Phrase Verified Voting: Verifiable Low-Tech Remote T&P Voting

Enka Blanchard, Ryan Robucci, Ted Selker, Alan T. Sherman

CSEE Department, UMBC

September 18, 2020

Problem

We propose a method by which members of the UMBC CSEE Department's Promotion & Tenure Committee can vote remotely during the pandemic in fall 2020. This method will not add significant effort, time, or expense to the process. The goals are to:

1. Assure that the outcome is accurate;

2. enable voters to verify the correctness of the outcome and that their votes are correctly recorded and tabulated;

3. provide ballot secrecy;

4. produce a list of people who voted and a list of eligible voters who did not vote;

5. require few steps or learning to use or administer; and

6. be acceptable to the UMBC administration.

Because the stakeholders are known and accountable, the method does not have to provide an extremely high level of security and privacy. Simplicity and usability are very important. The method requires one or more trusted parties.

The approximately 35 eligible voters are mainly the tenured faculty in the CSEE Department. One to a few candidates might be voted on in each meeting. For each candidate, there will be up to four referenda:

teaching, service, research, and overall. Each ballot choice is one of YES, NO, ABSTAIN. Voting ABSTAIN is different from not voting. Voters may vote during a committee meeting, or, with permission, they may vote by absentee ballot before the meeting.

Overview of Protocol -- Verifiable Low-Tech Remote Voting

For each referendum, each voter fills out a Google form in which they enter their vote V (YES, NO, ABSTAIN) and a passphrase R (two words chosen by the voter that are memorable but do not identify the voter). The form generates a spreadsheet of the (R, V) pairs and a tally of the votes. After the polls close, each voter can verify that this spreadsheet lists their (R, V) pair and that the tally is computed correctly from these data. Each voter is required to vote and to verify their (R,V) pair and the tally. After voting, each voter is required to fill in a second Google form that records their name, how they voted (absentee ballot, at meeting, did not vote), whether they attended the meeting, and the results of their vote verification. The second form generates a spreadsheet showing the verification results, organized to help visualize how the votes add up; it identifies who participated and any objections raised about the (R,V) values or tally. These two spreadsheets comprise the audit data.

Alternatives

In making our recommendation, we also considered three competing alternatives:

(1) (*Baseline*) With essentially no security, each voter emails their vote to a trusted party who tabulates them. (Variation: email votes to two separate trusted parties, each of whom independently tabulates them).

(2) (*Helios*) Use the Helio verifiable online voting system, which is available through a web interface (https://heliosvoting.org/).

(3) (*Public Vote*) With high integrity and no privacy, each voter fills in a Google form that generates a public spreadsheet that lists, for each voter, their name and vote.

We feel that our department ought to do better than Baseline or Public Vote. Public Vote may also violate university guidelines. Although Helios provides considerable integrity and is fairly easy to use, we have two concerns with it. First, it is not clear if the UMBC administration would find it acceptable, given that the servers do not run on the UMBC network, and considerable time and effort might be required to run it at UMBC. UMBC has a special relationship with Google that permits the use of Google servers. Second, CSEE faculty have experience using and administering Google forms but not using and administering Helios.

Notation and Terminology

EA denotes the Election Authority.

T1 and T2 denote two trusted parties.

V denotes a vote (one of YES, NO, ABSTAIN).

R denotes a passphrase, which is a pair of words selected by the voter.

The Adjudication Panel includes T1 and T2 and others.

A referendum is a specific question about one matter (e.g., research for Professor Z).

Each referendum has a REFERENDUM-ID, which uniquely identifies the referendum.

A committee meeting is a meeting during which one or more referenda are voted on.

A ballot is a Google form that includes a REFERENDUM-ID, referendum date, and place to enter an (R,V) pair.

High-Level Rules

1. All voters (including absentee voters) must use the same voting procedure (i.e., fill out an identical but individual Google form privately).

2. All absentee votes are due at least one hour before the scheduled committee meeting at which a referendum is to take place. Each absentee voter must verify their vote immediately after voting.

3. Late votes will not be permitted. The Google voting form will not accept any votes after the close of voting.

4. Election outcomes are announced at the committee meeting, immediately after voting ends, by displaying Google spreadsheets. No preliminary results are announced before voting ends.

5. All voters (including absentee voters) are required to vote and to engage in the vote verification step. Each voter present at the meeting must verify their vote during the meeting. Each referendum is separately verified.

6. Later in the semester, using Docusign, each committee member signs the committee report, which includes the two spreadsheets produced by the voting and verification steps.

Detailed Voting Procedure

1. The EA announces all referenda and the dates and times of the committee meetings at which they will take place.

2. For each referendum, the EA announces the number of eligible voters and who they are by displaying a Google document, and the deadline by which voters may request permission to vote absentee.

3. The EA identifies trusted parties T1 and T2, who do not vote in any way in the tenure and promotion process, and who preferably are not associated with the CSEE Dept.

4. For each referendum, voters vote by filling out a simple Google voting form, in which they enter R, V. This form does not record the voter's identity.

5. Each voter selects a fresh randomly-chosen R on each voting day. The voter may reuse their R for all referenda held on the same day.

6. The Google voting form creates a spreadsheet of (R,V) pairs.

7. For each referendum, immediately after voting ends, the EA releases the (R,V) pairs as described below, and the vote tally. These voting data are made available to all voters and the Adjudication Panel.

To facilitate verification of the tally, these data are listed as follows. The (R,V) pairs are arranged in three groups by the three possible votes (YES, NO, ABSTAIN). Within each group, the (R,V) pairs are sorted by R values. Within each group, each (R,V) pair is listed on a separate numbered line, with the first line of each group numbered 1.

8. After Step 7, each committee member must fill out a simple Google verification form. People attending the meeting immediately fill out the form during the meeting.

9. Immediately after the in-meeting verification step ends, the EA makes the verification results spreadsheet available to all voters and the Adjudication Panel.

10. Throughout the process, T2 receives the spreadsheets created by the Google forms at the same time as does T1. T2 also receives all communications from T1 to the voters. T2 verifies that the audit data (the two spreadsheets made available to the voters) are consistent with the data T2 received from the Google forms.

11. Absentee voting.

(a) If an eligible voter cannot attend the meeting, they must send an email to Rebecca requesting to vote absentee and stating a reason. Permission to vote absentee will be granted only for the most compelling reasons.

(b) To vote absentee, the voter will fill out the Google voting form at least one hour before the meeting. Immediately after voting absentee, the voter must verify their vote.

(c) Each absentee voter will be able to verify only their vote. In particular, they will see only their (R,V) pair. After the final audit data become available, the voter will also be able to check that these audit data include their (R,V) pair and vote.

Google Voting Form

Ballot for referendum REFERENDUM-ID held on DATE.

Enter two neutral words not associated with you; you might use this generator):

Enter your vote:

(checkbox selection:)

□ YES

□ NO

□ ABSTAIN

Google Verification Form for Voting at Meeting

Verification of public voting data for referendum REFERENDUM-ID held on DATE.

Name:

(automatically recorded)

Select one:

(checkbox selection:)

□ I attended the meeting and voted there.

□ I attended the meeting but did not vote.

□ I attended the meeting but voted absentee.

Are your word pair and vote accurately shown?

(checkbox selection:)

□ YES

□ NO

Are the vote totals correctly shown? That is, is it true that:

the number of votes does not exceed the number of eligible voters, and

the vote totals are correctly listed for YES, NO, and ABSTAIN ?

(checkbox selection:)

□ YES

□ NO

Google Verification Form for Absentee Voting

Verification of public voting data for referendum REFERENDUM-ID held on DATE.

Name:

(automatically recorded)

Select one:

(checkbox selection:}

□ I voted absentee.

□ I did not vote.

Are your word pair and vote accurately shown?

(checkbox selection:)

□ YES

□ NO

Dispute Resolution

1. To make a valid claim that their vote is incorrectly listed, the voter must reveal their name and (R, V) values to the Adjudication Panel. The Adjudication panel will broadcast to the voters that someone (without identifying this person) has filed a dispute involving the (R,V) values. For each valid claim, the EA will correct the V in the audit record and correct the tallies accordingly.

2. Any other dispute will be adjudicated by the Adjudication Panel, which will deliberate remotely in a conference call. The Adjudication Panel should include members who are not associated with the

department.

3. The Adjudication Panel will report the number of claims it received and, for each, a summary of the general nature of the claim and whether and how it was resolved.

Notes

1. To collect the names automatically on the verification form, each voter must authenticate themselves via Google. Although this step can create a small usability cost, it deters proxy voting.

2. Experts estimate that, with human-chosen word pairs, the chance is very small (less than 0.1%) that voters will select the same passphrase. Voters are welcome to use random word generators available on the web (e.g. https://randomwordgenerator.com/ or https://www.wordgenerator.net/random-word-generator.php). Doing so may unnecessarily complicate the voting experience and be superfluous, and duplicates do not necessarily compromise election integrity.

3. The proposed method is not intended to protect against undue influence (e.g., coercion).

How to Vote with Phrase Verified Voting

Every eligible voter is required to vote and to verify their vote. Permission to vote absentee will be granted only for the most compelling reasons. Late votes will not be permitted.

I. The Election Authority announces the meeting date and time, the number of eligible voters, and the deadline for requesting permission to vote absentee.

1. Note the number of voters eligible to vote.

II. Vote at meeting:

1. Open the Google form to vote.

2. Choose two words, and make your voting selection.

III. Verify at meeting:

1. Open the audit sheet made public by the EA and check that your word pair is present with your vote next to it.

2. Check the accuracy of the vote totals and check that the number of votes does not exceed the number of eligible voters.

3. Open the Google verification form and fill it out.

IV. If you cannot attend the meeting, vote early:

1. By the announced deadline, send Rebecca an email requesting permission to vote absentee. State your reason. Your absentee application will be reviewed and accepted or rejected expeditiously.

2. At least one hour before the meeting, open the Google form to vote.

3. Immediately after you vote, open the Google form to verify your vote.

Note: In Step 3, people who vote absentee will be able to verify only their vote; later they can also check the public audit data.