Asian Journal of Information Technology 15 (15): 2716-2720, 2016
ISSN: 1682-3915

A Study on How to Make a Secure e-Voting Protocol for Elections

Saeed Beheshtifard
Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran

Abstract: We can witness elections and voting in today's life. According to a large increase of activities on internet, the elections and voting behavior would be on internet called with electronic voting. The cost problem that occurs in traditional election can be solved by electronic voting. Some problems like completeness, uncoercibility, non-cheating problems have still existed in electronic voting. In the present research, a proposed electronic voting would be presented to solve the mentioned problems and also the properties of electronic voting would be discussed. In addition, this research examines how to solve the mentioned problems.

Key words: E-voting protocol, election, information security, electronic voting, activities

INTRODUCTION

However, voting is the main element at democratic society, there are many problems in traditional voting such as voting by paper or signature voting. In many countries, voting during elections costs social resources and the social cost is too much. According to this, it can clearly witness that it should bring about change in traditional voting method.

However, electronic voting schemes have been in development for about 20 years (Coleman, 2002), they can solve many drawbacks of traditional voting but some problems still cannot be eradicated such as the completeness problem (Juang and Lei, 1996), the uncoercibility problem (Juang and Lei, 1996; Riera and Borrell, 1998) and the non-cheating problem (Lin, 1997). Nowadays, information technology has made great progress under the efforts of the previous studies in related areas, caused to overcome the mentioned problems. Therefore, the present research aims to present a new electronic voting scheme to resolve these problems and more properties. Table 1 displays a complete view of the electronic voting properties. In the present research, a complete view of the electronic voting properties has been displayed. In this study, the previous works, related theories and techniques and new electronic voting scheme as well as security analysis have been displayed.

The complete view of electronic voting properties: The main purpose of the electronic voting scheme is to enable voting over the internet and achieve the minimum limits at the same time.

Main problems of electronic voting

Completeness problem: The definition of completeness (in some research this is called "'collision-free") mentioned earlier is "an eligible voter is always accepted by the administrator". In earlier research, some systems (Boyd, 1988; Chaum, 1988; Nurmi *et al*., 1991) did not achieve completeness. Boyd (1988) surveyed the problem of fake ballots and pointed out two situations that cause fake ballots. One is that of eligible voters voting twice; the other is when illegitimate voters forge ballots. A forger may try to generate the authority's private key or duplicate ballots in order to disturb an election. His scheme cannot achieve completeness because as the random numbers were generated in a distributed environment, voters may collide with each other.

Some electronic voting schemes (Coleman, 2002; Demillo *et al*., 1982; DTLR News Release, 2002; Fujioka *et al*., 1992; Nurmi *et al*., 1991; Pfleeger, 1989) were not suitable for large-scale elections. Because these schemes used global computation, it would involve huge data and high communication costs. Furthermore, elections would be disrupted when somebody's vote failed in these schemes. Voters pick up their aliases by ANDOS by Nurmi *et al*. (1991). The aliases are unique, thus enabling the authority to identify voters by their aliases but the authority cannot know the voters' real identity. Voters got hashed numbers and used the hash function to compute their aliases and intention in the voting phase and voters sent these hashed numbers and aliases to the authority. Although, Nurmi *et al*. (1991) assumed that the hash function was collision-free, this scheme can still stop an election by someone's failure to vote. Our scheme extends Juang and Lei (1996)'s method in order to achieve completeness in an electronic voting scheme of which there will be more discussion in the section on "theory to achieve completeness".

Uncoercibility problem: Most electronic voting schemes achieved verifiability; their voters got voting receipts from

Table 1: A general view of electronic voting properties

Property	Definition
Completeness	An eligible voter is always accepted by the administrator
Uncoercibility	A voter could not prove to a coercer how he has voted. As a result, verifiable votebuying is impossible
	Only a voter can decide his intention
Non-cheating	Voters can accuse the authority of cheating without revealing ballots to others
	To prevent the authority from being denounced by malicious voters
Robustness	Dishonest voters, other participants or outsiders cannot disturb or disrupt an election
	No one (including authorities) can interfere with a voter's intention through the voter's private data that were stolen
	The processes of receiving ballots and voting for every voter are independent so that, malicious voters cannot disturb the election by stopping the voting process
Uniqueness	Every voter votes exactly 1 time
Verifiability	Voters can check if their ballots have been correctly counted
Fairness	No one can get extra information about the tally result before the publication phase
Anonymous	Neither voting authorities nor anyone else can link any ballot to the voter who has cast it
Convenience	Voters to cast their ballots quickly in one session and with minimal equipment or special skills
Efficiency	The whole election should be held in a timely manner for instance, all computations done in a reasonable amount of time and voters are not required to wait for other voters to complete the process
Mobility	Voters are not restricted by physical location from which they can cast their votes
General election	The intentions of voters are not just in "yes" or "no", voters can choose someone from among several candidates

the authority in the voting phase. When a voter's ballot was not counted correctly, his voting receipt could challenge the tally result. The voting receipts in most cases can achieve verifiability. In earlier research, only a few schemes tended to solve the coercion problem. Some schemes achieved verifiability and receipt-free in some electronic voting research (Benaloh and Tuinstra, 1994; Jorba *et al*., 2003; Juang and Lei, 1997; Riera *et al*., 1998), these schemes did not use voting receipts before announcing the tally result. Receipt-free had been achieved certainly but it collided with mobility because these schemes all had cumbersome physical requirements.

Jorba *et al*. (2003) proposed a trustworthy electronic voting scheme and the scheme satisfied with many secure properties like completeness, non-cheating, verifiability, mobility and general election. It did not satisfy with the property of uncoercibility because this scheme did not mention how to avoid this disadvantage.

Non-cheating problem: Most of the earlier electronic voting schemes were designed with a single authority. The flaw of a single authority scheme is very potent; it can forge a tally result that no one can discover. This is a critical problem for the electronic voting scheme. These schemes set up a lot of scrutinizers or scrutiny systems. Some of them suggest that the scrutiny systems have to be composed by people with different political convictions in order to satisfy the assumption that the authorities and voters cannot collude and to achieve anonymity. Most schemes only solved the verifiability problem to allow voters to ensure their votes being correctly counted. When voters accuse the authorities of cheating, no one can establish whether the blame is with the authority or the voter. Moreover, when authorities and some voters collude to forge votes, other voters cannot provide critical evidence to prove it.

Hwang (1996) presented two electronic voting schemes. In the first scheme, voters got their identification numbers by passing on each other using the tree hierarchy. In the second scheme, it needs two opposing authorities; the certification authority and the voting center. If they colluded with each other, the voting content will be known.

Therefore, it could not satisfy anonymity. Jan and Tai (1997) presented an electronic voting scheme. The voting center must give every voter an IC card with the identification number and the authority's signature embedded in the IC card. Voters cannot vote without this IC card. Because the voting center knew all the private information about the voters, it could easily know the voters' choices which meant that it could not satisfy the property of anonymity. According to the problems mentioned above in this study, we propose an untraceable decryptor to solve the non-cheating problem.

Theory to achieve completeness: In a distributed environment, if the contents of the signed messages are the same, these signed messages will be verified as one. Since these persons do not want to disclose their messages and cannot prove the link between their identification and the signatures, the blind messages may collide with each other, then the eligible persons will be rejected by the administrator.

The technique of partial uncoercibility: Riera *et al*. (1998) presented an uncoercible and verifiable electronic voting scheme. Their scheme used a special smart card (called tamper-resistant smart card), it is an IC card with memory and it can keep secret part of the information even though voters are unable to get it. The scheme imposed this characteristic and voters could take voting receipts from smart cards after the authority published the

tally result and then voters could only check their votes when they received the just third party's private key. The purpose of this method is to delay the time that voters receive their voting receipts and to greatly decline the effectiveness of the voting receipts even if coercers or vote-buyers took them. Riera *et al.* (1998) called this method "hidden-receipt approach". Their electronic voting scheme achieved partial uncoercibility and kept the electronic voting scheme in mobility at the same time.

MATERIALS AND METHODS

The technique of the untraceable decryptor: In this study, we present an electronic voting scheme which involves an untraceable decryptor and a simple electronic voting protocol. An untraceable decryptor is a device which can feasibly be implemented. The random input selector with memory can store input data in a buffer and output data are randomly selected from the buffer, hence the input data sequence is not linked to the output data sequence. The output enable condition can control what conditions start the output of data. For instance, it can be designed to output data when receiving n records or it can be designed to output data at a specific time. Besides, after setting the output enable condition, it can no longer be modified.

The buffer can be produced using storage media with volatility (like RAM). After the output of all data, the buffer can be cleared out when the power is turned off. When receiving an enable signal, the public key decryptor will select a pair of parameters for itself automatically and the private key cannot be modified because it is stored in the PROM. When encrypted data are inputted, the public key decryptor begins to decrypt them with its internal private key. Finally, the messages will mask partial messages (assume m bits) first and then sign and output them as a result.

RESULTS AND DISCUSSION

Security analysis

Completeness: If every voter generates his identification by himself at his place, different voters may generate the same identification, resulting in legitimate voters being rejected from voting. This situation cannot occur in our scheme because ID is a unique identification number, f is a one-way permutation function and R is a random string selected by the voter, hence the output of foID; RÞ is unique, if the input was unique and the function was bijective. The situation in which eligible voters have been rejected because of votes having the same content can never occur in our scheme.

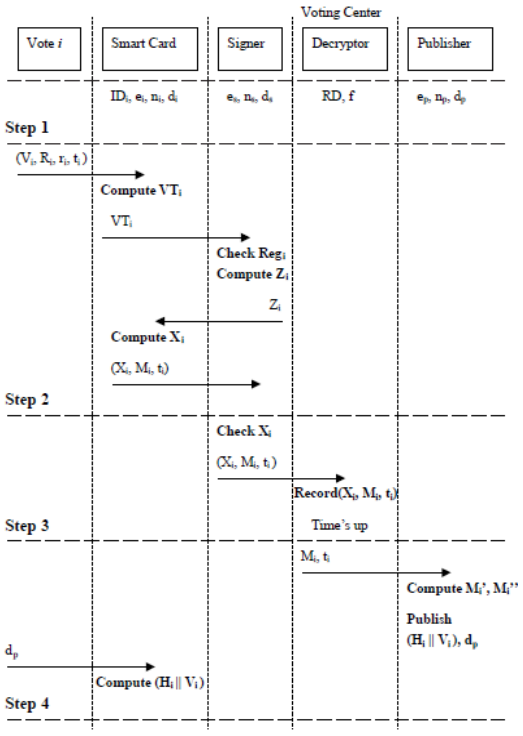

Fig. 1: Diagram of the process of our electronic voting scheme

Second, if the voting center used the global computation in order to allow voters to get a unique identification, legitimate voters are always accepted by the administrator. This certainly achieves completeness but it may not satisfy robustness and leaves the global computation with its huge data and high communication cost. Therefore, it is not suitable for a large-scale election. This situation cannot occur in our scheme because ID is a unique identification number and saved in a smart card in advance. Moreover, the global computation is needless and the huge data and high communication cost would never occur in our scheme (Fig. 1).

The same identification, resulting in legitimate voters being rejected from voting. This situation cannot occur in our scheme, because ID is a unique identification number, f is a one-way permutation function and R is a random string selected by the voter, hence the output of f(ID, R) is unique, if the input was unique and the function was bijective. The situation in which eligible voters have been rejected because of votes having the same content can never occur in our scheme. Second, if the voting center used the global computation in order to allow voters to get a unique identification, legitimate voters are always accepted by the administrator. This certainly achieves completeness but it may not satisfy robustness and

leaves the global computation with its huge data and high communication cost. Therefore, it is not suitable for a large-scale election. This situation cannot occur in our scheme because ID is a unique identification number and saved in a smart card in advance. Moreover, the global computation is needless and the huge data and high communication cost would never occur in our scheme.

CONCLUSION

In this study, we propose a secure and complete voting mechanism which is an electronic voting system suitable for the real world. It not only keeps the high efficiency of previous systems but also strengthens various security properties. Only our scheme can achieve all the properties (achieving partial uncoercibility) in the table. Our scheme achieves completeness, uncoercibility and non-cheating simultaneously as mentioned in the research purpose and no earlier research has been able to overcome this difficult target. Our research has obtained many advantages as follows:

- Our scheme achieves 11 properties, not counting its achievement of partial uncoercibility
- Only a small proportion of earlier research summarized the complete view of electronic voting properties. Our scheme approximately finished the electronic voting properties
- No earlier research tried to overcome the factors of completeness, uncoercibility and non-cheating at the same time. Our scheme achieves this difficult target except for uncoercibility which is achieved partially
- Our scheme is designed by considering the whole election, not only a few specific problems

It is both comprehensive and practical. Our research still has some flaws that future research can try to overcome.

Although, the physical assumptions are possible, there can still be a hardware restriction. In this study, we propose a secure and complete voting mechanism, which is an electronic voting system suitable for the real world. It not only keeps the high efficiency of previous systems but also strengthens various security properties.

Only our scheme can achieve all the properties (achieving partial uncoercibility) in the table. Our scheme achieves completeness, uncoercibility and non-cheating simultaneously as mentioned in the research purpose and no earlier research has been able to overcome this difficult target. Our research has obtained many advantages as follows:

- Our scheme achieves 11 properties, not counting its achievement of partial uncoercibility
- Only a small proportion of earlier research summarized the complete view of electronic voting properties. Our scheme approximately finished the electronic voting properties
- No earlier research tried to overcome the factors of completeness, uncoercibility and non-cheating at the same time. Our scheme achieves this difficult target except for uncoercibility which is achieved partially
- Our scheme is designed by considering the whole election, not only a few specific problems

It is both comprehensive and practical. Our research still has some flaws that future research can try to overcome.

Although, the physical assumptions are possible, there can still be a hardware restriction which mean it cannot replace traditional voting, we hope that our entire and practical research and follow up research can realize electronic voting for the real world as soon as possible.

REFERENCES

Benaloh, J. and D. Tuinstra, 1994. Receipt-free secret-ballot elections. Proceedings of the 26th Annual ACM Symposium on Theory of Computing, May 23-25, 1994, ACM, New York, USA., pp: 544-553.

Boyd, C., 1988. Some applications of multiple key ciphers. Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, May 25-27, Springer, Berlin, Germany, ISBN:978-3-540-50251-7, pp: 455-467.

Chaum, D., 1983. Blind Signatures for Untraceable Payments, Advances in Cryptology-Crypto '82. Springer-Verlag, Santa Barbara, CA, USA., pp: 199-203.

Chaum, D., 1987. Blinding for unanticipated signatures. Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, April 13-15,1987, Springer, Berlin, Germany, ISBN:978-3-540-19102-5, pp: 227-233.

Chaum, D., 1988. Elections With Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA. In: Advances in Cryptologyd Eurocrypt 88, C.G., Guenther (Ed.). Springer, Verlag, Berlin, Germany, pp: 177-182.

Chaum, D.L., 1981. Untraceable electronic mail, return addresses and digital pseudonyms. Commun. ACM, 24: 84-88.

Cramer, R., R. Gennaro and B. Schoenmakers, 1997. A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Trustworthy Global Computing, Fumy, W. (Ed.). Springer-Verlag, Berlin Heidelberg, pp: 103-118.

Cranor, L.F. and R.K. Cytron, 1997. Sensus: A security-conscious electronic polling system for the internet. Proceedings of the Thirtieth Hawaii International Conference on System Sciences, January 7-10, 1997, IEEE, Los Alamitos, California, ISBN:0-8186-7743-0, pp: 561-570.

DeMillo, R.A., N.A. Lynch and M.J. Merritt, 1982. Cryptographic protocols. Proceedings of the 14th Annual ACM Symposium on theory of Computing, May 5-7, 1982, San Francisco, California, United States, pp: 383-400.

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, 1992, Queensland, Australia, pp: 244-251.

Jan, J.K., C.C. Tai, 1997. A secure electronic voting protocol with IC cards. J. Syst. Software, 39: 93-101.

Jang, H.J., 1996. A conventional approach to secret balloting in computer networks. Comput. Secur., 15: 249-262.

Juang, W. and C. Lei, 1997. A secure and practical electronic voting scheme for real world environment. IEICE Trans. Fundam., E80-A: 64-71.

Juang, W.S. C.L. Lei and H.T. Liaw, 2001. Fair blind threshold signatures based on discrete logarithm. Comput. Syst. Sci. Eng., 16: 371-379.

Juang, W.S. and C.L. Lei, 1996. A collision-free secret ballot protocol for computerized general elections. Comput. Secur., 15: 339-348.

Juang, W.S., C.L. Lei and H.T. Liaw, 2002. A verifiable multi-authority secret election allowing abstention from voting. Comput. J., 45: 672-682.

Karro, J. and J. Wang, 1999. Towards a practical secure and very large scale online election. Proceedings of the 15th Annual Conference on Computer Security Applications (ACSAC'99), December 6-10, 1999, IEEE, Phoenix, Arizona, ISBN:0-7695-0346-2, pp: 161-169.

Neff, C.A., 2001. A verifiable secret shuffle and its application to e-voting. Proceedings of the 8th ACM Conference on Computer and Communications Security, November 5-8, 2001, Philadelphia, PA., USA., pp: 116-125.

Niemi, V. and A. Renvall, 1994. Cryptographic Protocols and Voting. In: Results and Trends in Theoretical Computer Science, Juliani, K.,H. Maurer and G. Rozenberg (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-58131-4, pp: 307-316.

Nurmi, H., A. Salomaa and L. Santean, 1991. Secret ballot elections in computer networks. Comput. Secur., 10: 553-560.

Pfleeger, C.F. and S.L. Pfleeger, 1989. Security in Computing. Prentice-Hall, New Jersey.

Riera, A., J. Borrell and J. Rifa, 1998. An uncoercible verifiable electronic voting protocol. Proceedings of the SEC'98 International Conference on Information Security, August 31-September 2, 1998, Osterreichische Computer Gesellschaft (OCG)-Austrian Computer Society, Austria, ISBN:3-85403-116-5, pp: 206-215.