Version of 29.7.05

A protocol for machine-based voting

D.H.Fremlin

University of Essex, Colchester, England

1 Introduction In this note I describe a protocol for machine-based voting which is relatively immune to incompetent or dishonest operation and to voter fraud. It is a minor development of the protocol described in Vernitski 05. It is assumed that a democratic tradition or aspiration gives real power to public opinion, to the point that a sufficient scandal can force a new election, but that individual officials may not always be honest and that unscrupulous local party organizers are to be expected.

Five organizations A, B, C, D and E are required; it is assumed that each individually may be untrustworthy but that the risk of corrupt collaboration between any two organizations can be ignored. E is responsible for organizing electoral rolls, communicating with voters and administering polling stations; B is responsible for the machines collecting votes; A, C and D act in the background as coders.

2 The protocol Let $C = \{c_1, \dots, c_m\}$ be the set of candidates in (say) alphabetical order, and N a set of identifiers (I will speak as if it is a set of numbers) with $\#(N) \gg \max(\#(V), m!)$ where V is the set of voters. V and $c_1, \dots, c_m$ are publicly known before the electoral process begins, but N is known only to A, B, C and D.

step 1 A chooses an injective function $\phi : N \to N$ and a set $N' \subseteq N$ with $\#(N') = \#(V)$, B chooses a bijective function $\beta : N \to N$, C chooses a bijective function $\gamma : N \to N$ and D chooses a function $\delta : N \to S_m$, the set of permutations of $\{1, \dots, m\}$; none of these functions are divulged to anyone else except as detailed below. All should be 'random'; in particular, $\delta^{-1}[\{\pi\}]$ should be large for every $\pi \in S_m$.

step 2 B tells A what the function β is; C tells D what the function γ is; D tells A what the function $\delta\gamma$ is (but *not* what the function γ is); D tells B what the function δ is; A tells B what N' is. A opens a website which will provide the list $(c_{\pi_n(1)}, \dots, c_{\pi_n(m)})$ to any enquirer submitting a correct pair $(n, \phi(n))$.

step 3 For each $n \in N'$, A calculates $\pi_n = \delta\gamma\beta(n) \in S_m$ and sends the triplet $(n, \phi(n), \pi_n)$ to E.

step 4 E sends each voter a different triplet $(n, \phi(n), \pi_n)$ in the form of the 'voter number' n, a 'check number' $\phi(n)$ and a list of the candidates in the order $c_{\pi_n(1)}, \dots, c_{\pi_n(m)}$.

step 5 The actual election now takes place; each voter sends B the pair (n, j) where his voter number is n and his chosen candidate is $c_{\pi_n(j)}$.

step 6 B collects the pairs $(n, j) \in N' \times \{1, \dots, m\}$ received from voters and for each such pair sends the pair $(\beta(n), j)$ to C.

step 7 C collects the pairs (n', j) received from B and for each such pair openly publishes the pair $(\gamma(n'), j)$.

step 8 D reviews the pairs (n'', j) published by C and for each such pair publishes the pair (n'', c_k) where $k = \delta(n'')(j)$.

step 9 The votes for each candidate can now be calculated from D's published list, since if the voter with number n chooses candidate c_i then

B receives $(n, \pi_n^{-1}(i))$

C receives $(\beta(n), \pi_n^{-1}(i))$

D receives $(\gamma\beta(n), \pi_n^{-1}(i))$ and publishes $(\gamma\beta(n), c_k)$ where

$$k = (\delta\gamma\beta(n))(\pi_n^{-1}(i)) = \pi_n\pi_n^{-1}(i) = i.$$

3 The basic defensive structure Since nobody knows both the functions β and γ, nobody can associate a published result (n'', j, c) with any particular voter v, even if they have induced v to divulge his voter number.

C does not know the functions δ and β, so can affect the output only by random distortions which will, on average, do no more than narrow the gap between candidates. D's output at the critical step 8 will be checked by B, and if he has given false values for $\delta\gamma$ at step 2 this also will merely add noise. B can bias the result, since he will know the physical location of voters and can disenfranchise selected groups by randomising or deleting their votes. He does not know the permutation π_n associated with a voter, so cannot know for sure what the effect of his malfeasance is. (This is the reason for the 'checking number' $\phi(n)$; B should not be able to search A's website systematically without it being obvious that something is going on.) A has more scope, since he knows $\delta\gamma$ and can arrange that votes for favoured candidates are correctly treated while others are randomised, by providing false values of the π_n.

E can use the traditional methods of losing voter forms in the post or blocking polling stations, but these are immediately detectable by voters. He can send false values of π_n; but any suspicious voter can detect this from A's website. He can duplicate voter forms, so that opposition supporters appear to be voting twice, but this is picked up in real time by B.

Concerning voter fraud, attempts to vote twice and attempts to vote with home-made voter numbers can be detected in real time by B.

4 Further checks (a) Candidates will ordinarily know where their support is concentrated. For this reason, it might be right to require A to give each voter a 'location' tag l, so that B receives a triplet (n, c', l), and C receives the triplet $(\beta(n), c', l)$. As B will usually know the location and time at which a vote was cast, he is getting little new information from the tag. Actual publication of the tag should be done by D, ordinarily publishing triplets (n'', c_k, l), but omitting tags in cases where the pair (c_k, l) is repeated by too few other votes. Candidates will then be able to see the locations from which most of their votes were gained, and can organize a protest if they feel cheated.

If it is felt undesirable for C to be told where voters live, a code shared by B and D (e.g., a bijection from $L \times M$ to N, where L is the set of locations and M is a large set) can be used to isolate him from this information.

(b) There must be no mechanism for any voter to obtain official confirmation that his individual vote was correctly handled, since any such mechanism would open a method of coercion. However, a *block* of voters, of sufficient size (at least 100 in each location from which they come), could ask for a re-run of the process on their votes. The basic method of protest against an apparently rigged election would be to organize such a block of voters willing to repeat their votes in public. B would be able to declare a figure for the number who had changed their votes, and the same number should appear from the final output. If there were many of these, there would then be an ordinary row about whether the voters were dishonest, or intimidated, or forgetful, or whether B or C was cooking the result. If the declared vote derived from D's output was different from the input, then it would be clear that something had gone wrong with the system.

(c) If E were to send duplicate papers out, half of these would be detected at voting time by B, and the voters notified. Complainants would be able to advertise their numbers, so that if E has sent two identical papers to members of opposition groups both will be presented, and he will be reduced to claiming that one is a forgery. Similarly, if a voting paper fails the test of A's website there will be something for an opposition newspaper to publish.

5 General elections No new ideas are needed to handle general elections. If (as in the UK at present) electoral rolls are administered locally, the part of E in the scheme here becomes divided between many authorities; there is much to be said for them all following the same format. The functions β, γ and δ now become functions of two variables, voter number and constituency; only A and D really have to take any notice, since the different constituencies may have different numbers of candidates.

6 Practicalities The following details are suggested as a minimal change on the present UK system, but the ideas would I think be generally applicable.

(a) The 'polling card' each voter is sent before the election, currently carrying name, address, polling station and electoral roll number, would now have also have to have the voter's numbers n and $\phi(n)$, his list of candidates and (if applicable) constituency and location tag. These should be delivered in sealed envelopes. To avoid large numbers of mistyped voter numbers, the voter number, constituency and location tag should be in machine-readable form, e.g., as a barcode, as well as in human-readable form.

(b) At present, no identification beyond a declaration of name and address is required in UK elections; even the polling card is not essential, as the polling officers have the electoral register before them, and mark the names of those who have voted. On the system described in this note, electors would need to take polling cards to vote. They would no longer be issued with ballot papers. The voter would approach a machine with a screen, a barcode reader and a number-pad, pass the barcode on the polling card over the reader, and key in the number of the chosen candidate. The pair (n, j) would be displayed on the screen with a 'confirm/cancel' option.

It would in my view be right to allow a 'null' vote, corresponding to a spoilt ballot paper; this would pass through the system and be finally published as $(n'', -)$ in both C's and D's lists.

(c) At present, ballot papers are punched, in the presence of the voter, with an identifying code; this is I suppose a precaution against forged ballot papers being slipped into the box under cover of a genuine one. This would no longer be a concern. But a real danger in present UK conditions is of an individual pressuring others to allow him to cast their votes. Once he is in the polling booth it may be difficult for the polling officers to be sure that a voter is voting only once. Some mechanism - e.g., a plastic disk to tell the voter which machine to use, and a button to tell the machine that one and only one vote is expected - could, and probably should, be in place to check this.

(d) There would have to be provision for correcting misread barcodes. Depending on the sophistication of the electorate, this could either be open to ordinary voters, or require the intervention of a polling officer. The polling officer would be responsible to the organization E, so there would be no great breach of security in his seeing the voting number, as long as he did not see the vote.

(e) If B detects double-voting, the natural response would be to put both votes into limbo, and send the voter number and the times and locations of the votes to E (but not, of course, the votes themselves). E would then be in a position to contact the voter and ask which, if either, of the votes (identified by place and time) should be counted. I am suggesting this only for the purpose of maintaining the morale of electors who are told that they have already voted. If there were enough such cases to make a difference enough people would know to make a scandal of it.

This is not quite the same as the phenomenon considered in 4c, where a voter is protesting and E knows, or ought to know, that there is more than one voter with that number.

(f) In the last couple of years, the UK has experimented with postal voting. The results have not been satisfactory, and there have been many accusations of stolen votes and mild coercion. In my view all voting should be done in the presence of an official polling officer; in particular, no form of on-line electronic voting should be considered. We could, however, allow away-from-home voting, in ordinary polling stations, subject to a tightening of the identification process; e.g., requiring driving licence or passport with name and address matching the polling card. Even embassies and consulates abroad could be equipped with voting machines to accept the votes of expatriates. Similarly, one can imagine a travelling voting machine, accompanied by a polling officer, for the use of those physically unable to attend a polling station.

7 Further remarks (a) Since the functions of A, C and D are purely computational, they can easily be performed by organizations which are independent to the point of being in different continents. Because they have very little actual work to do, organizations could be found for which their reputations matter more than the profit to be gained by repeat business from the same authorities.

(b) There is a greater vulnerability in the organization B. B would have a local investment to protect, and local employees who might be partisan. In one way, machines would be easier to guard than ballot boxes because greater expertise would be required to manipulate them. On the other hand, since they would (on the scheme suggested here) be on-line during voting, there would in principle be a danger of interference from a distance, and they had better have non-standard firewalls.

(c) In preparing these notes I have had in mind not just the UK experience but what I have read recently about such places as the Philippines and the Ukraine. Some of the original interest in improved designs for machine voting came from the experience of the US presidential election in 2000. But while a scheme such as this might have reduced the time wasted and the bitterness engendered by court proceedings, it would only by chance have made that result any more representative of the people's will, as the margin between Bush and Gore in Florida was less than the change to be expected if the vote had been held one day earlier or later.

Reference

Vernitski A. [05] 'A simple protocol for voting', Technical Report 2005-2, Department of Mathematical Sciences, University of Essex, July 2005.