Voting Protocol

Vermont Technical College

Last Revised: December 18, 2013

1 Introduction

This document describes a voting protocol. Many such protocols exist with slightly different properties. The protocol here is simple enough to be reasonably understandable while at the same time effective enough to provide useful guarentees.

The principals are V, the voter, and C the *Central Tabulation Facility*. C is an official office charged with tabulating votes and otherwise coordinating the election. C has a public/private key pair $\kappa_c^{(p)}$ and $\kappa_c^{(r)}$. However the voter(s) do not require public/private keys themselves.

The protocol is intended to have the following properties. The primary property is emphasized.

- *V is able to cast a vote with no possibility of anyone (particularly C) associating V's vote with V.*
- V is unable to cast multiple votes.
- Only legitimate voters can vote.

The protocol described here also has the property that it allows V to verify his/her vote was recorded. This protocol has some weaknesses, however. In particular C can cheat and generate fake votes without being detected. In addition if V discovers that C modified his/her vote, V can't do anything about it (at least not without publically claiming the vote).

This protocol makes use of *blind signatures*. This subprotocol works as follows: Alice mathematically modifies her document in a special way that mixes in a random *blinding factor* known only to her. The result of this operation is indistinguishable from a random number. Bob then digitally signs the blinded document. Bob is not able to see the original document. Alice removes the blinding factor resulting in the original document properly signed by Bob. In effect, Bob has signed a document he can't read.

There are several blinding algorithms available but they have to be matched with the digital signature algorithm. In effect the blinding and signing algorithms have to commute. In what follows I will use the notation $B(f, m)$ to

represent the blinded value of m using blinding factor f. I will use the notation $U(f, m)$ to represent the result of unblinding m with factor f. We have

$$S(\kappa^{(r)}, B(f, m)) = B(f, S(\kappa^{(r)}, m))$$

after unblinding both sides of the equation above we have

$$U(f, S(\kappa^{(r)}, B(f, m))) = S(\kappa^{(r)}, m)$$

Note that m is unreadable given $B(f, m)$ without f. In this respect blinding is similar to encryption except that, in general, encryption algorithms don't commute with signature algorithms.

2 Protocol

The protocol proceeds as follows:

1. V prepares a set of message pairs $\mathcal{M}$ where each member of the set m_i consists of two messages $(Y \parallel \mathrm{ID}_i, N \parallel \mathrm{ID}_i)$. Here Y represents a "Yes" vote and N represents a "No" vote. The ID number is an integer randomly choosen by V that is large enough so the probability of anyone else choosing the same integer is negligible. Each message pair m_i has a different ID number but the two messages inside the pair have the same ID number.

   The size of this set is chosen by C. However it might contain, for example, 100 message pairs.

2. V blinds each message in $\mathcal{M}$ with separate blinding factors. For example the pair m_i might become $(B(f_i, Y \parallel \mathrm{ID}_i), B(f_i, N \parallel \mathrm{ID}_i))$. It is important that different blinding factors be used with each m_i.

3. $V \rightarrow \mathcal{M} \rightarrow C$. The voter sends all the blinded message pairs to the CTF, authenticating to the CTF in the process.

4. C verifies that V is a legitimate voter who has not yet voted.

5. C chooses one message pair at random from $\mathcal{M}$ to set aside. For all other message pairs C requests the blinding factors from V.

6. V complies by sending all requested blinding factors to C.

7. C unblinds all but the one message pair previously set aside (and for which C doesn't have the blinding factor anyway) and verifies their correct format. If an invalid message pair is found (for example a pair with different ID numbers on each message) V is penalized to a sufficient degree to make attempts at cheating unprofitable.

8. C signs the blinded messages that were previously set aside. Returning the following to V

$$(S(\kappa_c^{(r)}, B(f_i, Y \parallel \mathrm{ID}_i)), S(\kappa_c^{(r)}, B(f_i, N \parallel \mathrm{ID}_i)))$$

9. V unblinds the two messages in the pair. The result are two votes each signed by C. V chooses the desired vote and then sends $S(\kappa_C^{(r)}, v \parallel \mathrm{ID})$ to C anonymously. Here v is V's vote and ID is the associated ID number on that vote.

10. C verifies the signature on the received vote, checks that the ID has never been used before, tallies the vote, and publishes the pair (v, ID) on a public web site.

11. V searches the web site for her ID to verify that her vote was recorded properly.

3 Informal Analysis