Some Problems with End-to-End Voting

Douglas W. Jones
Department of Computer Science
University of Iowa
Iowa City, Iowa
Email: jones@cs.uiowa.edu

I. Introduction

End-to-end cryptographic voting faces several hurdles. I would like to discuss two of them. One involves the legal question, what is a secret ballot? The other involves a marketing question, how can we explain this to election administrators?

II. What is a secret ballot?

One of these is a legal hurdle, centering on one key question: What is a secret ballot? There are two sides to this question: How secret are the ballots cast using end-to-end voting, and what exactly do we mean when we say that voters have a right to a secret ballot?

While the cryptographic models of most end-to-end voting systems are receipt free, the cryptography is always embedded in some kind of physical medium. In some cases, this embedding weakens the secret ballot properties of the system. Scantegrity II ballots, for example, have unique numbers printed on each ballot. Regardless of the cryptosystem, voters wishing to sell their votes may use these numbers to sell their votes to anyone with access to the original paper ballots. In contrast, Prêt à Voter does not have this weakness. It would be a worthwhile effort to carefully classify the different end-to-end schemes according to the degree to which they are receipt free.

All end-to-end voting systems issue some kind of number to voters so that they may verify that their ballots have been delivered, in encrypted form, to the public bulletin board for counting. By necessity, this number is linked to the encrypted ballot, and by necessity, it is possible to decrypt the ballot – if this were not so, the ballot could not be counted. Mix nets and other cryptographic trickery must therefore be considered to be procedural safeguards, albeit very strong ones, for preventing abuse of this linkage.

Unfortunately, there does not appear to be a clear legal answer to exactly what it means to say that voters have a right to a secret ballot. When the right to a secret ballot was instituted in the 19th century, there were two legally distinct approaches to ballot secrecy.

The British Ballot Act of 1872 required that "each ballot paper shall have a number printed on the back" and required that this number be recorded in the pollbook with the voter's signature. The numbering required by this act is comparable to that used for Scantegrity II ballots, but the Ballot Act goes one step farther by requiring that the state explicitly link this number to the voter who cast each ballot.

Voting in Great Britain is still conducted under the terms of this 1872 law, and it fair to ask how it is that this law grants British voters any right to a secret ballot. The answer lies in what is done with the pollbooks after each election. The Ballot Act requires that these be sealed, to be opened only under order of parliament or of a competent court. In effect, the linkage between voter and ballot is a state secret.

End to End voting systems, in general, incorporate aspects of the British model of ballot secrecy. In general, they do not explicitly link voter identity to the ballot, but the ballot number taken away by the voter can, with the cooperation of the custodians of the cryptographic keys, be linked to the plaintext of the ballot.

A stricter model of ballot secrecy emerged in the 19th century in many U.S. Jursidictions. The Washington state constitution of 1889 exemplifies this, requiring that the state "secure to every elector absolute secrecy in preparing and depositing his ballot." The Wyoming constitution of 1889 and the Virginia constitution of 1902 contain similar provisions. Virginia's constitution went further, prohibiting any distinguishing marks from being printed on the ballot. By 1911, legislation in Delaware forbade election clerks from making any "distinguishing mark of any kind" on ballots, and Michigan legislation forbade voters from making any such mark.

A legislative prohibition against ballots that bear any distinguishing mark would clearly seem to prohibit the ballot numbers required by many end-to-end voting schemes, whether or not these marks are intended to be human readable or obscured, for example, by using bar codes.

Distinguishing marks are merely a mechanism that can be abused. Forbidding one such mechanism does not necessarily prevent the abuse, if other mechanisms are available. The wording of the Washington State Constitution, on the other hand, addresses the end goal, "absolute secrecy," without mention of mechanisms that might subvert or support that goal.

The example from the Washington state constitution illustrates an important point. While the wording seems to take an absolutist stance toward ballot secrecy, the tradition of

interpretation of that wording is what matters. Washington has moved in recent decades toward universal use of postal voting. It is very difficult to interpret postal voting as a technology that secures "to every elector absolute secrecy," since a voter may easily permit someone to examine how they vote while filling out a postal ballot at home.

What has happened in Washigton is that the wording of the state constitution has been interpreted as granting each voter the right to vote in secret, and voters are free to waive their rights. When the secret ballot was instituted in the 19th century, it was generally understood that one aspect of the secret ballot was that it deterred dishonest voters from selling their votes. This aspect of the secret ballot appears to have been lost in the move to interpreting secrecy narrowly as a right.

International law also has something to say about what is and is not a secret ballot. The Charter of Paris for a New Europe was signed in 1990 by all of the member states of the Conference on Security and Cooperation in Europe, including the US and the USSR. Annex I requires that the participating states "(7.1) ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public." The phrase "or equivalent free voting procedure" serves as an effective definition of what is intended by the phrase "secret ballot." In effect, this rules out interpretations of ballot secrecy that permit voters to be subject to coersion.

The Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe released a discussion paper in 2008 entitled In Preparation of Guidelines for the Observation of Electronic Voting. This paper discusses, at some length, the interpretation of Annex I of the Charter of Paris, in the context of electronic voting. Clearly, a discussion paper is not the binding final interpretation of the law, but the arguments in this paper reflect careful thought and the results of considerable experience observing the use of electronic voting in many of the OSCE member states.

I suspect that end-to-end cryptographic voting methods will face significant legal challenges in many states. The fundamental problem is not that these new voting methods are more or less secure than existing methods, but they are different, and they involve mechanisms, notably various cryptographic schemes, that are both hard to understand and not anticipated in current secret ballot law.

Unfortunately, I think these challenges lead to significant risks. It would be very easy to set some very bad precedents that muddy the already murky answers we get when we ask exactly what is required by the right to a secret ballot.

It would be very helpful if we could involve lawyers in an effort to draft a model statement of what we want from the right to a secret ballot that could serve as the basis for new legislation. The work already done on interpreting the Charter of Paris may provide useful guidance, in this effort.

III. Transparency

I participated in the 2006 election assessment mission to the Netherlands, sponsored by the Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe. One voting system tested in the election we observed was the Rijnland Internet Election System, used by about 20,000 expatriate voters in the 2006 Dutch parliamentary elections.

RIES is a publicly verifiable end-to-end cryptographic voting system allowing remote voting over the Internet, designed specifically as an alternative to postal voting. It incorporates a public bulletin board where voters can inspect all of the encrypted ballots that have been cast, and at the close of the polls, the bulletin board is decrypted and the votes counted.

RIES is not receipt free. It was designed to have secret-ballot properties comparable to postal voting. If a voter discloses an encrypted ballot before the public decryption, that can serve as a receipt. However, the issues that concern me lie in areas where this shortcoming is not important.

In practice, an election cycle using RIES begins with the preparation of envelopes each containing one pseudo-random authorization to vote. These printed in pseudo-random order on self-carbon security envelopes, like bank statements, so that nobody can see what is printed inside. These envelopes are then distributed to voters on a first-come first-served basis, so that nobody (in theory) knows which voter gets which authorization code.

The problem is, how do you guarantee that the set of authorization codes has been destroyed? Proving that the seeds for the pseudo-random sequence have not been retained somewhere is difficult under the best of circumstances. The developers of RIES suggested inviting observers to the process followed by public destruction of the entire computer system used to generate this file as the best solution.

The government opted to do the printing in a secure facility behind locked doors without observers. This move would give a corrupt government intent on running a sham election all the opportunity it needed to engage in a wide range of fraud.

We are going to face this kind of mistake routinely with voting systems based on cryptography. The "security instincts" of computer system administrators will push for closed doors and exclusion of observers again and again when the actual security requirement is transparency. They will want to enforce backup policies for data that must not be duplicated.

This illustrates a second problem. With classical paper-based elections, the primary security critical activities occur on election day, in polling places and immediately after the polls close. This period is one where it is fairly straightforward to mobilize large numbers of observers – it is common,

for example, to find observers from several major parties at each polling place.

In contrast, with electronic voting schemes, and particularly with cryptographic voting schemes, some of the most critical events occur very early in the election cycle, at a time when it is difficult to find observers. With the Dutch parliamentary elections, the international election assessment mission had not even been organized at the time when the key activities took place. We need to find ways to bring these early critical activities out of the closet, both figuratively and literally, before we can really make strong statements about the safety of these new voting technologies, particularly when they are in the hands of governments that have less than stellar records with regard to election conduct.