Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract)

Orhan Cetinkaya
Institute of Applied Mathematics,
METU, Ankara, Turkey
e113754@metu.edu.tr

Abstract

Electronic voting refers to the use of computers or computerized voting equipment to cast ballots in an election and it is not an easy task due to the need of achieving electronic voting security requirements. The cryptographic voting protocols use advanced cryptography to make electronic voting secure and applicable.

In this paper, formal definitions of security requirements for cryptographic voting protocols (privacy, eligibility, uniqueness, fairness, uncoercibility, receipt-freeness, accuracy, and individual verifiability) are provided, and elaborate checklists for each requirement are presented. The voting problem is clearly defined in terms of security requirements. The voting problem arises from the trade-off between receipt-freeness and individual verifiability. This paper suggests the Predefined Fake Vote (PreFote) scheme as an applicable solution to overcome the voting problem. The PreFote scheme is not a voting protocol; however, it is a building block that can be used by any voting protocol.

1. Introduction

Due to the rapid growth of computer technologies and advances in cryptographic techniques, electronic voting is now an applicable alternative to paper based voting. The majority of people may accept and use electronic voting, but people have some concerns about the privacy, security and accuracy of the election. They cannot easily trust the voting system unless security of the system is achieved.

A secure and complete voting protocol should meet some security requirements. Requirement analysis is an important part of the system design process and it is impossible to develop the right system in the right way without a correct and complete set of requirements. In this manner all cryptographic voting studies mention voting requirements in some way, and different sets of requirements are defined. Almost all proposed voting protocols and implementations focus on a subset of the requirements [13]. In addition there is no obvious consensus about the definitions.

There are some studies on requirement analysis of electronic voting protocols. McGaley and Gibson [10] define basic requirements for any voting system and they examine the e-voting system bought by the Irish Government to see whether it can meet those requirements. Schryen [14] presents a structural security framework for e-voting systems. Heindl [9] deals with the legal requirements for e-voting in Austria. Mitrou *et al.* [11] addresses the democracy-oriented legal and constitutional requirements for any e-voting system. Cetinkaya [4] provides a comprehensive set of voting requirements. All of these studies give informal definitions, whereas more detailed and formal definitions are strongly needed. A recent work of Delaune *et al.* [6] formalizes some of the requirements in applied pi calculus and shows the strong relationship between privacy, receipt-freeness and uncoercibility. However, their study does not provide a complete guidance.

In this paper, the formal definitions of cryptographic voting security requirements are proposed by using a widespread review [4] of secure election system characteristics in the literature. These are privacy, eligibility, uniqueness, fairness, uncoercibility, receipt-freeness, accuracy and individual verifiability. Also, checklists of special cases for each requirement are defined in detail.

This paper clearly defines the voting problem in terms of security requirements. The voting problem arises from the combination of receipt-freeness and individual verifiability requirements since they conflict with each other obviously. If a voting system provides any receipt which enables the voter to verify his vote in the final tally, then that receipt can also be used for vote buying or selling.

In voting systems, there is a noticeable contradiction between verifiability and secrecy. On the one hand, the voter wants to verify that the entire voting process has taken place appropriately. In particular, he wants to be assured that his individual vote was counted correctly. However, if the voter obtains adequate information from the voting process, then he can convince a vote buyer of how he voted, which in turn increases the likelihood that vote selling becomes a threat. In some way, we want the voter to obtain enough information to be personally convinced that his vote was indeed recorded as he cast, but not to unduly reveal information by which he could convince someone else.

Finally, this paper suggests an applicable solution in order to overcome the voting problem by introducing Predefined Fake Vote (PreFote) scheme which provides direct individual verifiability without sacrificing receipt-freeness and accuracy. The PreFote scheme is not a voting protocol; however, it is an approach that can be directly applied by existing voting protocols.

The remainder of the paper is organized as follows: Section 2 analyzes the security requirements for cryptographic voting protocols by providing formal definitions and elaborate checklists. Section 3 states the voting problem; and a solution to the problem is suggested in Section 4. Finally, conclusions are drawn and future work is suggested.

2. Security Requirements for Cryptographic Voting Protocols

In this section, the security requirements for voting protocols, adapted from [4], are explained. Some of the definitions in the original work are extended, and another naming which is "Security requirements" is used instead of the original naming "Core requirements". A secure and complete cryptographic voting protocol should satisfy the following security requirements:

- *Voter Privacy:* It is the prevention of associating a voter with a vote [5], [12]. Voter privacy must be preserved during the election as well as after the election. In order to assure privacy both unlinkability and untraceability should be satisfied.

- There are two identities which directly identify the voter and are probably known publicly. They are the voter's registration identity and the voter's public key. No one should be able to deduce any relationship between these two identities and the voter's cast vote. This is called as unlinkability.

- Voter may have one more indirect identity, which is the IP address of the computer via which the voter casts his vote. No one should be able to trace the IP address or be able to deduce any relationship between the voter and his vote. This is called untraceability.

- *Eligibility:* Only eligible voters participate in the election [3], [8]. They should register before the election day and only the eligible voters who have registered can cast votes.

- *Uniqueness:* Only one vote per voter should be counted [7]. It is important to notice that uniqueness does not mean unreusability (i.e. voters should not vote more than once).

- *Fairness:* No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision [1]. Even the counting authority should not be able to have any insight into idea about the results.

- *Uncoercibility:* Any coercer, including the authorities, should not be able to extract the value of the vote [3] and should not be able to coerce a voter to cast his vote in a particular way. Any voter must be able to vote freely.

- *Receipt-freeness:* It indicates that the system does not provide a confirmation of the receipt of the vote which may yield its content. In other words, voters should not obtain a receipt, nor can they construct one, which can be used to prove the content of their votes a third party [9] both during the election and after the election ends. This is to prevent vote buying or selling.

- *Accuracy:* The published tally should be correctly computed from correctly cast votes [3]. Accuracy can be analyzed in two ways:

- All valid votes should be counted correctly. Any cast vote cannot be altered, deleted, invalidated or copied [2]. Any falsification on the votes should be detected.

- All counted votes should be valid and correct, i.e. eligibility and uniqueness should be satisfied. No participants, voters or authorities can disrupt or influence the election and final tally by adding false votes (a.k.a. Soundness and Completeness). Nobody should be able to vote in the place of others, even if they are eligible voters but they do not vote for some reasons (a.k.a. Abstaining Voter problem) or they abandon the voting process in any stage.

Remark about universal verifiability: The literature highlights universal verifiability as another common requirement. The definition of universal verifiability is very similar to the definition of accuracy. It can be stated that universal verifiability is the provability that the election is accurate. If a protocol claims that it satisfies accuracy, it should be able to prove its claim. In this perspective, any protocol claiming that they satisfy accuracy should also satisfy universal verifiability. Evidently, universal verifiability is not an e-voting requirement, whereas accuracy is. Thus, in this paper only accuracy is listed as a security requirement.

- *Individual Vote Check* (a.k.a. Individual Verifiability): The voter should be able to check that his encrypted vote was counted and tabulated correctly in the final tally [7]. In traditional paper-based voting systems, people cannot make individual vote check directly. However, the voter puts his vote into the ballot box himself. Since the security of the ballot box is guaranteed, individual vote check is, in a way, assured. Although this requirement is not directly satisfied in paper based voting, it should explicitly be fulfilled in electronic voting protocols due to the nature of computer systems and electronic equipment.

2.1. Elaborate Checklists for Security Requirements

This section provides a guideline for evaluation of the voting systems by explaining the specific cases of the security requirements and offers a systematic approach for analyzing them. For each requirement, checklist items are given below and they should be satisfied by cryptographic voting protocols.

- Privacy:
  - Voter-Vote unlinkability
  - Voter-Vote IP untraceability
  - Voters cannot add identifiable information
  - Authorities cannot add identifiable information
- Eligibility:
  - Eligible voters can vote
  - Ineligible voters cannot vote
  - Authorities cannot give voting credentials to ineligible voters
  - Authorities cannot usurp suffrage
- Uniqueness:
  - At most one valid vote is counted for each eligible voter
  - Each eligible voter has voted only once
- Fairness
  - Result is not published till the end of the election
  - Counting comes after the voting stage
  - No one can guess the content of any cast vote
  - No one can gain any partial knowledge about the tally before the counting stage
  - Encrypted votes are used and they are decrypted at the end of the election
- Uncoercibility
  - Nobody can force the voter to vote in a particular way
  - Nobody can force the voter physically being next to him
  - Coercer cannot receive any proof from the voter after voting
  - Coercer cannot force the voter to use a particular proof provided before voting
  - Coercer cannot vote instead of voter with his personal ID
  - Nobody can coerce voter to abstain from voting
- Receipt-freeness
  - Voter is not identifiable from the receipt
  - Vote is not revealed from the receipt
  - Voter cannot prove his vote
  - Vote selling/buying is prevented
  - Authority gives correct receipt
  - Any public data do not give any information about voter's vote
  - Voter cannot use a particular proof defined before voting
  - Voter cannot prove his vote even if he records his activity
  - Voter cannot obtain a particular proof after voting
  - Voter cannot use a personal ID or private keys to prove his vote
- Accuracy
  - Voter can vote as intended
  - Vote is recorded correctly
  - All valid votes are counted correctly
  - No valid votes are deleted
  - No valid votes are modified
  - No valid votes are spoiled
  - No valid votes are copied
  - No false votes are added
  - Nobody can vote instead of abstained voters
  - Any single authority corruption is detected
  - Any number of authorities' corruption is detected
  - No one, not even a dishonest voter can disrupt the voting
  - Voter can make objection during the voting process if there is an error
  - Authorities respond correctly
  - Ballot representations are correct
  - Voters can complete voting process even if there is a physical error
- Individual Verifiability
  - Voter can validate that his vote is recorded correctly
  - Each eligible voter can verify that his vote is counted correctly by using published data

- Voter can validate that the ballot is correct
- Voter can validate that authorities response correctly
- Voter can safely re-request data during the voting process if authority response time outs

2.2. Formalization of Security Requirements

While electronic voting has been studied for the past two decades, research on analyzing voting systems has begun only recently [13]. In this section, a method to analyze voting systems is proposed. This method helps to evaluate as well as compare the voting protocols and it is not protocol specific. In order to define a voting protocol VP, let:

$E = \{e_1, e_2, e_3 \ldots e_q\}$ be the set of all eligible voters where q is the number of eligible voters;

$A = \{a_1, a_2, a_3 \ldots a_n\}$ be the set of voters that performed a voting process where a_i is any voter and n is the number of voting attempts;

$B = \{b_1, b_2, b_3 \ldots b_n\}$ be the set of votes where b_i is the vote of voter a_i;

$D = \{d_1, d_2, d_3 \ldots d_n\}$ be the set of transactions in voting processes where d_i denotes all transactions of voter a_i during the voting process;

$V = \{v_1, v_2, v_3 \ldots v_m\}$ be the set of all valid votes (including all data) where m is the number of valid votes, $V \subseteq B$ and $m \leq n$;

$W = \{w_1, w_2, w_3 \ldots w_m\}$ be the set of published data at the end of the election, w_i denotes the published data for each valid vote v_i and $w_i \subseteq v_i$;

$C = \{c_1, c_2, c_3 \ldots c_k\}$ be the set of all candidates;

$S = \{s_1, s_2, s_3 \ldots s_h\}$ be the set of all eavesdroppers;

$f_{bv}: B \rightarrow V,\ f_{bv}(b_i) = v_j$ matches each b_i to a v_j if b_i is a valid vote;

$f_{ae}: A \rightarrow E,\ f_{ae}(a_i) = e_j$ matches each a_i to an e_j if a_i is an eligible voter;

$f_{vc}: V \rightarrow C,\ f_{vc}(v_i) = c_j$ matches each valid vote to an actual candidate;

$$T = \{(c_1, \sum_{i=1}^{m} add(f_{vc}(v_i), c_1)) \ldots (c_k, \sum_{i=1}^{m} add(f_{vc}(v_i), c_k))\}$$

be the tally.

Note that if any recasting occurs then it is handled as a new voting process, so it can be that $n \geq q$. If recasting is not allowed then it should be that $n \leq q$. In addition, D is not required to be hidden.

This study proposes the following definitions for cryptographic voting security requirements:

Definition 1 *(Privacy)*:
If $\forall d \in D \forall v \in V \forall e \in E[\neg(\exists f(S, W, d, v) = e)]$ for a voting protocol *VP*, then *VP* satisfies privacy.

Definition 2 *(Eligibility)*:
Let $f{:}V \rightarrow B,\ f(v_i) = b_j$ and $g{:}B \rightarrow A,\ g(b_j) = a_j$. If $\forall v \in V[f_{ae}(g(f(v))) \in E]$ for a voting protocol *VP*, then *VP* satisfies eligibility.

Definition 3 *(Uniqueness)*:
Let $f{:}V \rightarrow B,\ f(v_i) = b_j$ and $g{:}B \rightarrow A,\ g(b_j) = a_j$. If $\forall v_i \in V \forall v_j \in V[f_{ae}(g(f(v_i)) = f_{ae}(g(f(v_j)) \leftrightarrow i = j]$ for a voting protocol *VP*, then *VP* satisfies uniqueness.

Definition 4 *(Fairness)*:
If $\forall b \in B[\neg(\exists c \in C(f(D, S, b) = c))]$ for a voting protocol *VP* during the election, then *VP* satisfies fairness.

Definition 5 *(Uncoercibility)*:
If $\forall s \in S \forall a \in A \forall v \in A[\neg(\exists f(D, W, s, a) = v)]$ for a voting protocol *VP*, then *VP* is uncoercible.

Lemma 6 *(Receipt-freeness)*:
If $\forall a \in A \forall v \in V[\neg(\exists f(D, W, a) = v)]$ for a voting protocol *VP*, then *VP* is receipt-free.

Definition 7 *(Accuracy)*:
Let $h{:}\ E \rightarrow A,\ h(e_i) = a_j;\ g{:}A \rightarrow B,\ g(a_j) = b_j;\ f{:}V \rightarrow B,\ f(v_i) = b_j$ and $g'{:}B \rightarrow A,\ g(b_j) = a_j$. If $\forall e \in E[f_{bv}(g(h(e))) \in V] \wedge \forall v \in V[f_{ae}(g'(f(v))) \in E]$ for a voting protocol *VP*, then *VP* satisfies accuracy.

Definition 8 *(Individual Verifiability)*:
If $\forall e \in E \forall w \in W \exists! v \in V[\exists f(e, w) = v)]$ for a voting protocol *VP*, then *VP* satisfies individual verifiability.

Theorem 1: A voting protocol *VP* is a complete and secure protocol if and only if it satisfies *Definition 1-8.*

3. The Voting Problem

Security requirements are explained in the previous sections. Designing secure voting systems is extremely difficult since the requirements are apparently contradictory. According to the definitions of receipt-freeness and uncoercibility, we can conclude that a voter could neither obtain nor is able to construct a receipt that proves the content of his vote by coercion or voluntarily. This is to allow voting freely and to prevent vote buying or selling.

According to the definitions of individual verifiability and accuracy, we can conclude that the published tally should be correctly computed from correctly cast votes in a verifiable manner and the voter himself should be able to check that his vote is counted correctly in the final tally.

The voting problem arises from the combination of these requirements. Specifically, the voting problem between receipt-freeness and individual verifiability is described since there is a noticeable trade-off between them. If the voting system provides any receipt which enables the voter to verify his vote in the final tally, then that receipt can also be used for vote buying or selling. Individual verifiability also contradicts privacy and uncoercibility because they have a close relationship with receipt-freeness. For example, checking a receipt is more convenient for a coercer than buying or stealing access keys and casting all the votes himself. If receipt-freeness is not fulfilled then uncoercibility and privacy cannot be assured.

When voting takes place in an electronic environment, the possibility of fraud is unavoidable since ensuring the trust is not an easy task. People cannot easily trust the e-voting system unless they individually verify that their votes are cast, recorded and counted correctly. Individual verifiability is important to raise public trust in electronic voting.

Research studies in the literature generally achieve either individual verifiability or receipt-freeness. Most of them sacrifice receipt-freeness at the cost of accuracy and individual verifiability. A few protocols, which claim that they satisfy receipt-freeness, provide only universal verifiability or even worse no verifiability. In the literature, there is no protocol which satisfies receipt-freeness, uncoercibility and individual verifiability at the same time, even with conditions or assumptions. [13]

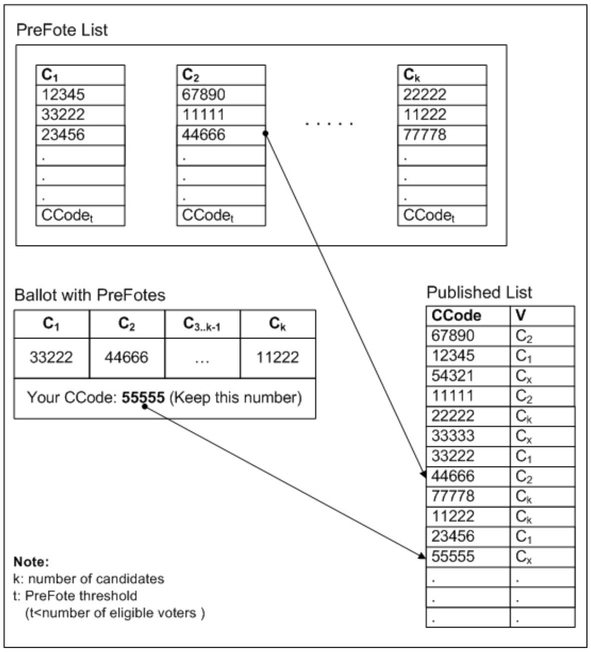
4. Predefined Fake Vote (PreFote) Scheme

In this section, an applicable solution namely Predefined Fake Vote (PreFote) scheme is proposed in order to overcome the voting problem. The PreFote scheme is not a voting protocol; however, it is an approach to solve the voting problem and it can be used as a building block in any voting protocol. The PreFote scheme uses an intentionally prepared predefined fake vote list where each PreFote consists of a unique code and an associated candidate from the candidates list.

The PreFote list is prepared just before the election starts. Authorities participate in the PreFote list generation process. For each candidate, a constant threshold number of PreFotes are generated and listed in PreFote list.

In order to use the PreFote list, firstly the voter should obtain a unique check code (CCode) from the voting system with his empty ballot, which is the real CCode. In addition to real CCode, voter learns a set of fake CCodes, which are in fact PreFotes, linked with candidates on the ballot. PreFotes are chosen randomly from the PreFote list. Thus, the voter obtains a CCode and a set of PreFotes.

At the end of the election the PreFote list and real CCodes with revealed actual votes are published together in a random order. The voter uses his real CCode for individual verifiability and directly checks his vote from the published list. He can use PreFotes in case of coercion. The PreFote list does not affect the result of the tally, since the published list is only used for individual verifiability. Any voting protocol which uses the PreFote list should also announce another election result list without CCodes. Figure 1 depicts the PreFote list structure.



PreFote List

C_1
12345
33222
23456
.
.
.
$CCode_t$

C_2
67890
11111
44666
.
.
.
$CCode_t$

C_k
22222
11222
77778
.
.
.
$CCode_t$

Ballot with PreFotes

C_1	C_2	$C_{3..k-1}$	C_k
33222	44666	…	11222
Your CCode: **55555** (Keep this number)			

Published List

CCode	V
67890	C_2
12345	C_1
54321	C_x
11111	C_2
22222	C_k
33333	C_x
33222	C_1
44666	C_2
77778	C_k
11222	C_k
23456	C_1
55555	C_x
.	.
.	.
.	.

Note:
k: number of candidates
t: PreFote threshold
(t<number of eligible voters)

Figure 1: Predefined Fake Vote list structure.

The CCode does not allow the voter to prove to anyone else how he voted, as nobody except the voter knows which CCode belongs to him. The voter can give any PreFote (fake CCode) to the coercer or vote buyer. Nobody can find the difference between real CCodes and PreFotes in the published list. It is not possible for any coercer or vote buyer to reveal the actual vote. As an implementation detail, the PreFote list should not be announced directly. However it can be known by some authorities.

The PreFote scheme provides direct individual verifiability without sacrificing receipt-freeness and accuracy. Any voting protocol can use the PreFote scheme as a building block to solve the voting problem. Furthermore, the PreFote scheme can be directly employed within the cryptographic voting protocols that perform poll-site voting or kiosk voting.

5. Conclusion

In this paper, cryptographic voting security requirements are formally defined and checklists to analyze voting systems are provided. The tradeoff between receipt-freeness and individual verifiability is detailed and a solution to voting problem is suggested.

In future work, we will elaborate our formalization and we will illustrate how the PreFote scheme can be employed within existing voting protocols.

6. References

[1] R. Aditya, B. Lee, C. Boyd, and E. Dawson, "Implementation issues in secure e-voting schemes", *The 5th Asia-Pacific Industrial Engineering and Management Systems Conference*, Goldcoast, Australia, 2004.

[2] J. Benaloh, and D. Tuinstra, "Receipt-free secret-ballot elections," *Proceedings of the 26th ACM Symposium on the Theory of Computing*, 544-553, 1994.

[3] M. Burmester, and E. Magkos, "Towards secure and practical e-elections in the new era", *Information Security - Secure Electronic Voting*, Kluwer Academic Publishers, pp. 63-76, 2003.

[4] O. Cetinkaya and D. Cetinkaya, "Towards Secure E-Elections in Turkey: Requirements and Principles", *International Workshop on Dependability and Security in e-Government (ARES'07),* Vienna, Austria, pp. 903-907, 10-13 April 2007.

[5] L. Cranor, and R. Cytron: "Sensus: A security-conscious electronic polling system for the Internet," *Hawaii International Conference on System Sciences,* Hawaii, 1997.

[6] S. Delaune, S. Kremer, and M. D. Ryan, "Verifying Properties of Electronic Voting Protocols", *Proceedings of IIAVoSS Workshop On Trustworthy Elections (WOTE'06)*, Cambridge, UK, pp. 45-52, 2006.

[7] O. Forsgren, U. Tucholke, S. Levy, and S. Brunessaux, "Report on electronic democracy projects, legal issues of Internet voting and users (i.e. voters and authorities representatives) Requirements Analysis", *European Commission CYBERVOTE Project*, D4 Volume 3, 2001.

[8] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," *AUSCRYPT'92*, Australia, pp. 244-251, 1992.

[9] P. Heindl, "E-Voting in Austria legal requirements and first steps," *Workshop on Electronic Voting in Europe*, Bregenz, Austria, 2004, pp. 165-170.

[10] M. McGaley, and J. P. Gibson, "Electronic voting: a safety critical system," *National University of Ireland, Dept. of Computer Science*, Technical Report: NUIM-CS-TR2003-02, Ireland, 2003.

[11] L. Mitrou, D. Gritzalis, and S. Katsikas, "Revisiting legal and regulatory requirements for secure e-voting," *Proceedings of the 16th IFIP International Information Security Conference*, Egypt, 2002.

[12] Safevote, "Voting system requirements", *The Bell Newsletter*, ISSN 1530-048X, 2001.

[13] R. Sampigethaya, and R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," *Elsevier Computers & Security*, Vol. 25, No. 2, pp. 137-153, 2006.

[14] G. Schryen, "Security aspects of internet voting," *Proceedings of the 37th Hawaii. International Conference on System Sciences*, Big Island, Hawaii, 2004.