Electronic Voting Protocols Based on Blind Signatures

Orhan Çetinkaya[1] and Ali Doğanaksoy[2]

[1] Institute of Applied Mathematics, METU 06531 Ankara, Turkey
e113754@metu.edu.tr
[2] Department of Mathematics, METU 06531 Ankara, Turkey
aldoks@metu.edu.tr

Abstract. In this paper, we review the electronic voting protocols based on blind signature scheme. These protocols try to fulfil the following electronic voting requirements: eligibility, privacy, receipt-freeness, fairness, accuracy, individual verifiability and universal verifiability. Some of them like eligibility and privacy are easily achieved by the nature of blind signatures; on the other hand, some others like universal verifiability and accuracy are not achieved without some assumptions and conditions. Thus, the certain number of voter involvements into the voting process is definitely required; otherwise the malicious authority can add extra votes or impersonate abstained voters.

1 Introduction

Voting is regarded as one of the most effective methods for individuals to express their opinions on a given topic. Electronic voting (e-voting) refers to the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots and record votes [9].

With the advent of Internet technology, electronic voting will become universally accepted in the upcoming years. Although current implementations for Internet elections are rife with security problems, research community promises to address such problems. Furthermore, the use of cryptographic protocols seems to be a technical response to the loss of all traditional means that were used so far to establish security in democratic elections.

Electronic voting has been intensively studied for over the last decades. Up to now, many electronic voting protocols have been proposed, and both the security as well as the effectiveness has been improved. However, no complete solution has been found in neither theoretical nor practical domains.

The voting protocols could be categorized by their approaches into three main types: protocols using blind signatures, protocols using mix-nets and protocols using homomorphic encryption. The suitability of each of these types varies with the conditions under which it is to be applied.

In the protocols using blind signatures, the voter firstly obtains a pseudonym - a blindly signed message unknown to anyone except himself. Next, the voter sends his

pseudonym together with his vote anonymously. These protocols require voter's participation in more rounds.

The basic process of any democratic election is almost standard although a wide variety of voting systems and protocols exist. In general, this process consists of the following four tasks [6]: *Registration* - gathering a list of people eligible to vote. *Validation* - checking the credentials of those attempting to vote and only allowing those who are eligible and who have not already voted to proceed. *Collection* - collecting the voted ballots. *Tallying* - counting the votes.

The aim of this work is to point out the state of research on electronic voting protocols based on blind signatures and to assess some of them according to the requirements of e-voting. The rest of the paper is organized as follows: In Section 2, the requirements of e-voting are explained; in Section 3, an overview of e-voting protocols based on blind signature is pointed and some of these protocols are discussed. Finally, the concluding remark is given in Section 4.

2 E-Voting Requirements

There is a wide variety of e-voting requirements definitions [6], [10], [13] with different naming convention such as requirements, properties, characteristics etc. These requirements can be grouped and summarized as following:

Eligibility (Authentication): Only eligible and authorized voters can vote and each voter can vote only once.

Privacy: All votes must be secret. No participant other than a voter should be able to determine the value of the vote cast by that voter, in other words, neither election authorities nor anyone else can link any ballot to the voter who cast it.

Receipt-Freeness (Uncoercibility): No voter should be able to convince any other participant of his vote.

Fairness: Nothing must affect the voting. No participant can gain any knowledge about the (partial) tally before the counting stage.

Accuracy: The dishonest voter cannot disrupt the voting. No one can falsify the result of the voting. Every participant should be convinced that the election tally accurately represents the "sum" of the votes cast. It is not possible for a vote to be altered, it is not possible for a validated vote to be eliminated from the final tally, and it is not possible for an invalid vote to be counted in the final tally.

Individual Verifiability: Each eligible voter can verify that his vote was really counted.

Universal Verifiability: A system is verifiable if anyone can independently verify that all valid votes have been counted correctly. Any participant or passive observer can check that the published final tally is really the sum of the votes.

In addition to these requirements, [6] proposed three extra properties that an electronic voting system should possess. Two of these properties are important for ensuring a high voter turnout, something that is often desired but not always achieved.

Convenience: A system is convenient if it allows voters to cast their votes quickly, in one session, and with minimal equipment or special skills.

Flexibility: A system is flexible if it allows a variety of ballot question formats including open ended questions.

Mobility: A system is mobile if there are no restrictions (other than logistical ones) on the location from which a voter can cast a vote.

3 E-Voting Protocols Based on Blind Signature

3.1 Definition of "Blind Signature":

The concept of blind signatures was introduced by Chaum [3] as a method to digitally authenticate a message without knowing the contents of the message. A distinguishing feature of blind signatures is their unlinkability: the signer cannot derive the correspondence between the signing process and the signature, which is later made public.

Blind signatures are the equivalent of signing carbon paper lined envelopes. Writing a signature on the outside of such envelope leaves a carbon copy of the signature on a slip of paper within the envelope. When the envelope is opened, the slip will show the carbon image of the signature.

The blind signatures, based on RSA, can be restated as following. Blind signatures can be accomplished by the following steps. (e, n) is the public key of the signer and (d, n) is the private key of the signer.

1. The provider generates a random number, r. Calculates $x = r^e m \bmod n$. Sends x to the signer.
2. The signer signs x: $t = x^d \bmod n$. Sends t to the provider.
3. The provider reads t. Since

$$t = x^d \bmod n$$

$$t = (r^e m)^d \bmod n = r^{ed} m^d \bmod n = r\, m^d \bmod n,$$

4. The provider calculates

$$s = t\, r^{-1} \bmod n = m^d \bmod n$$

This is the sign of m.

The signer cannot know the content of m. m is blinded by a blinding factor of r.

3.2 Overview of These Protocols

Blind signature method was originally conceived for e-cash applications and then it was used to solve the problem of validating votes without sacrificing privacy.

Protocols using anonymous channel and blind signatures are very popular in practice due to their efficiency as communication and computation overhead is fairly small even when the number of voters is large and their support for any type of voting. These protocols can easily be managed and realize elections with multiple candidates.

However, the voter has to act in more rounds (registration, voting, counting, verifying, complaining...), in other words, every eligible voter should not abstain after the registration phase, otherwise a corrupted validator can add extra votes on behalf of abstaining voters. In general, these protocols only provide individual verifiability and no universal verifiability.

These protocols work in the following way:

Firstly, each voter obtains a pseudonym from the administration authority. In fact, pseudonym is a message, encrypted by the voter and blindly signed by the authority. The authority checks whether voter is allowed to vote or not, then helps the eligible voter to construct the pseudonym only once, so the voter could obtain at most one pseudonym. The authority has no idea how the voter's pseudonym looks like because of blind signature.

Next, the voter sends the ballot containing the pseudonym and his vote through the anonymous channel to the tabulation authority. The authority will not accept the ballot with invalid token or with the token that has already been used. This ensures that only eligible voters can vote and that they can vote at most once. Anonymous channel is used to keep the privacy and to assure the anonymity of the voter. As no one (even the authority) can make any connection between the voter and the pseudonym or trace the cast ballot back to the voter, no one can deduce anything about how the voter voted. The authority collects the votes and publishes valid votes together with the pseudonyms. Voters can verify that their vote is being published correctly.

The terms administration authority and tabulation authority can refer to the two different authorities, or to the same authority acting both as the administrator and as a tabulator, depending on the protocol.

Several election protocols based on blind signatures have been proposed [1], [4], [10], [12], [14], [15], [19], [20], [21].

Chaum [2] pioneered the notion of e-voting and then several protocols were proposed. However, these earlier protocols suffer from providing most e-voting properties. Later, Chaum [4] proposed a protocol based on the sender untraceable email system, which assumes that at least one mix is trust. It has large communication complexity at the registration phase. Ballot tallying authority can immediately open ballots upon receiving them and therefore leaking intermediate results can effect the voting. Also, voter must reveal his vote to prove that it was not counted correctly which violates privacy concerns. Fairness and privacy are violated.

Boyd's protocol [1], based on multiple key ciphers, is more efficient. There is one administrator carry out elections and issue valid voting slips to every potential voter exactly one. However, the voting authority can easily falsify the ballots. Furthermore, the voting authority can substitute spurious votes of its choice in the final tally. Knowledge of the intermediate results could distort further voting. Thus, it is not fair and not verifiable.

The first practicable protocol ensuring both the privacy and the fairness is of Fujioka et al. [10]. The proposed e-voting protocol is capable of solving the fairness problem by using the bit-commitment function. No one, including the voting authority, can know the intermediate result of the voting. Thus, it prohibits the fraud by either the voter or the authority. The voter has to participate in three rounds and he has to send

two messages through anonymous channel. Reduced number of rounds appears in the protocol of Juang et al. [14], [15].

Juang et al. [14] proposal introduces scrutineers other than administrator. The protocol uses threshold cryptosystem to guarantee the fairness among the candidates campaign. It preserves privacy of the voter against the administrator and scrutineers.

The protocol of Radwin [20] mainly concentrates on tracing double-votes, the protocol is constructed on the idea of double spending [5], most of the requirements are not fulfilled properly.

There are also several implementations that have been piloted in small-scale elections: The SENSUS system [6] was the first to be implemented. The Davenport et al system [7] was used to conduct student governmental elections. The EVOX system [11] was used at MIT for undergraduate association elections. DuRette [8] improved EVOX system in order to eliminate single entities capable of corrupting the election (the EVOX Managed Administrator).

Both DuRette's system and EVOX are very sensible to failures in communication or servers, these problems were solved by REVS which is proposed by Joaquim et al. [17] as another implementation based on DuRette's work. Furthermore, the DuRette's system has problems concerning the authentication of voters, allowing an easy impersonation of voters by the servers running the election. In REVS, this problem was solved as redesigning the voters' authentication algorithm. Later, some improvement was done on REVS to make it more robust [18].

3.3 Some Proposed Protocols

3.3.1 Fujioka et al. Voting Protocol

In Fujioka et al. voting protocol [10] is one of the milestone proposals on e-voting area, especially on protocols based on blind signature. In this protocol, there are two authorities: administrator and counter. The administrator handles preparation and voting stages by interacting with voters; the counter collects the votes, counts them and publishes the election result. Voter prepares a pseudonym (encrypted ballot) and sends it to administrator by proving his identity; administrator checks the voters' eligibility and blindly signs the pseudonym and sends it back to him. Then, the voter sends his ballot via an anonymously communication channel to the counter. The counter collects the ballots, counts them, and publishes the list. The voter checks his ballot in the list, and sends his key together with the ballot number to the counter via anonymously channel. The counter decrypts the votes with the keys and announces the result of the election.

This protocol satisfies some of the e-voting requirements but not all.

Eligibility: Administrator just allows eligible voters to vote and a voter cannot use the pseudonym more than once. Hence, eligibility is achieved.

Privacy: Since the relation between the voter's identity and his ballot is hidden by the blind signature scheme, the voter's privacy is preserved even if the administrator and the counter conspire. The voter sends his ballot as well as the key through anonymous channel, so no one can trace it back. Thus the privacy is preserved.

Receipt-Freeness: Anyone who gets to know the voter's pseudonym can easily find out his vote in the list published by the counter at the end of the election. Therefore, the receipt-freeness is not achieved.

In order to achieve receipt-freeness, Okamoto [19] proposed another voting protocol, which is in fact a modification of the Fujioka et al. protocol, guaranteeing receipt-freeness strongly relying on voting booth. One more authority is introduced as a collector in addition to the administrator and the counter.

Fairness: Counting of the ballots does not affect the voting, as the counting stage comes after the voting phase. So, fairness is achieved in this protocol.

Accuracy: During opening phase, voter can send illegal key or key can be changed in somehow. According to the bit-commitment algorithms, changing key will not help getting a meaningful another vote, but will make the vote something meaningless. The change of key will not invalidate the sign, and cannot be verified or validated at any stage. This change of key can even be done via some active attacker. Furthermore, at this point, a dishonest voter cannot be distinguished from a dishonest counter. To prevent this, voter could send this key to several parties, assuming parties of the election do not collaborate. Hence, accuracy depends on authorities.

Individual Verifiability: Counter publishes the election result as a list. The voter can check whether his ballot is on the list or not and whether his key and vote pair has been added to the list or not. Thus, the protocol is individually verifiable.

If any voter proves that there is a fraud while verifying, then the disputed votes are omitted. If the number of omitted votes affects the result of the election, the voting process should be invalidated and election should be restarted. Since the claiming voter is allowed to register for the second time to obtain the new pseudonyms, at the counting stage, everybody can know which votes were sent by the claiming voters.

Universal Verifiability: The voter has to participate in three rounds: registration, voting and opening. After the registration phase, no voter abstains from the voting. This is impractical. The protocol is not universally verifiable.

If some voters abstain from voting after the registration phase, the administrator and the counter can conspire and they can add false vote to the list. To avoid this failure, instead of using just a single administrator and a single counter, more administrators and the more counters can be used.

3.3.2 Radwin Voting Protocol

Radwin's voting protocol [20] mainly focuses on preventing double voting. In this protocol, voter should participate in two phases. In the first phase, the voter should register with the voting authority so that he can obtain a digitally signed pseudonym which is constructed from his special identification number to trace his vote back to him in case of attempting to vote second time. In the second phase, he submits his ballot to the voting authority by using the pseudonym. The pseudonym does not contain the actual vote.

This protocol satisfies some of the e-voting requirements but not all.

Eligibility: Firstly, the voter identifies himself as an eligible voter to the authority and then the voter and the authority interactively determine a numerical pseudonym. The voter needs the authority's signature to construct pseudonym. The authority gives

only one pseudonym to the voter. Thus, the eligibility is achieved depending on the authority's honesty.

Privacy: As the relation between the voter's identity and his pseudonym is hidden by the blind signature scheme, the voter's privacy is preserved while he does not try to use his pseudonym more than once. The voter sends his ballot as well as the pseudonym through anonymous channel, so no one can trace it back. Thus the privacy is preserved.

Receipt-Freeness: If the authority publishes other details in addition to the ballots and pseudonyms in the list, the voter can easily prove that how he voted by showing the details which is used to interact with the authority. Hence, the protocol is not receipt-free.

Instead of publishing the whole list, if the authority publishes just a final sum of the votes, the protocol is now receipt-free, the voter has no way to acquire the relation between the votes and pseudonyms. Individual and universal verifiability are not preserved anymore.

Fairness: Since the publishing the result of election comes after the voting phase, counting of the ballots does not affect the voting. However, nothing is clearly mentioned about the counting in the proposal. Hence, it is not so easy to say that the protocol is fair.

Accuracy: If the voter tries to use his pseudonym twice, his identity is revealed with high probability. However, the accuracy completely depends on the authority.

Individual Verifiability: If the authority publishes just a final sum of the votes, only the authority can see the pseudonyms. Hence, the voter cannot verify whether his vote is really counted by the authority or not. In this situation, individual verifiability is not provided. If the authority publishes a list which is containing received ballots and pseudonyms, the protocol is individually verifiable. The voter can verify whether his pseudonym and his vote are on the list. However, when the voter complains that his vote is not counted, he should show some internal details used while interacting with the authority. In this case, the voter's privacy is violated; at least the authority can know the voter's vote.

Universal Verifiability: If the authority publishes other details in addition to the ballots and pseudonyms in the list, the protocol can be universally verifiable. However, in this case, the property of receipt-freeness is no longer preserved. In addition, as the authority can impersonate the abstaining voters and add its own votes, or provide some voters with more pseudonyms. Thus, universal verifiability is not achieved.

3.3.3 Juang et al. Voting Protocol

In [14] protocol mainly focuses on practical voting protocol applicable for real world environment. It involves one administrator and several scrutineers. The voter communicates three times with the administrator. The protocol consists of six phases: initialization, global key generation, registration, voting, announcement and publication. The role of the scrutineers is to generate the threshold verifiable public key that is used in encrypting the votes and distribute shares to each other without a trusted third party. Encrypted vote is a part of the pseudonym. Like all other single administrator voting protocols, the voter cannot abstain from the voting process after the registration phase. Otherwise, malicious administrator can add extra votes instead of abstained voters.

However, the protocol is revised to distribute the power of a single administrator to several administrators in [15] and [16].

This protocol satisfies some of the e-voting requirements but not all.

Eligibility: Only eligible voters can obtain pseudonyms and just one for each voter is given by the administrator. If any voter attempts to use his pseudonym more than once, the administrator just counts one of those votes; the rest is discarded in the final tally. Thus, the eligibility is achieved.

Privacy: Since the relation between the voter's identity and his ballot is hidden by the blind signature scheme, the voter's privacy is preserved. Extracting identity of voter from the ballot is also computationally infeasible because of RSA. The voter sends his ballot through anonymous channel, so the sent ballot cannot be traced back to the voter. Therefore the privacy is preserved.

Receipt-Freeness: Since the voter's receipt is his pseudonym, anyone gets to know the voter's pseudonym can easily find out his vote in the list published by the administrator at the announcement phase. Thus, protocol is not receipt-free.

Fairness: As every voter's ballot is published in the announcement phase that comes after the voting phase and any vote cannot be added after beginning of the publication phase, counting of the ballots does not affect the voting. Therefore, the protocol is fair.

Accuracy: Since the uniquely (collision free) blind signature is used, the signed pseudonyms requested by the honest voters are distinct. A dishonest person may construct a pseudonym, but he could not impersonate the voter. Any validated vote cannot be eliminated from the final tally. However, whether the published tally is accurately represents the actual result of election is questionable. The encrypted ballots opened correctly in the publication phase depend on whether certain number of scrutineers out of all is honest or not. If any voter abstains voting after registration phase, the administrator can add extra votes. There is a strong assumption that no voter will abstain from. Moreover, if the administrator is not honest, there is a possibility that any voter can disrupt the election when the voter makes an open objection in the publication phase. Therefore, the accuracy depends on administrator and scrutineers.

Individual Verifiability: Administrator publishes the election result. The voter can check whether his ballot is published or not. Thus, the protocol is individually verifiable.

Universal Verifiability: The protocol is based one the assumption: After the registration phase, no voter can abstain from the voting process. This assumption is impractical. If some voters abstain from voting, malicious administrator can add extra votes. Thus, the protocol is not universally verifiable. To overcome the abstention problem, Juang et al. proposed some other protocols with multi authorities [15], [16].

4 Conclusion

Despite extensive work on the e-voting protocols, no complete solution has been found in either theoretical or practical domains. A number of voting protocols have been proposed with widely differing security properties.

Electronic voting protocols based on blind signature solve some of the issues but not all of them. In general, eligibility and privacy are achieved because of blind signature scheme; and fairness is achieved if counting stage comes after the voting stage. However, in some cases privacy is violated, at least the administrator can gain knowledge about the voter's cast, when the voter complains the election result after individually verifying his vote in the final tally. In this case, individually verifiability is not preserved anymore. Accuracy is fulfilled conditionally depending on the authority. If there is single authority, accuracy can be violated easily since the voters abstain from the voting process after the registration stage. If there is more than one authority, achievement of accuracy depends on the protocol and relation between the authorities that they can conspire. In general, as the malicious authority can impersonate the abstaining voters and add its own votes, or provide some voters with more pseudonyms, universal verifiability is not achieved. If the abstaining from voting is solved in somehow (distributing the authority), the universal verifiability is fulfilled but in this case receipt-freeness is sacrificed.

5 References

1. Boyd, C.: A new multiple key cipher and an improved voting scheme. Advances in Cryptology - EUROCRYPT '89, pp. 617-625. Springer-Verlag (1989)
2. Chaum, D. L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of ACM, Vol. 24, pp. 84-88 (1981)
3. Chaum, D. L.: Blind Signatures for Untraceable Payments. CRYPTO '82, pp. 199-203 (1982)
4. Chaum, D. L.: Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. EUROCRYPT'88 (1988)
5. Chaum, D. L.: Achieving Electronic Privacy. Scientific American, pp. 96-101, (August 1992)
6. Cranor, L. and Cytron, R.: Sensus: A Security-Conscious Electronic Polling System for the Internet. Hawaii International Conference on System Sciences, Wailea, Hawaii (1997)
7. Davenport, B., Newberger, A. and Woodard, J.: Creating a Secure Digital Voting Protocol for Campus Elections. Princeton University (1996)
8. DuRette B. W.: Multiple Administrators for Electronic Voting. Bs. Thesis, MIT (May 1999)
9. "Electronic Voting". Encyclopedia of Computers and Computer History (2001).
10. Fujioka, A., Okamoto, T. and Ohta, K.: A practical secret voting scheme for large scale elections", Advaced in Cryptology - AUSCRYPT'92, 1992.
11. Herschberg, M.: Secure Electronic Voting Using the World Wide Web. Ms Thesis, MIT (June 1997)
12. Horster, P., Michels, M. and Petersen, H.: Blind Multisignature Schemes and their Relevance to Electronic Voting. 11th Annual Computer Security Applications Conference, IEEE Press, pp. 149-155 (1995)
13. "Report of the National Workshop on Internet Voting: Issues and Research Agenda", Internet Policy Institute (March 2001)
14. Juang, W. S. and Lei, C. L.: A secure and practical electronic voting scheme for real world environment. IEICE Trans. On Fundamentals, E80-A(1) (January 1997)
15. Juang, W. S., Lei, C. L. and Yu, P. L.: A verifiable multi-authorities secret election allowing abstaining from voting. International Computer Symposium, Tainan, Taiwan (1998)

16. Juang, W. S., Lei, C. L. and Liaw, H. T.: A Verifiable Multi-Authority Secret Election Allowing Abstention from Voting. Computer Journal, 45(6), pp. 672-682 (2002)
17. Joaquim, R., Zuquete, A. and Ferreira, P.: REVS - A Robust Electronic Voting System. Proceedings of IADIS International Conference e-Society 2003, Lisbon, Portugal, pp. 95-103 (2003)
18. Lebre, R., Joaquim, R., Zuquete, A. and Ferreira, P.: Internet Voting: Improving Resistance to Malicious Servers in REVS. IADIS International Conference on Applied Computing 2004, Lisbon, Portugal (March 2004)
19. Okamoto, T.: Receipt-Free Electronic Voting Schemes for Large Scale Elections. 5th Security Protocols Workshop '97, LNCS 1163, Springer-Verlag, pp. 125-132 (1997)
20. Radwin, M. J.: An untraceable, universally verifiable voting scheme. Seminar in Cryptology (1995)
21. Sako, K.: Electronic Voting Schemes Allowing Open Objection to the Tally. Trans. of IEICE, E77-A(1), pp. 24-30, 10 (1994)