# MODELLING CONTEXT FOR THE DESIGN OF REMOTE ELECTRONIC VOTING SCHEMES

**ABSTRACT**

There exists in the academic literature, a plethora of electronic voting schemes(for example (Cranor & Cytron 1997, Juang & Lei 1997, Benaloh & Tuinstra. 1994)). Typically, proposed schemes are accompanied by a description of the properties that an implemented electronic voting scheme would be expected to exhibit. These properties are described informally as for example, "ballot secrecy" or "universally verifiable". To evaluate the proposed scheme, these informal notions are commonly incorporated in a mathematical model before a proof is outlined demonstrating that the proposed scheme does indeed exhibit the necessary properties.

A disadvantage of this approach is that the required properties for a electronic voting schemes are implied to be static, with each new scheme to be evaluated against that standard. However, the context in which a voting system is employed varies considerably. Voting systems are employed in a variety of applications, with varying properties required as a result. Even voting systems that are employed in similar contexts, such as different electoral systems, exhibit varying properties according to the priorities of an entity organising a vote.

This paper outlines the perceived failing of the current approach to designing and implementing electronic voting schemes, with regard to the considerable variation in the properties required. In addition, an approach is outlined that models the required properties of voting systems with the intention of providing a basis for evaluating electronic voting schemes in a particular context.

## 1. INTRODUCTION

In the academic literature, the design of electronic voting schemes has commonly been assumed to be an application of cryptography (Rjašková 2003, Murk 2001). Indeed, a plethora of electronic voting schemes employing cryptographic primitives have been proposed, analysed and refined, for example (Cranor & Cytron 1997, Juang & Lei 1997, Benaloh & Tuinstra. 1994). Typically for such proposals, before the new electronic voting scheme (or refinement of an existing scheme) is introduced, the properties against which the scheme will be evaluated are defined.

Implicitly in this consideration is the distinction between a *voting system*, which specifies certain properties as to how the vote will be conducted; and a *voting scheme*, which should be implemented with the desired properties. The voting system is therefore the specification of how a decision will be reached, via some vote casting process, a definition similar to Farquharson's (Farquharson 1969).

The properties of the voting system may be defined informally for example, *"secrecy: only the voter may know how they voted"*, before being modelled more formally alongside the cryptographic primitives of the new scheme. Proofs are then developed in order to demonstrate that the scheme does conform to the required properties for the voting system. Some indication of the complexity of the voting scheme, with respect to number of computations or communications for different participants (voters, election authorities etc) may also be included.

The assumption that remote electronic voting schemes require cryptography does result in some limitations for the schemes. Most significantly, each voting scheme is only evaluated within a specific voting system context. The potential applicability of electronic voting schemes is limited to voting systems that mirror the particular properties that the scheme is shown to satisfy. Such properties may sufficiently describe a single voting context, but there is no indication of the appropriateness of the voting scheme with regard to other voting system contexts. This limitation may be illustrated by the range of electronic voting schemes that have been proposed for highly specific contexts, for example Jury Voting Protocols (Hevia & Kiwi 2002) or circumstances where the relationship between votes and voters may need to be revealed (Lee 1999). More

subtly, the range or properties associated with voting systems used to select representatives for government of organisations (electoral systems) prevents electronic voting schemes developed for one electoral context unsuitable for another.

By example, consider the electoral system for the United Kingdom (UK) and the Republic of Ireland (RoI). Both currently employ a paper ballot and ballot box voting scheme, and so it may be argued that the scheme employed in the UK is transferable to the RoI. However, the specific implementations of the voting scheme vary to reflect the required properties of the voting system. The UK electoral system employs a simple plurality mechanism for choosing a single candidate in a constituency (RPA 1983), whereas single transferable vote is employed in RoI (Jackson, Rosenstiel & O'Connell 1997). As a consequence, Irish voters must mark the ballot paper with an ordering of candidates, an action which would spoil a ballot in the UK. More significantly as a result of a legal ruling, the marking of ballot counter-foils with a voter's electoral roll number is specifically barred in the RoI, in order to guarantee that in no circumstances can a voter's choice be identified (McM 1972). In the UK, the same technique is employed to permit a scrutiny of ballots in order to remove those found to be cast illegally from the tally (Jackson et al. 1997).

This example indicates that although there has been a substantial body of research developing electronic voting schemes, there has been less consideration of the context in which an electronic voting scheme may be deployed. This presents a difficulty for election administrators, and indeed for commercial vendors, since at present, there is no appropriate framework for deciding which electronic voting scheme is optimally suitable for a particular context. Indeed, such a framework might indicate that no existing electronic voting scheme adequately satisfies a particular context for a voting system.

## 2. PROPOSED MODELLING FRAMEWORK

The above introduction outlines the difficulty of evaluating and comparing the properties that voting systems require for their implementing voting schemes. To remedy this situation, it is proposed to develop a modelling framework for voting systems that identifies the particular properties required for an implementing voting scheme. Using this model, it is anticipated that, for example, election administrators would be able to determine the properties of the voting system for their context. This model would then be employed in choosing an existing voting scheme that is demonstrated to be suitable, or for vendors to develop a new voting scheme for the context desired by a vote administrator. The significant contribution of this approach would be permit the context of a voting system to be specified within a standardised framework, permitting the evaluation of voting schemes in different contexts.

In the remainder of this paper, the scope of the various components of the proposed framework is outlined. An outline of the various parameters that will be specified for each component is included to outline how the new framework will be constructed.

### 2.1 SECRECY

As noted above, secrecy is a commonly assumed property required by voting systems, particularly electoral systems. However, as noted in the comparison of UK and RoI electoral law, the notion of what constitutes secrecy varies considerably, depending on the context of a voting system. Including statistical information regarding the vote (the tally of values cast, for example) further complicates the notion of secrecy. For example, certain jury voting systems require the result of a vote to be announced as being within a certain threshold (unanimous guilt, undecided etc), rather than the precise tallies of votes. In other circumstances, far more information is released regarding the vote, for example in committee voting where votes are recorded as being associated with their choice.

In order to model the secrecy requirements of a voting system, it is proposed that the release of information concerning votes cast be specified by a set of *permitted channels*. Each channel is specified by a set of properties:

- Participants - roles within the voting system. This may include voters, voting authorities, external observers, or other roles necessary for the voting system. An entity may adopt several roles in parallel during the operation of the voting system.

- Capabilities - the on the channel (read and/or write). Through the specification of Participant capabilities, types of channel are identifiable.
  - Unicast - a single participant in the voting system has read capability.
  - Multicast - at least two participants in the voting system have read capabilities.
  - Broadcast - all participants in the voting system have read capability.

  Given that an entity may adopt several participant roles simultaneously, the framework must also provide the capability to regulate participants active on several channels.
- Persistence - the period through which participants may employ their capabilities. The persistence of a channel may be further specified by a start and stop event, for example a date and time.
- Legal Content - the information that may be legally written onto the channel by a participant with the appropriate capabilities.

Through this approach, all information is assumed secret, unless permitted for release via a designated channel. This approach permits a concise definition of secrecy for a voting context, and in particular permits an evaluator to determine whether a voting scheme releases extra information than is desirable.

## 2.2 VERIFIABILITY

Ensuring that information released concerning votes cast is a requirement commonly associated with voting schemes designed for electoral systems (Benaloh & Tuinstra. 1994). Verifiability for electoral systems is often complicated by the requirements outlined above, which limit the amount of information released concerning votes cast. However, which particular components of information need to be verified varies between voting systems. Further, the action of verifying different components is the capability of different participants in the voting system. Consequently, verification requires the following parameters to be specified:

- The specification of a component of information generated for the voting system to be verified.
- A participant who wishes to verify the information from the voting system.
- The criteria by which the participant will decide whether they have verified the information from the voting system. This criteria should not make reference to the verifying mechanism, a consideration for the particular voting scheme implementation.

## 2.3 COMPLEXITY

The complexity of a particular voting system has considerable impact on the choice of voting scheme to implement. For electoral systems, where a considerable variation exists in the methodology for electing representatives exists (various proportional and plurality systems for example), the choice of an implementing mechanism that would ameliorate increased complexity for the voter may be desirable. Further, voting schemes that reduce the effort required by authority participants to compute a tally for complex electoral systems may also be desirable. However, modelling complexity for voting systems is non-trivial, and may be expressed in a number of elements of the system.

To begin the modelling of complexity for vote casting, it is possible to provide a generic definition of a vote for which parameters may be chosen to model a particular voting system. Such parameters would include:

- Number of options on the ballot
- Maximum and minimum number of options to be selected by the voter.
- A yes/no option as to whether an ordering is applied to the options selected by the voter.

Other, more complex requirements also need to be specified, for example, the number of interactions necessary between participants during vote casting. Evaluation of a voting scheme against complexity requirements thus provides a description of practicality, independent of the assurance achieved for secrecy, verifiability, or other requirements.

## 3. CONCLUSIONS

Research into electronic voting has resulted in a considerable number of schemes that are analysed with respect to the particular properties they exhibit, rather than the particular context within which they may be employed. The framework proposed here attempts to remedy this deficiency by providing a standard method for specifying the properties of voting systems. This framework, rather than evaluating each voting scheme in isolation, would permit each to be evaluated against particular requirements as specified by the context of a voting system, rather than the designers of a voting scheme.

## ACKNOWLEDGMENTS

This work is supported by Microsoft Research, Cambridge.

## REFERENCES

Benaloh, J. & Tuinstra., D. (1994), 'Receipt-free secret-ballot elections.'.

CES (2002), 'e-voting security study', Communications and Electronic Security Group (CESG). Available at `http://www.edemocracy.gov.uk/library/papers/study.pdf`.

Cranor, L. & Cytron, R. (1997), Sensus: A security-conscious electronic polling system for the internet, *in* 'Proceedings of the Hawai'i International Conference on System Sciences', IEEE Computer Society Press, Wailea, Hawaii.

Farquharson, R. (1969), *Theory of Voting*, Yale University Press, New Haven.

Hevia, A. & Kiwi, M. A. (2002), Electronic jury voting protocols, *in* 'Latin American Theoretical INformatics', pp. 415–429.

Jackson, P., Rosenstiel, C. & O'Connell, S. (1997), 'Ballot secrecy', Electoral Reform Society.

Juang, W.-S. & Lei, C.-L. (1997), 'A secure and practical electronic voting scheme for real world environments', *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Science* **E80-A**(1), 64–71.

Lee, J.-H. (1999), 'The big brother ballot', *Operating Systems Review* **33**(3), 19–25.

Malkhi, D., Margo, O. & Pavlov, E. (2003), E-voting without 'cryptography'.

McM (1972), 'McMahon vs Attorney General'. IR69 at p106.

Murk, Ö. (2001), 'Designing electronic voting'.

Rjašková, Z. (2003), Electronic voting schemes, Master's thesis, Comenius University, Bratislava.

RPA (1983), 'Representation of the People Act'. Ch. 2.