- Invariableness

In the proposed protocol the voter can use per credential to vote the same ballot many times and also can use per credential to vote different ballot many times. But in the tallying phrase the search algorithm can deal with the two statuses. The tallying result is not variable. So it is invariableness.

- Receipt-free

In the proposed protocol, $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ is sent by the authority through a one-way anonymous channel.

That means the vote buyer don't know that $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ is sent by the authority.

The voter can't prove that $E^V\left(c_{i,j}\right),P_{v_j}$ is the decryption of $E^{v_j}\left(E^V\left(c_{i,j}\right),P_{v_j}\right)$ that is sent from authority. So the voter can't reveal how to generate the vote $E^S\left(E^V\left(C_j+B_j^t\right)\right)$ that is compatible with the receipt $E^S\left(E^V\left(C_j+B_j^t\right)\right)$ and

$E^{v_j}\left(E^{V}\left(c_{i,j}\right),P_{v_j}\right)$. So the proposed protocol is receipt-free.

◆ Coercion-resistant

According to definition of coercion-resistant, firstly the proposed protocol is receipt-free, and then we prove that it can prevent randomization attack, forced-abstention attack and simulation attack.

(1) Randomization attack

Voter wants to prevent randomization attack. He can generate a false credential to cheat coercer because coercer can't recognize it true or false owning to the specialty of designated verifier proof. Then voter can use true credential to vote a ballot. So the protocol can prevent randomization attack.

(2) Forced-abstention attack

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

(3) Simulation attack

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

4. Conclusion

The secure and practical Internet voting protocols should have the following properties: privacy, completeness, soundness, unreusability, fairness, eligibility, and invariableness, universal verifiability, receipt-free, coercion-resistant. The hot point is implementation of receipt-free and coercion-resistant without strong physical assumptions. In this paper we propose a new Internet voting protocol with the properties of invariableness, receipt-free and coercion-resistant, which promote the development of Internet voting protocols.

In the future we will work on the Internet voting secure model based on Applied PI calculus.

5. References

[1] R. A. DeMillo, N. A. Lynch, M. Merritt, Cryptographic Protocols, In the proceeding of Of 14th Annual ACM Symposium on Theory of Computing, 1982: 383-400.

[2] Josh Benaloh, Dwight Tuinstra. Receipt-free secret-ballot elections. In the proceeding of STOC '94, 1994:544–553.

[3] Ronald Cramer, Matthew Franklin, Berry Schoenmakers, Moti Yung. Multi-authority secret ballot elections with linear work. In the proceeding of EUROCRYPT '96, Springer-Verlag, LNCS1070, 1996: 72–83.

[4] Ronald Cramer, Rosario Gennaro, Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In the proceeding of EUROCRYPT '97, Springer-Verlag, LNCS 1233, 1997: 103–118.

[5]Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Guillaume Poupard, JAcquistiues Stern. Practical multi-candidate election system. In the proceeding of PODC '01, ACM, 2001: 274–283.

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

[7]Ivan Damg°ard, Mads Jurik, Jesper Buus Nielsen. A generalization of paillier's public-key system with applications to electronic voting, 2003. http://citeseer.ist.psu.edu/cache/papers/cs/27234/http:zSzzSzwww.daimi.au.dkzSz~ivanzSzGenPaillier_finaljour.pdf/damgard03generalization.pdf

[8]Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In the proceeding of EUROCRYPT '00, Springer-Verlag, LNCS 1807, 2000: 539–556.

[9] Byoungcheon Lee , Kwangjo Kim. Receipt-free electronic voting scheme with a tamperresistant randomizer. In the proceeding of ICISC2002, 2002: 405–422.

[10] Alessandro Acquistiuisti. Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots, Technical Report 2004/105, International Association for Cryptologic Research, May 2, 2004, and Carnegie Mellon Institute for Software Research International, CMU-ISRI-04-116, 2004. http://www.heinz.cmu.edu/~Acquistiuisti/papers/Acquistiuisti-electronic_voting.pdf

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

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

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

[14] Ari Juels, Dario Catalano, Markus Jakobsson: Coercion-resistant electronic elections. One older version was at Cryptology ePrint Archive: Report 2002/165 http://eprint.iacr.org/; latest version on Juels web page: http://www.rsasecurity.com/rsalabs/node.asp?id=2030 as of June 2005.

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

[16] Kazue Sako and Joe Kilian. Secure voting using partial compatible homomorphisms. In the proceedings of CRYPTO'94, Springer-Verlag, LNCS 839, 1994: 248–259.

[17] David Chaum. Secret-ballot receipts and transparent integrity. Draft, 2002. www.vreceipt.com/article.pdf.

[18] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In the proceeding of Security Protocols Workshop, Springer-Verlag, LNCS 1361, 1997: 25–35.

[19] David Chaum. Elections with unconditionally- secret ballots and disruption equivalent to breaking rsa. In the

proceeding of EUROCRYPT ’98, Springer-Verlag, LNCS 330, 1988: 177–182.
[20] 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. 244–251.
[21]Michael J. Radwin, An untraceable, universally verifiable voting scheme, http://www.radwin.org/michael/projects/voting.html
[22] Wen-Sheng Juang, Chin-Laung Lei, Pei-Ling Yu. A verifiable multi-authorities secret elections allowing abstaining from voting. International Computer Symposium, Tainan, Taiwan, 1998.
[23] Patrick Horster, Markus Michels, Holger Petersen. Blind multisignature schemes and their relevance to electronic voting. In the proceeding of 11th Annual Computer Security Applications Conference. IEEE Press, 1995: 149–156.
[24] Lorrie Cranor and Ron Cytron. Sensus: A security-conscious electronic polling system for the Internet. In the proceedings of the Hawaii International Conference on System Sciences, 1997.
[25]Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. An improvement on a practical secret voting scheme. In the proceedings of ISW ’99, 1999: 225–234.
[26] Kazue Sako , Joe Kilian. Receipt-free mix-type voting scheme. In the proceeding of EUROCRYPT ’95, Springer-Verlag, LNCS 921,1995:393–403.
[27]Choonsik Park, Kazutomo Itoh, Kaoru Kurosawa. Efficient anonymous channel and all/nothing election scheme. In the proceeding of Advances Cryptology - EUROCRYPT’93, Springer-Verlag, 1993: 248–259.
[28]Markus Jakobsson, Ari Juels, and Ronald L. Rivest. Making mix nets robust for electronic voting by randomized partial checking. In the proceeding of USENIX ’02, 2002: 339–353.
[29] Emmanouil Magkos, Mike Burmester, and Vassilios Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In the proceeding of I3E, 2001: 683–694.
[30] Birgit Pfitzmann. Breaking an efficient anonymous channel. In the proceedings of EUROCRYPT ’94. Springer-Verlag, LNCS 950, 1995: 332–340.
[31] Markus Michels , Patrick Horster. Some remarks on a receipt-free and universally verifiable mix-type voting scheme. In the proceedings of ASIACRYPT ’94, Springer-Verlag, LNCS 1163, 1996: 125–132.
[32] Masayuki Abe. Universally verifiable mix-net with verification work independent of the number of mix-servers. In the proceedings of EUROCRYPT ’98,. Springer-Verlag, LNCS 1403, 1998: 437–447.
[33]Andrew Neff. Detecting malicious poll site voting clients, 2003. http://votehere.com/vhti/documentation/psclients.pdf.
[34] Aggelos Kiayias, Moti Yung. The vector-ballot e-voting approach. http://theory.lcs.mit.edu/~rivest/voting/papers/KiayiasYung-TheVectorBallotEVotingApproach.pdf
[35] Byoungcheon Lee , Kwangjo Kim. Receipt-free electronic voting through collaboration of voter and honest verifier, 2000. hhttp://citeseer.nj.nec.com/lee00receiptfree.html.
[36] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 1981: 84–88.
[37] Markus Jakobsson, Kazue Sako, Russell Impagliazzo. Designated verifier proofs and their applications. In the proceeding of EUROCRYPT ’96, Springer-Verlag, LNCS 1070, 1996: 143–154.
[38] Zuzana Rja¡¦skov´a, Electronic Voting Schemes, master thesies. Department of Computer Science Faculty of Mathematics, Physics and Informatics Comenius University, Bratislava, April 2002.
[39]G.R. Blakley. Safeguarding cryptographic keys. In the proceedings of AFIPS Conference, 48, 1979: 313-317.
[40] Ran Canetti, Cynthia Dwork, Moni Naor, Rafail Ostrovsky. Deniable encryption. In the proceeding of CRYPTO ’97, Springer-Verlag, LNCS 1294, 1997:90–104.