Randomized voting with observers

Gregory S. Warrington
warrings@wfu.edu
June 4, 2007

N.B.: This protocol was first developed in late 2004 and has most recently been drafted as [1]. *For simplicity and the desire to compare with other recent voting systems, we sketch a version here.*

The voting protocol we present here aims for the usual goals of voter privacy and verifiability. However, we also impose the restrictions that we do not trust the administering body (or its agents) and that we do not want to use sophisticated cryptography. Other protocols have been suggested under similar constraints and with similar solutions to ours.

The protocol ours most closely resembles is the Twin voting system of Rivest and Smith [2]. Our protocol is significantly more complicated than Twin. We feel that this added complication yields two main benefits. First, a significant portion of the voters get to verify their *own* ballots, rather than the ballots of earlier voters. Second, certain independent observers are able to directly verify (to a certain degree) the aggregate results of the election.

Our mechanism for allowing some voters to check their own ballots is most easily viewed as a minor modification to Twin (with which we assume familiarity on the part of the reader). We call this new version TwinPrime. In Twin, the voter receives a randomly selected "red" ballot, cast by a previous voter, from a bin. However, at this stage in TwinPrime, a randomly selected red ballot is placed in a canister along with the red ballot just produced by the current voter. The canister is closed, mixed and opened. One ballot is presented to the voter to take home and the other ballot is returned to the bin. This allows one out of every two voters to take home her own receipt. We will refer to this procedure as a Potential Ballot Swap (PBS). If desired, a window could be added to the canister so that the voter can determine whether she ultimately receives her own ballot before she even retrieves it.

While the PBS is a small modification, we feel that TwinPrime will lead to more confidence in the election than Twin. This is for two reasons. First, there is a psychological benefit to seeing that your *own* vote is listed on the PBB. Second, we assume that more voters will be motivated to check the PBB if they know they have their own receipt. Of course, allowing some voters to retain their own ballots opens the door to coercion, but we feel that such coercion would be inefficient enough to not be attractive (see [1] for an analysis). If this were still a concern, the odds of a voter receiving her own ballot could easily be reduced to 1 out of m by placing $m-1$ red ballots in the canister along with the red ballot produced by the current voter.

We now turn to the aforementioned independent observers. In our view, a significant drawback of most verification schemes is that each individual voter is, at best, only allowed to verify a correspondly small part of the results. While this may suffice to ensure integrity of the results on a mathematical level, it does not give each voter a trusted, broad view of the election. The independent voters act as powerful, proxy checkers who have access to much more information than any one voter. A given voter will hopefully have a modicum of trust in at least one of the observers. We remind the reader that the details of our scheme can be found in [1].

We now describe the role played by these observers. First, assume that $n > 0$ observers (such as the LWV) have been registered at a given polling station. After casting her ballot, a voter is given $n+1$ identical receipts. The voter gives one receipt to the administering body. Then she determines a value $0 \leq k \leq n$ by rolling an $(n+1)$-sided die. If $k = 0$, she gives one of her remaining receipts to each of the observers and then exits the polling station empty handed. If $k > 0$, she gives one receipt to each observer *except* observer k. She then performs an PBS with observer k, exiting the station with a receipt that may or may not be her own.

If there are T voters in the election, a given observer will expect to retain approximately $nT/(n+1)$ receipts. He can thereby make a correspondingly comprehensive assesment of the listings on the PBB. For example, he can check that all of the serial numbers on receipts he retains are distinct and that they all appear on the PBB. This guards against the administrator throwing out receipts or generating receipts with the same serial numbers for different voters. He can also, of course, check that the number of votes on the PBB equals the number of voters he witnessed in the polling station. These two checks together can let him be reasonably confident that no "virtual votes" (i.e., votes not actually cast by any voter) have crept onto the PBB.

References

[1] G. S. Warrington. Randomized voting. `http://users.wfu.edu/warrings/research/votingmath.pdf`

[2] R. L. Rivest, W. D. Smith. Three voting protocols: ThreeBallot, VAV, and Twin. `http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf`