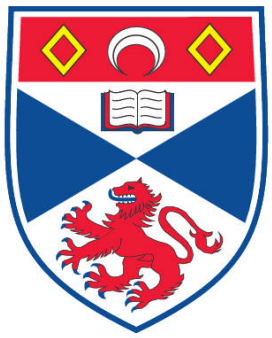
PRACTICAL POLLSTERLESS REMOTE ELECTRONIC VOTING

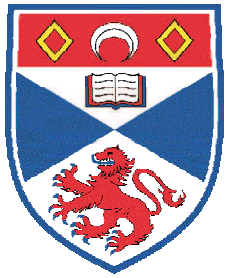
Timothy W. Storer

A Thesis Submitted for the Degree of PhD
at the
University of St. Andrews



2007

Practical Pollsterless Remote Electronic Voting



A thesis to be submitted to the
UNIVERSITY OF ST ANDREWS
for the degree of
DOCTOR OF PHILOSOPHY

by

Timothy W. Storer

School of Computer Science

University of St Andrews

April 2006

But it appears to me indispensable that the signature of the elector should be affixed to the paper at a public polling-place, or if there be no such place conveniently accessible, at some office open to all the world, and in the presence of a responsible public officer. The proposal which has been thrown out of allowing the voting papers to be filled up at the voter's own residence, and sent by the post, or called for by a public officer, I should regard as fatal. The act would be done in the absence of the salutary and the presence of all the pernicious influences. The briber might, in the shelter of privacy, behold with his own eyes his bargain fulfilled, and the intimidator could see the extorted obedience rendered irrevocably on the spot.

– John Stuart Mill.
Considerations on Representative Government,
1860.

Abstract

This thesis describes the design of a novel class of *pollsterless* voting schemes. Many cryptographic voting schemes necessitate a pollster because the client side computations are beyond the understanding or ability of the voter. Such interactions require that the voter trust the software to perform operations on their behalf, and in effect, the pollster acts as the voter. Conversely, the pollsterless schemes presented here permit voters to interact with an election authority directly, without complex computations. Pollsterless schemes have the additional advantage of permitting voting on virtually any networked device, increasing the potential *mobility* of voting.

The proposed pollsterless schemes are implemented and then evaluated with respect to the particular requirements of the UK public election context. The flexibility of pollsterless schemes in particular are demonstrated to fulfill the diverse requirements that may arise in this context, whilst the mobility of pollsterless schemes is demonstrated to fulfill requirements to improve the convenience of voting.

I, Timothy W. Storer, hereby certify that this thesis, which is approximately 55000 words in length, has been written by me, that it is the record of work carried out by me, and that it has not been submitted in any previous application for a higher degree.

date _____ *signature of candidate* _____

I was admitted as a research student in September 2002 and as a candidate for the degree of Doctor of Philosophy in September 2003; the higher study for which this is a record was carried out in the University of St Andrews between 2002 and 2006.

date _____ *signature of candidate* _____

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

date _____ *signature of supervisor* _____

In submitting this thesis to the University of St. Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any *bona fide* library or research worker.

date _____ *signature of candidate* _____

Acknowledgement

This thesis, and the work it describes, would never have been completed without the support of many others.

Those who have provided academic guidance during the course of this project include my initial supervisor, Ursula Martin, who provided much early input; Pam Briggs and Linda Little at the PACT Laboratory at Northumbria University; and James McKinna within the School. In addition, the work was generously funded by Microsoft Research, and later by ESRC.

Many members of the School played a part in ensuring that this thesis was completed and submitted on time. I thank in particular Graeme Bell, James McKinna and Tom Kelsey, who gave their time to read the final drafts and/or provided practice for the oral defence. Thanks also to my friends in the School who contributed by simply making another four years as a student so worthwhile; and to my parents for not asking too often whether I would be getting a job soon.

My supervisor, Ishbel Duncan, deserves special thanks for her constant support over four years, ensuring that the work was completed. Ishbel proved an endless source of advice, ideas, encouragement and (most importantly) candid criticism.

And finally, Amanda, who will almost certainly never read this, I couldn't have done it without you.

Published Research

Tim Storer and Ishbel Duncan.
Polsterless remote electronic voting.
Journal of E–Government, 1(1):75–103, October 2004.

Tim Storer and Ishbel Duncan.
Practical remote electronic elections for the UK.
In Stephen Marsh, editor, *Privacy, Security and Trust 2004 Proceedings of the Second Annual Conference on Privacy, Security and Trust*, pages 41–45, Fredericton, New Brunswick, Canada, October 2004. National Research Council Canada, University of New Brunswick.

Tim Storer and Ishbel Duncan.
Modelling context for the design of remote electronic voting schemes.
In Pedro Isaías, Piet Kommers, and Maggie Macpherson, editors, *IADIS International Conference e-Society 2004*, volume 2, pages 1001–1004, Avila, Spain., July 2004. IADIS Press.

Tim Storer and Ishbel Duncan.
Two variations of the mCESG pollsterless e-voting scheme.
In Randal Bilof, editor, *COMPSAC 05 The 29th Annual International Computer Software & Applications Conference*, pages 425–430, Edinburgh, Scotland, July 2005. IEEE Computer Society.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Overview

This chapter describes the motivation for this thesis and formulates the hypothesis that for a remote electronic voting systems to be deployed in the UK, a remote voting *scheme* must be designed with respect to the particular requirements of the UK's specific context. The chapter concludes by describing the structure of this thesis.

1.1 Remote Electronic Voting in Computer Science

In recent years, voting systems have become a highly politicised and controversial topic for computer scientists and other researchers [34], with many raising the prospect of the accuracy of public elections being violated by the use of electronic technologies [57, 91]. Electronic voting systems have even been used to direct discussion on the risk of interaction between digital technologies and society in university courses [4]. Yet the 'automation of honesty' which is embodied in the topic of electronic voting has a long history stretching back to the ancient Greeks [13]. More recently, the introduction of networked voting technologies has raised the prospect of voters participating in elections remotely without the

need to attend a polling station. Remote electronic voting has been proposed as a means of improving the experience of voting through increased convenience, improved accuracy in recording voter intentions and improving equality of access to a voting system across a broad spectrum of voter capabilities [3]. In the UK, the government was until recently conducting pilots of remote electronic voting, as a possible mechanism for increasing turnout [41, 42]. In addition, electronic voting systems, both remote and supervised, are used in a wide variety of contexts, generally without controversy.

This thesis places a novel class of remote voting schemes within a framework for voting systems as a whole. The thesis describes a new class of pollsterless remote voting schemes. A prototype implementation of the scheme is then described and evaluated with respect to the specific requirements of the UK public election context. The results of the evaluation will be used to argue that pollsterless schemes are particularly suited for the UK context.

1.2 Thesis Hypothesis

The hypothesis of this work is as follows. Voting schemes and voting technologies can only be understood with respect to the requirements of the particular voting context at which they are targeted, else the motivation for the properties of a particular scheme is unclear. The choice of voting scheme and implemented voting system is dependent on the requirements of the context in which they are to be employed. Whilst it is not necessary for a scheme to precisely match the requirements of a context, the discrepencies that emerge between requirements and schemes should be explicitly acknowledged. For the UK, a pollsterless remote electronic voting scheme (to be described in this thesis) fulfills many of the requirements of the UK public election context, in particular the Government's desire for more convenient and mobile voting systems.

1.3 Major Contributions

The major contributions of the work are as follows:

- A novel class of remote pollsterless remote electronic voting schemes, mCESG.
- An investigation of the requirements for new voting systems specific to the UK public context.
- A demonstrable implementation of the mCESG scheme as a prototype system to support a range of requirements (and therefore contexts).
- An evaluation of the mCESG class of schemes and the prototype system with respect to the requirements for alternative voting systems in the United Kingdom context.
- A novel evaluation of the user acceptance aspects of the mCESG prototype implementation using focus group observation of video-taped scenarios.
- A survey of the existing research efforts into voting systems, structured as a hierarchical framework.
- A discussion of potential future expansions of the work presented in this thesis, notably the prospect of further adaptations to the basic mCESG scheme and prospects for conducting pilots of the prototype system within a research agenda.

1.4 Organisation of Thesis

This thesis is organised as follows. In Chapter 2, a survey of the various research efforts into voting systems (in both academia and government) is presented. The survey is presented within a hierarchical framework in which the topic of voting systems consists of voting contexts, requirements, schemes and systems. Chapter 3 develops requirements for the United Kingdom's public elections voting context with respect to the framework described in Chapter 2.

Chapter 4 reviews the properties of *pollsterless* remote voting schemes and describes two previously proposed pollsterless schemes. Chapter 5 describes a new pollsterless remote voting scheme, together with a variety of useful properties for the UK voting context. Several adaptations to the basic scheme are described to illustrate the flexibility of the mCESG scheme. The adaptations demonstrate that mCESG is a class of novel voting schemes. Chapter 6 describes several evaluations of the mCESG scheme with respect to UK requirements, including a user acceptance study and a threat analysis.

Chapter 7 describes some further research avenues for the work described in this thesis, including further adaptations to the mCESG scheme to obtain improved robustness of operation and the prospect of conducting further pilots of the scheme presented in Chapter 5 as part of a research agenda. Chapter 8 reviews the original hypothesis of this work described in Section 1.2 in light of the work discussed.

Chapter 2

Voting and Technology

How hard is it to count ballots? Harder than you think. Well, maybe not harder than you all think, but harder than a lot of the electorate thinks.

– Jim Adler

Overview

This chapter introduces the history of the association between technology and voting. A framework is presented for collating the various research efforts into voting systems as a hierarchical model of:

- the voting contexts which describe the circumstances and motivation in which a vote is conducted.
- the requirements and standards which are specified for a voting system to be used in a given context, imposing constraints on the release of information from an election, for example.
- the voting schemes which provide an abstract description of a voting system that will achieve the desired properties specified by a voting context's requirements.

- the collection of participants, technologies, media and processes which are employed to implement a particular scheme as a voting system.

A survey of the research efforts at each of the levels of the framework is then conducted. The survey illustrates the validity of the proposed framework with respect to existing research efforts. The chapter concludes by noting the diversity of voting contexts for which voting systems must be designed and deployed.

2.1 Voting and Automation

The association between technology and vote casting has a long history. The ancient Greeks used coloured pebbles (*ballota*) for decision making in the Athenian parliament, or *Agora*. The practice has been noted as an early attempt to 'automate honesty' in public affairs [13]. Later, the inventor Thomas Edison patented an 'automatic vote recorder' capable of recording and automatically tallying the for/against votes of a congressional motion. However, Edison was unable to sell the invention to Congress, because, as one congressman noted, the device made democracy too quick [36].

The later introduction of electro–mechanical lever machines to US elections (circa 1890) was a result of a desire to eliminate the frauds associated with the practice of *chain voting*, an attack using paper ballots. To initiate the attack, a voter enters a polling station, authenticates their identity to a polling clerk and obtains the ballot papers on which they may record their vote. However instead of voting, the voter leaves the polling station with their ballot paper un–marked, which they give to an agent of a malicious candidate. The agent then marks the ballot paper as desired and gives this to a second voter, who enters the polling station, authenticates and obtains their own ballot paper. The second voter then votes with the pre–marked ballot paper and leaves the polling station with the blank paper, to allow the attack to be 'chained'. Another, more subtle attack, was employed prior to standardised ballot papers being the norm. Political parties in the US provided voters with pre-printed ballot papers with the preferences of the party. The ballot papers were printed

using a small type face for candidate names in order to make customization by the voter difficult. The practice gave rise to the term ‘party ticket’ [73].

Many attacks on paper ballots are not possible on lever machine devices, since there is no separate ballot record for the voter to manipulate – rather a vote is cast by incrementing mechanical counters. Despite preventing chain–voting and party tickets, the lever machine is instead vulnerable to an attack on the vote counting mechanism, a phenomenon common to voting systems that do not retain a separate copy of each voter’s choice (‘ballotless’ technologies). For lever machines, the attack requires access to the internal mechanisms of the device, where the incrementation of counters can be modified such that a proportion of votes for a particular candidate are not counted [91].

Electronic counting machines were introduced in the United States during the 1950’s. Initially, votes were counted using punch card reader machines, a technology that persisted into the 21st century. To make a selection in a particular race a vote uses a stylus to remove small pre-scored ‘chads’ from a card ballot. Electronic counting devices are intended to provide a cross between the efficiency of vote counting of lever machines and the supposed desirability of retaining an individual physical record of each vote cast.

However, the punch card voting systems used in Florida caused controversy in the 2000 Presidential elections due to the combination of a high rejection rate of votes and a close contest between the Republican and Democratic candidates for the electoral college votes available in the state. A significant proportion of votes were rejected by the counting technology because the chads were left partially in place by worn or damaged punching equipment (the infamous ‘hanging, dimpled and pregnant chads’) [20, 127]. The effect was to register a higher than anticipated rate of ‘under votes’ (votes where no choice is recorded for a particular race). It is unclear whether this benefited either candidate, since the attempt to undertake a manual recount (for which there was no provision in law) was halted by the courts [54, 142].

As a result of the 2000 controversy, legislation passed two years later mandated the gradual phasing out of punch card voting systems across the United States [58], although the Direct

Recording Electronic (DRE) Machines which have replaced them have proved to be equally problematic for a range of political activists, election officials and computer scientists [34, 57]. Analysis of the source code for a voting system used in public elections in the United States suggested a range of potential attacks on an election using the system including the ability to modify results or bring voting to a halt [77]. Similarly, the SERVE project which was intended to provide overseas military voters with a remote voting system to replace existing inadequate methods, was cancelled following a critical evaluation of the system [69].

In the United Kingdom and elsewhere in Europe, voting technology has, until very recently, been largely unchanged since the late 19th Century. In the UK, electoral fraud, which had been prevalent for much of the 19th Century, had largely been eliminated by legislative reforms completed in the early 20th Century, notably including harsh penalties for treating (bribing of voters) and the introduction of the secret ballot [106, 112]. Resulting levels of public confidence in the employed voting system combined with relatively high levels of participation in public elections [132] limited the motivation to employ alternative voting systems until relatively recently.

Following successively lower turnouts at elections in 1997, 1999 and 2001, [40, 146] the UK Government began investigating and implementing methods to improve the convenience of voting and reverse the trend [122]. Besides changes to voter registration rules to reflect greater population mobility and the introduction of postal voting on demand, the Government began to conduct research on (and introduced a series of pilots to test) the possibilities for alternative voting channels. These include remote electronic voting channels via telephone, Internet and SMS technologies [42, 113]. The aim of the pilots was to test the extent to which technologies offering greater convenience for vote casting would improve turnout to local elections, to which it had been traditionally low. Whilst the pilots were generally considered to be a success and no substantial evidence of electoral fraud was reported from their use, the discovery of anomalies caused by the widespread use of postal voting at the 2004 local elections suggested that similar difficulties could arise with other remote voting technologies [87]. In addition, the effect on turnout of using the new technologies

was less pronounced than the introduction of postal voting [60, 102] and as a result, the Government has postponed further large scale pilots at least until 2007 [55]. Despite the lack of progress directly on electronic voting systems, the Government is continuing to introduce new technology into the UK's voting system in order to improve convenience and efficiency; legislation has been introduced, for example, to provide a nationwide electronic electoral register, with the required technology already under investigation [37, 70]. Small scale pilots are planned for 2006 to test the use of new technologies and procedures out with pilots of remote electronic voting systems. The pilots will test, for example, the use of online electoral rolls, coupled with the printing of ballot papers on demand [1, 62].

Besides the experimentation with electronic voting technologies for public elections, new schemes and/or systems have been proposed and implemented for a variety of contexts in which voting takes place. Voting schemes have been proposed for: jury voting contexts where it is desirable to publish only whether the result of a vote has reached some criteria, plurality or unanimity for example [61]; parliamentary or committee voting where the association between votes and voters is sometimes published in order to hold the parliamentarians responsible for their decisions [81]; and shareholder voting where voters are allocated different weighting strengths for their votes [67]. Similarly, electronic voting systems have been deployed for a variety of voting contexts out with the scope of binding public elections. In the early 1970s, a telephone voting system was deployed for polling citizen in San Francisco in non-binding referenda [104]. Recently non-government organisations have begun using remote electronic voting to replace postal voting [92]. Organisations such as professional associations, trade unions, political parties and societies use remote electronic voting systems to elect office bearers and pass motions, where the use of a paper ballot and polling station system would be inconvenient for the organisation's members. Consideration has also been made for enabling proxy voting using electronic technologies for shareholder voting contexts [31].

From this published evidence, it is hypothesised that the development of voting technologies is a result of a combination of contexts and motives. The diversity of contexts in which voting systems are to be deployed has consequences for the required properties that

systems must exhibit. When deciding to implement a new voting system, two particular motives may be identified. First, new technologies are proposed as a means of eliminating the vulnerabilities which permit attacks in current technologies. Flaws identified in the existing system inform requirements of the new technology to prevent these abuses. Second, new voting technologies are proposed as a means of improving the accessability of an election and the convenience of participating.

The diversity of contexts in which new voting systems are deployed, coupled with the differing motives for transitioning to different voting systems implies that when the requirements for electronic voting systems are specified the diversity must be accommodated. The next section of this chapter describes a framework to be used throughout this thesis for discussing the contexts, requirements, schemes and systems involved in voting. Using the framework, a survey is then conducted of the research efforts at each of the levels in the framework hierarchy. Given the diversity of the field, the survey necessarily describes topics which are not restricted to computer science. To be able to discuss the design and implementation of voting systems from the perspective of Computer Science, it is necessary to cover those topics from other fields which impact on that process. The chapter concludes by noting that the diversity of voting contexts is reflected in the diversity of requirements approaches, schemes and systems that have been developed to accommodate them.

2.2 Voting Framework

Throughout the literature related to the field of voting systems, relevant terminology is often used interchangeably. Several terms may be used to describe a single concept (voting system or electoral system for example), or alternatively, a single term (vote) may apply to several definitions.

In some cases, this confusion may occur within the same document. In this work, terminology is standardised to refer to the specific concepts described. The advantage of this approach is that terms are disambiguated and that a clearer understanding of the concept

of voting can be portrayed prior to consideration of particular voting technologies as a topic. The terminology may then be organised into a layered framework into which the various research efforts concerning voting systems may be integrated. Figure 2.1 illustrates a framework for organising the terms described below in a structured manner. The goal of the framework is to provide structure for the field of voting systems, illustrating where the various diverse research efforts (from a range of disciplines and backgrounds) may be integrated.

Voting Context. The organisational and/or geographical context in which voting occurs, General elections to the Westminster Parliament in the United Kingdom for example. A voting context gives rise to a set of requirements for the manner in which voting is to be conducted. Such requirements are unique to the context for which they are described, although there may be similarities between sets of requirements for similar contexts. Requirements for elections to the United States House of Representatives should bear some similarities to requirements for United Kingdom elections to the Westminster Parliament, whilst not being identical. Requirements for voting systems may be categorised, for example, in terms of electoral system and usability. Requirements from the voting context are used to generate lower level requirements for technologies, for example, the strength of encryption for communication of tallies on unsecured channels.

Electoral System. Expresses the rules for voting in a particular voting context. An electoral system may be modelled as consisting of a set of *voting round types*, rules for transitioning between round types and rules for deciding whether to terminate the election. For each voting round type, constraints on how votes may be expressed and the algorithm for aggregating votes to produce a tally for that round must be described. Rules for transitioning between voting round types and termination are dependent on the tally of votes cast in that round and the independent set of inputs for that round.

Franchise. The description of eligibility to vote with a type of vote in a voting round of an

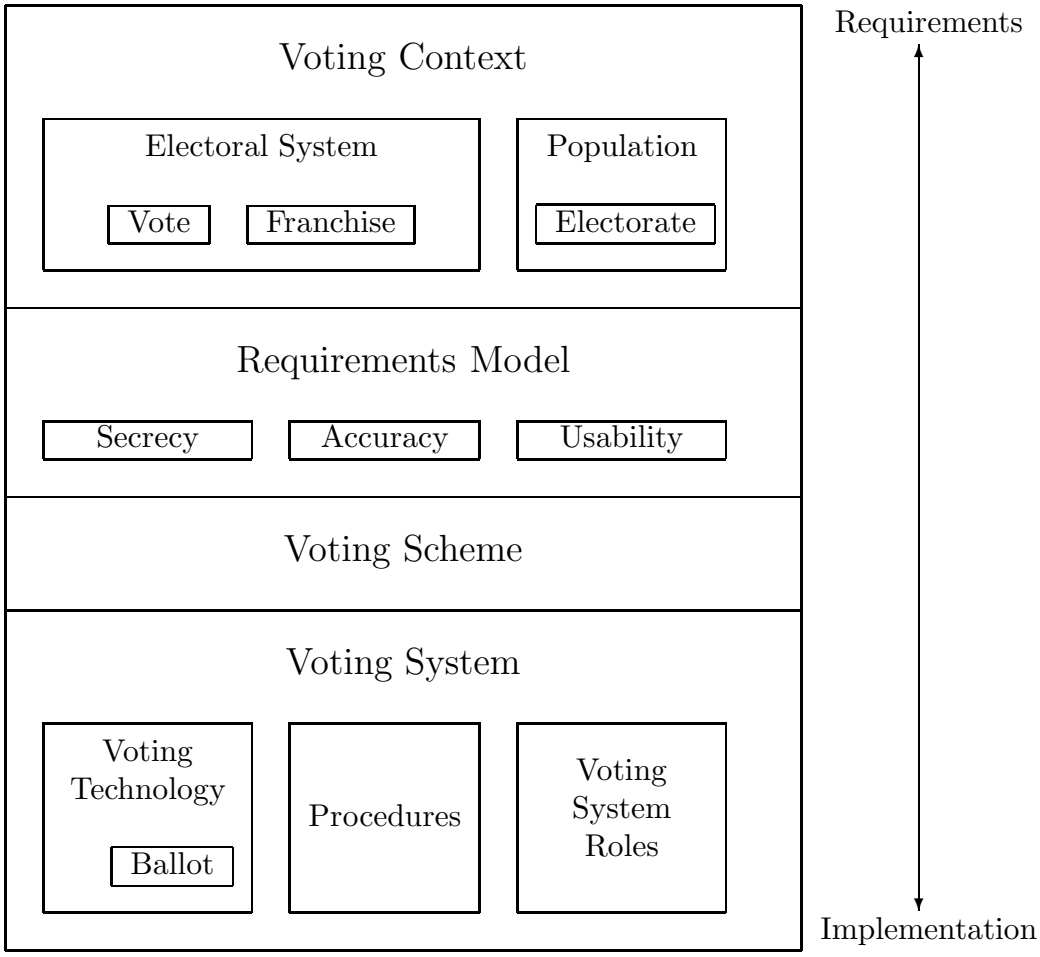


Figure 2.1: Illustration of levels of abstaction of the framework for voting systems. At the highest level, a voting context exhibits the properties that must be captured by a requirements model. The voting context encapsulates the terms of eligibility for voters (the franchise) and the electoral system rules by which vote casting is conducted. The electoral system specifies the constraints on how a vote may be expressed and counted. The role of a requirements model is to capture this context such that they may be fulfilled by the *voting scheme*. The *voting system* is an implementation of an envisaged scheme which combines both voting technology and manual processes outwith the technology. As such, roles other than that of voter occur at the system level of the terminology, since aspects of a scheme may be either automated or conducted by human operators, depending on the voting system implementation.

election. Members of a population which satisfy a franchise are considered eligible to vote.

Proposal. The manner in which a decision to be made is presented to a voter, including constraints on how the voter may express a choice (through a vote).

Vote The abstract expression of a voter's choice within the constraints expressed by an associated *electoral system*.

Voter. An entity (typically human) eligible to vote in at least one round of the electoral system. Franchises are used to distinguish between different voting eligibilities.

Tally. The aggregate of votes cast in a round of voting according to rules specified by the electoral system.

Requirements Model The methodology for capture of requirements for a voting context.

Voting Scheme. The abstract description of the technology, agents and procedures designed to satisfy the requirements of a particular voting context.

Voting System. The collection of technologies and procedures implemented to satisfy the conditions and requirements of a *voting context*. A brief example of a voting system is a Constituency Returning Officer implementing the terms of the Representation of the People Act 1983 (as amended) in order to conduct a parliamentary election using paper ballots marked in a polling station on a single day and placed in a box which is sealed until all votes are counted after the close of poll.

Voting Technology. An implementation of the technological aspects of a voting scheme. Voting technologies without associated voting schemes are commonly hard to evaluate with respect to the requirements of the underlying voting context.

Ballot. The implementation of a proposal and/or vote as a distinct record within the voting system. For example, paper ballots as printed in accordance with UK election law is an example ballot. Note that not all voting schemes explicitly implement a ballot, paper or otherwise. Such technologies are denoted *ballotless*.

A further set of definitions related to the framework which provide descriptions for the *execution* of a voting system are as follows:

Election. An single execution of the procedures and technologies implemented in a voting context. Given that a voting system must accommodate all the circumstances that occur, an election represents an execution path through an electoral system and also through a voting system.

Voting. The collective act of casting votes to obtain some decision, electing officials from a larger set of candidates or deciding whether to accept or reject a motion before a parliament or committee for example.

A significant departure from some other works on voting systems is that a description of the term *democratic* is excluded from the definitions employed in this work, although more unusually, a definition is provided of the related term *franchise*. The choice is deliberate since the understanding of the term democratic is dependent on the voting context in which it is used. Defining democracy as a requirement for a voting system becomes problematic for a single definition as:

- Democratic may refer to the results obtainable from a given electoral system. A common political argument, for example, is that "proportional electoral systems" are more democratic with respect to participating groupings of candidates (political parties), whilst the converse argument is that non proportional electoral systems are more democratic to unorganised candidates [115].
- A voting context may be specifically undemocratic, for example, individual shareholders in a company receive votes weighted by the proportion of total shares in the company they possess. The framework discussed here is designed to capture the broad range of contexts in which voting takes place.
- Definitions of democracy commonly refer to "all eligible citizens", for public elections, which might be generalised for all voting contexts to "all those eligible". However, this then limits the definition of democracy to that of equality of those included

in the eligibility criteria (franchise). The satisfaction of a 'democracy requirement' then, is dependent on what one considers to be reasonable criteria for franchise.

- Where definitions refer to "equal access to the voting system", necessary trade–offs resulting from the disparate circumstances of voters are either ignored, or the definition of democracy through equal access is diluted. For example, a common technique for public election is to require that most voters attend polling stations to cast a vote on a paper ballot with those voters unable to do so able to complete their paper ballot at home and send it via a postal service. Whilst this approach ensures that all voters (or at least all voters able to complete paper ballots) are able to participate in the voting, those voters who complete their ballots at home necessarily experience a reduced level of voting privacy compared with voting in a supervised polling station.

Therefore, in this work, the term "democratic" is defined indirectly in terms of the requirements of a given voting context, rather than attempting to adopt a uniform definition to be applied to all contexts.

2.3 Voting Contexts

In this section, the classification of voting contexts is discussed in terms of the properties that a voting scheme is required to exhibit, together with a discussion of the characteristics of common classes of voting contexts.

2.3.1 Classification of Voting Contexts

In order to specify the requirements for an electronic voting scheme and the voting system which implements it, it is necessary to consider the voting context in which it is to be deployed. Here, a classification is presented of voting contexts in terms of the requirements that voting schemes and the voting systems which implement them must fulfill.

2.3.1.1 Electoral System

The collection of rules under which elections are conducted are referred to as electoral systems [103]. The classification and/or characterisation of electoral systems is considered a topic within the domain of political science, since the design of such systems have significant consequences for the organisations which operate them [115]. The classification of electoral systems in political science is therefore concerned with the consequences of an electoral system's rules. A typical classification (Norris or Reynolds for example [103, 115]) begins with a high level description of a system as being either "proportional", "combined" or "majoritarian", in reference to the system's likelihood of distributing representation proportionately amongst organisations of candidates [103]. Further subclassifications are also dependent on the degree of proportionality of a system, with Norris decomposing Majoritarian electoral systems into those requiring a majority of votes for a winning candidate (Alternative Vote, for example) and those requiring only a plurality (Simple Plurality, or First Past The Post). The approach adopted by political science, then, is to categorise electoral systems by the emergent properties of the results from the elections which are run under them.

However, an alternative approach to the classification of electoral systems has been to identify discrete characteristics for comparison [72]. Adapting this approach allows an electoral system to be described as:

- A series of voting round types and rules for transition between rounds of voting [47]. Whilst many electoral systems incorporate only a single round of voting leading to a result, other electoral systems (French Parliamentary and Presidential elections, for example) incorporate two rounds of voting in the circumstances where a candidate does not win a simple majority of first round votes. Farquharson describes electoral systems as consisting of multiple rounds of decision making [47].

- A categorisation of eligible voters, typically referred to as the franchise. The franchise for UK public elections, for example, includes most British and Common-

wealth citizens over the age of 18 resident in the country; those excluded include, 'peers of the realm' and 'lunatics' [121]. The franchise may also incorporate geographical qualifications, with a voter required to be resident within the boundaries of a specified district.

- A description of the legal expression of a voter's choice, which shall be termed a *proposal* to a voter throughout this work in an attempt to avoid ambiguity. A vote cast under Single Transferable Vote (STV), for example, requires voters to rank options in order of preference, whilst referenda permit a vote to consist only of an accept (yes) or reject (no) of the statement under question.

- The algorithm by which votes are aggregated to produce a *tally*. Whilst simple electoral systems such as Simple Plurality total up votes for each candidate, more complex electoral systems may perform vote re-distribution over a series of tallying iterations until a sufficient number of winning candidates have been identified. The tallying algorithm may also need to take account of results from other elections. A mixed member system, as used to elect representatives to the Scottish Parliament, weights the number of list members elected according to the number of constituency members elected for a given party [125].

Whilst there is considerable diversity in the electoral systems used across different voting contexts, it is possible to identify commonality to the extent that *classes* of electoral systems may be identified. Such classes of electoral system are described below and sample votes cast on paper ballots are presented in Figure 2.2.

Single Member Simple Plurality (SMSP) More commonly known by the analogy to racing, First Past The Post (FPTP). In a SMSP election, voting occurs in a single round. Voters express their preference for a single candidate from any number of options presented. The candidate with the most votes is elected.

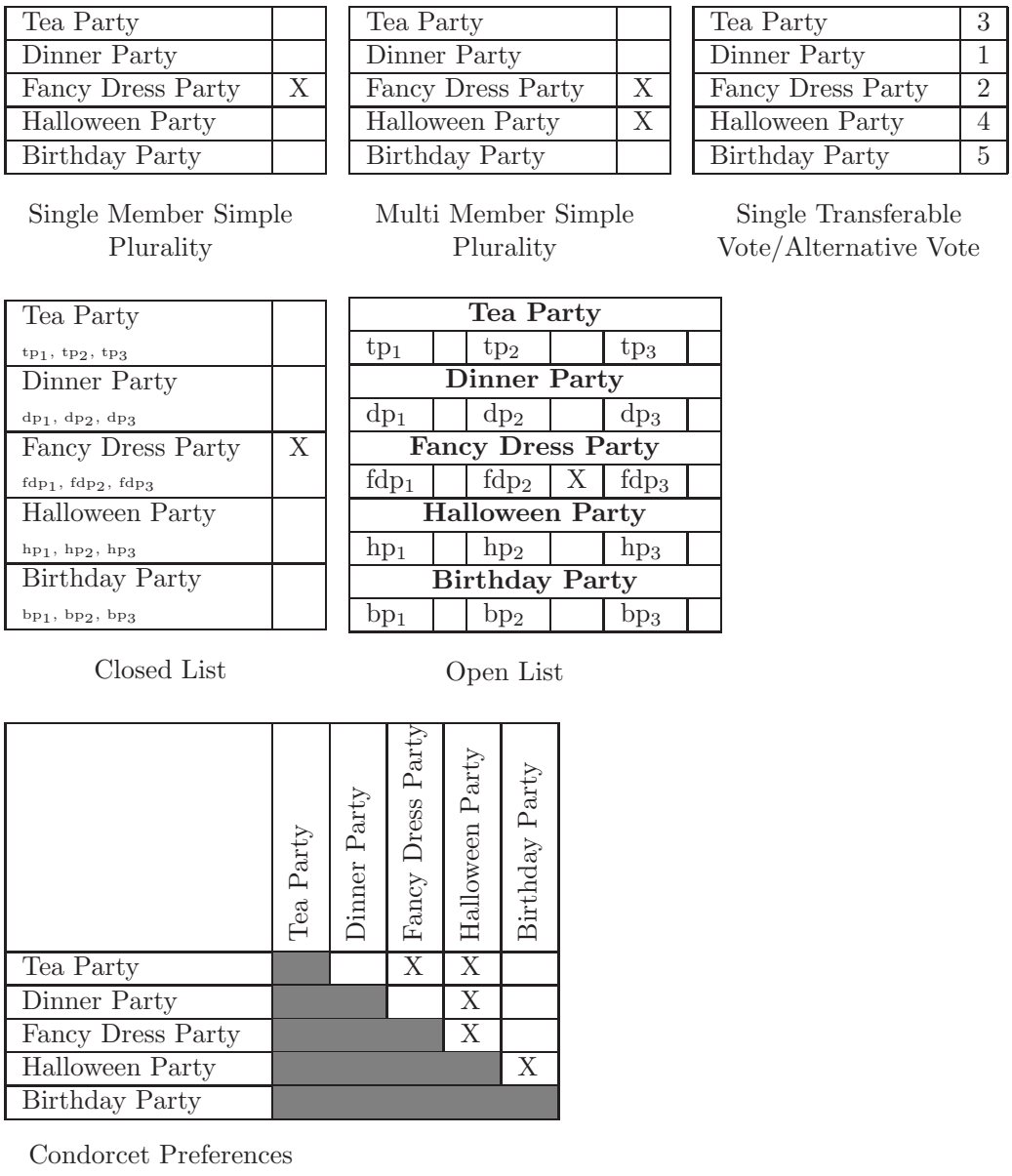


Figure 2.2: Ballot paper representations of votes for sample electoral systems. Simple Plurality votes are expressed as choices for one or more options, each choice having equal value. An ordinal vote (used for Single Transferable and Alternative Vote electoral systems) is expressed as a ranking of one or more options. A Closed List vote is expressed as a choice for a list of pre-ordered options. An Open List vote is expressed as a choice for both a list and a particular option within that list (strictly, the options are a set which are arranged as a list during tallying). A Condorcet Preferences vote is expressed as a comparison between all pairs of options.

Multi Member Simple Plurality (MMSP) Voters may choose as many options as there are vacancies. Tallying is the same as for SMSP systems. When voters are only provided with a single vote, the system is re-named Single Non-Transferable Vote. Some instances of MMSP mandate that a voter must not cast more than one vote for the same option.

Closed List Votes are represented by a choice for a list of candidates from a set of lists. The number of candidates elected from a list depends on the number of votes received by the list and the particular algorithm used for tallying. In general for each round of tallying, the option at the top of the list with the most number of votes is selected as a winner and removed from that list. The tally of votes for the winning list is then reduced by some amount. For example, the d'Hondt Closed List algorithm divides a list's votes by the number of options currently chosen, plus one for each round of tallying.

Open List As for closed list systems, options are organised into sets. However votes are cast for individual options rather than the set of options. Sets of options are ordered during tallying into lists by the number of votes for each option. Options are then selected from lists in the same manner as the closed lists. For public elections, open list electoral systems permit voters to choose a candidate within a political party's list, as well as voting for the candidate.

Single Transferable Vote (STV) Votes are represented by an ordering of options by preference. Winning options are calculated in a series of tallying rounds, in which a winning option must obtain more than a specified *quota* of votes. The calculation of the quota varies, although the *Droop* calculation is commonly adopted in which the quota is calculated as the total number of votes divided by the number of vacancies+1:

$$Q = \frac{votes}{vacancies + 1}$$

An option in a four vacancy STV election, for example, requires 20% of the votes cast in order to be elected. In order to fill all vacancies during tallying, votes are distributed during

successive rounds of tallying. If after a round of tallying, no option has more votes than the calculated quota, the least favoured option (the option with the current least number of votes) is eliminated and each of its votes is distributed to the next preference on the vote. Conversely, if an option receives more than the necessary quota of votes, a surplus proportion of the votes is distributed to other options. This process occurs repeatedly until all vacancies have been occupied. Where only one option is to be elected, STV is the same as for the Alternative Vote system, since no distribution of surplus votes occurs, as the quota is 50% of votes cast.

STV is used for public elections in the Republic of Ireland.

Non-Instant Run-Off Votes are cast as for SMSP elections, although a winning candidate is required to obtain a majority of votes cast (more than half). Voting thus proceeds in rounds, with one or more least favoured options eliminated after each round of voting until a candidate receives half of all votes cast in a round. Non-instant Run-Off is used for French Presidential and Parliamentary Elections.

Condorcet Preference Voting Votes in Condorcet schemes represent all possible comparisons between options, with an X in Figure 2.2 indicating that the option in that row is preferred when compared to the option in that column. Winners in Condorcet elections are calculated by summing the number of comparisons that an option wins. Condorcet schemes may result in ambiguities that are non-trivial to resolve if there is no clear *Condorcet winner*, or preferred option.

The description of an electoral system above discusses how information flows during the execution of an election. However, further properties of a voting context must also be specified with respect to the core electoral system. In this approach then, the same electoral system may be employed in two different contexts for different purposes, yielding two different decision making processes as a result. For example, Single Transferable Vote might be employed to select five successful grant proposals from twenty submitted to a

research council, where the votes of the decision making committee are published. Conversely, the same electoral system might be used to select parliamentary representatives for a constituency, but in this case the individual choices of voters are not published – the same electoral system is employed with two different sets of secrecy requirements. The following sections discuss further properties of voting contexts which are not part of an electoral system, but are specified with respect to one.

Electoral Systems used in Specific Voting Contexts For specific instances of electoral systems, substantial variation from the general classes described above may be identified. For example, variations of the STV system may use different mechanisms to re-distribute surplus votes of different candidates. Surplus votes for re-distribution may be selected randomly, or all votes of a winning option may be re-distributed with a reduced value (which can be calculated using a variety of functions), or indeed a hybrid of both options may be used. The above examples provide only common classes of electoral systems, since providing an exhaustive survey is not practical within the confines of this work.

2.3.1.2 Secrecy, Privacy and Anonymity

Although not mandatory for vote casting itself, many voting contexts impose restrictions on the communication of information associated with voting. These restrictions are categorised here as *secrecy requirements*, referring to stipulations that particular items of information may not be communicated between participants during some period of time (possibly unlimited). Such requirements are enforced via a variety of mechanisms (technological, procedural or legal) depending on the voting context and deployed voting system.

Requirements for secrecy of information processed by an electoral system are most commonly associated with public election voting contexts. Many proposals for voting schemes incorporate a requirement in natural language referring to *voting privacy* as the inability to associate a particular vote with a voter. Such requirements are derived from the need to protect voters from undue influence on their choice, from intimidation or bribery by

competing candidates, for example O'Leary [106]. Typical of such definitions is:

> "Nobody should be able to link a voter's identity to his vote, after the latter has been cast." [53, pp 104]

This definition is problematic for several reasons. As Kremer notes, any scheme designed to fulfill this requirement will fail in the circumstances where a tally of results is published and the results are unanimous [78], since the result eliminates uncertainty as to any voter's choice. Whilst for large electorates, the likelihood of such circumstances arising is small, certain contexts do increase the possibility of secrecy violations. For a practical example, consider the context of public elections in the United States where a large number of elections are often voted on together (President, US Senator, US Congressman, State Senator etc). A common practice is for each polling place to post a local tally of results, sometimes for each Direct Recording Electronic (DRE) machine used to collect votes. For polling places with a small electorate (commonly in rural districts), there is a substantial probability that all voters will choose the same option, violating individual secrecy.

Several approaches have been advocated to accommodate this possibility. Several authors suggest that voter privacy requirements should be weakened by reference to a *system indistinguishability* property, that is, an external observer should not be able to distinguish between two executions of a voting system in which the votes of two voters have been switched, for example [78]. A system can thus fulfill this requirement even if results are published, despite voters being in unanimity. This approach therefore advocates weakening formal definitions of privacy requirements for voting systems in the context where the weaker definition is still acceptable.

Others have argued that voting schemes and their implementations should be designed to provide stronger properties in which a unanimous result does not reveal the association between a voter and a vote. One approach is for schemes to incorporate *coercion resistance* which prevents an external observer determining whether an eligible voter participated (through vote casting) in a particular election [74]. This approach is related to

the *voter anonymity* - the identities of participating voters is not externally determinable. Mercuri notes the Common Criteria definition of *anonymity*:

> "ensure that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity." [91, 101]

Similarly, anonymity is a commonly adopted requirement for voting schemes that employ anonymous channels, for example Michels and Horst:

> "*Privacy:* The votes are casted [*sic*] anonymously." [95]

However, adopting anonymity to protect voting privacy fails when voting is compulsory (in Australian public elections, for example), since all voters are assumed to participate in all elections.

A further alternative is to restrict the amount of information published regarding the tally of votes. In the example of US public elections described above, a crude approach would be to only report the total tally of results, rather than reporting by polling place and machine. An external observer would require unanimity across a far larger range of voters in order to violate anonymity. More sophisticated voting schemes do not report the tally at all, instead, only the necessary information about the tally is published. For, referenda for example, it is only necessary to publish whether the total number of 'yes' votes is greater than some threshold in order to reach a decision. The absolute proportions of the two tallies ('yes' and 'no') are less important, although they may have some *political* value. Candidates in successive elections may wish to use sequential results to demonstrate changing opinions within an electorate, for example. Voting schemes which implement this approach must produce proofs regarding assertions about the tally of votes without revealing the values of the tally themselves [61]. A voting scheme that does not produce a tally of results may also be unacceptable for decision making purposes, for example, where the relative tally of votes is of significance (the Single Transferable Vote electoral systems, for example).

Further complexities arise in terms of the required protection that must be assigned to voting privacy. Whilst international agreements (such as the European Convention on Human Rights) specify that voter privacy is an absolute, the United Kingdom employs a voting system that provides election authorities with the ability to associate votes with voters. Arguments have been made that the practice has limited value as an auditing tool and should cease [68, App. 3]. In addition, some have suggested the practice is contrary to international law [111]. Article Three of the First Protocol of the European Convention on Human Rights, for example:

> "The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature." [17, Prot 1. Art. 3]

However, there has been no indication from the UK government that a change in procedure is imminent. Particular circumstances therefore must be taken into account when designing voting schemes or implementing existing schemes with weakened properties.

The discussion thus far has considered the difficulty of establishing a uniform definition of voting privacy during the conduct of public elections. However, stipulations regarding the communication of information processed by an electoral system occur beyond this narrow context. For example, in some contexts, voting privacy may be explicity excluded, for parliamentary or committee voting contexts for example, where voters are considered accountable to those they represent or act on behalf of. Similarly, a new phenomenon in online opinion polling is to publish an on-going tally of votes as they are cast, although the association between voters and votes remains secret. Such techniques may be viewed as a mechanism for encouraging participation (if an opposing opinion is doing well), or alternatively to deter participation where the will of the majority appears overwhelming. Alternatively, secrecy may be more restrictive than is normally associated with public elections, in the case of jury voting already described for example. In the examples cited, the

specification of secrecy requirements is concerned with individual voters, their votes and the final published tally.

The preceding section has discussed the complexity of specifying requirements for secrecy for voting contexts. To summarise, a general approach must identify the *target information* of the requirement (voter, vote, tally etc), the participant(s) who must not receive the information (from an electoral system perspective) and temporal constraints (the period of time the information must be kept secret).

2.3.1.3 Accuracy, Verifiablity and Dependability

A common requirement of elections conducted in most voting contexts is that the final published tally is accurate with respect to the votes cast by individual voters and the algorithm specified by the electoral system for producing a tally. Schneier has argued that requirements must extend to the voters themselves, that is, accuracy should refer to a tally being accurate with respect to the vote a voter *intended* to cast [130]. Such a definition considers (whether accidently or intentional) misleading user interface design to be an attack on the accuracy of an election.

For certain voting contexts, the demand for an accurate tally is complicated by restrictive secrecy requirements as discussed in Section 2.3.1. For example, an ordinary voter participating in public elections in the United Kingdom is able only to observe the act of vote casting (marking a paper ballot and placing it in an opaque box). The voter is not able to observe their or other voter's votes being transported and then tallied at a count. Indeed, electoral rules prohibit voters remaining in the polling place once they have cast their vote unless they have been provided with passes because they are part of a candidate's polling day team [121, Sch 1. R. 37]. Instead, voters are required to accept that a combination of factors will ensure that the tally of votes is accurate. Measures include trusting the polling place clerks who are the custodians of ballot papers prior to a count and the activism of opposing candidates at the vote count, who will each monitor the counting of their own votes in order to maximise their advantage.

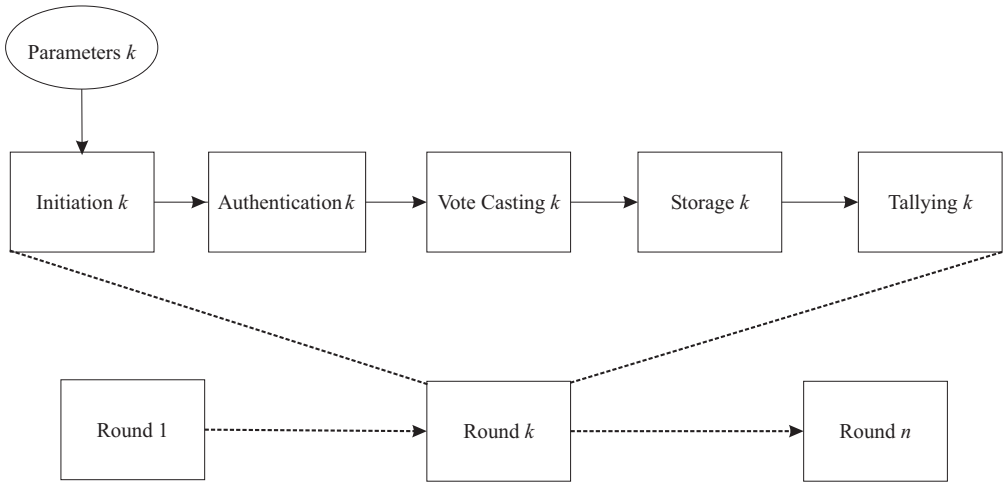


Figure 2.3: The problem of ensuring accuracy of an election result. An attacker is presented with several points at which to perform an attack. The feasibility of attack depends on the specification of secrecy requirements discussed in Section 2.3.1.

The conflict in public elections thus illustrates that the accuracy of a tally may be dependent on an observer's perspective and access to other information during the execution of a vote. The assessment of accuracy of the tally then becomes dependent on the accuracy of other information provided to an observer, which may have been established as accurate, or alternatively the accuracy must be taken on trust.

Ensuring the accuracy of an election is therefore an end-to-end process, as noted by Schneier [130]. Figure 2.3 illustrates a generic electoral system in which voting proceeds in a series of rounds. Each round consists of vote casting, storage, collection and tallying. Transitions occur between each round of voting depending on both tallies from the previous round and the parameters specified for the election.

An attacker may choose to violate the accuracy of the election at any one of the points (or multiple points) in the election process:

During initiation. Attacks on a voting system during initiation can violate the accuracy of an election before it is executed. For example, an attack on the registration of voters

may prevent some otherwise eligible voters from participating. Several authors have documented the use of literacy criteria for participating in public elections in the United States as a mechanism for disenfranchising poorer voters [52, 54, 126].

During voter authentication. The accuracy of an election is violated if non-eligible voters are permitted to participate, since the result of the election will no longer reflect the intention of legitimate voters.

At the voting interface. According to the definition of accuracy proposed by Schneier [130], a user interface which obstructs accurate vote casting constitutes an attack on the accuracy of an election. During the 2000 US General election, the layout of punch cards ballots in a 'butterfly' was criticised because voters mis-construed which hole to punch for a particular candidate [2, 39]. Other deliberate attacks have been noted with voting interfaces which use labelled buttons to indicate voting options. To attack these systems, labels are switched in precincts where voters are thought to have a preference for an opposing candidate, such that that candidate's votes are unintentionally cast for an opponent.

During vote casting. The vote casting process records the vote cast by a voter at the interface. Thus, vote casting attacks are distinguished from interface attacks by accurately obtaining the voter's choice, but altering the choice prior to storage.

During storage and communication. Attacks on a collection of votes include altering cast votes, adding extra votes (either for non-existent voters, non-participating voters or by adding extra votes not associable with particular voters), or removing votes (either through 'intelligently' removing votes identified for an opposing candidate, or 'blindly' removing all votes in a collection suspected of being biased towards a particular candidate).

During vote tallying. Whilst simple tallying algorithms are possible to verify if the collection of votes cast are available for inspection, the implementation of more complex algorithm may introduce subtle errors which are difficult to detect in results. For example, an inspection of a vendor's implementation of the STV electoral system's

tallying algorithm revealed a minor defect in the allocation of votes once candidates had been elected [134]. Whilst such a minor flaw would not affect the determination of winners, the case illustrates that correct tallying of votes is an element of election accuracy. Alternatively, if the collection of votes for tallying are not available for inspection, then the accuracy of the resulting tally becomes more difficult to ascertain. Pieters has attempted to differentiate between voting schemes where collections of votes are published to enable open tallying and those where a tally is derived from an encrypted collection of votes [110]. Publishing the collection of votes for inspection by external observers may not be possible, for example, in circumstances where the expression of choice represented by a vote may be used to identify a vote in a tally. This possibility was again identified in the context of the STV electoral system, when the vendor proposed electronically publishing the list of votes cast to demonstrate the correctness of their tallying algorithm. An STV vote lists candidates in order of preference. Commentators noted that lower-order preferences (which are unlikely to affect the result of an election) may be configured to produce a unique *preference signature* such that the vote may be identified in the published list and an attacker can ensure a voter has organised their higher order preferences 'correctly' [134]. Figure 2.4 illustrates this potential attack on secrecy.

The result of attacking the accuracy of one or more processes within the accuracy model is dependent both on the voting context and the nature and goal of the attack. Attacks which undetectably alter results of elections are considered the most problematic since by their definition, they are not expected to be identified or if identified, they may not be correctable. Mechanisms for preventing such attacks include quality control techniques on the technologies and processes employed in a voting system; and the use of voting schemes which provide external verifiability of the correctness of an election result.

Denial of Service (DoS) attacks on voting systems (which prevent a decision being made) are considered a low level threat since the consequence is only that the election must be re-run. Further, disruptive attacks are by their nature detectable (otherwise the disruption would not lead to a cancellation of the existing election and initiation of a new process).

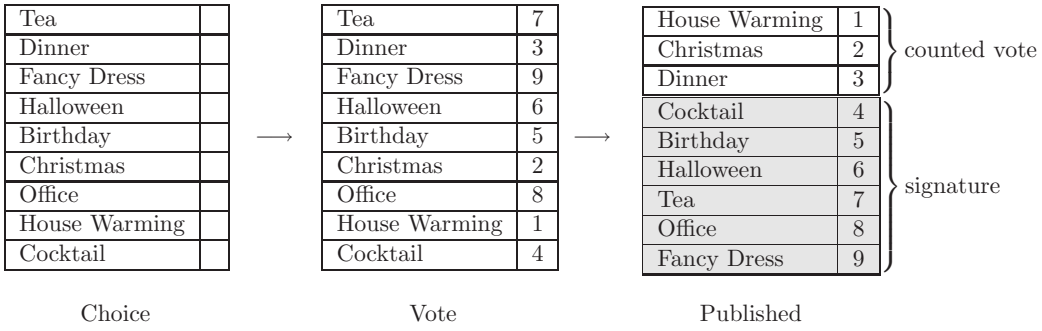


Figure 2.4: The vote signature attack on ordinal electoral systems, where all votes are published as a means of verifying the accuracy of the tallying algorithm. In the illustration, an attacker from the House Warming Party instructs the voter on the order of the party's candidates. Then, the voter is assigned a unique permutation of preferences 4–9, which are not used to elect candidates, but identify the vote when published, violating the vote's secrecy. In this example, an attacker would be able to assign signatures to 720 voters.

However, as noted by Mercuri, many elections are time sensitive [91]. The issues which influence voter choices at one point in time may not be replicated later. A further problem with successful DoS is that the confidence of an electorate in a voting system (and the resulting choice made) may be reduced when an attack is reported. Election systems that cannot resist DoS may be suspected of being vulnerable to more subtle undetected attacks on the tally itself. It may be noted that an attack on the result of an election that is detected will degenerate into a DoS attack if the voting system cannot recover from the damage caused.

The ability for a voting system to recover from an attack rather than cause the relevant election to be re-run is dependent on the choices made for a particular voting context. For example, the UK voting system for public elections is designed with the ability to identify and invalidate illegally cast votes (under court order) whilst the possible violation of voter privacy makes this practice illegal in the Republic of Ireland [89]. The properties of voting systems need to be designed to reflect the priorities of the contexts in which they are deployed.

The ability to target individual processes during an election is dependent on the requirements for secrecy for the electoral context, discussed in Section 2.3.1. Providing for a

voting system which ensures accuracy at all steps in the voting process is simplified if secrecy is not required. However, since a variety of voting contexts incorporate some form of secrecy requirement with respect to the votes cast in an election, ensuring accuracy at the successive processes described above is non-trivial. For a particular voting context, it is necessary to identify the steps in the voting process for which ensuring accuracy is non-trivial due to requirements specified for secrecy. Generally, the more restrictive the requirements for secrecy, the greater the difficulty is for a voting scheme and implementing voting system to ensure secrecy.

Voting systems may well be implemented on the understanding that certain components are trusted in order to fulfill requirements that are otherwise in conflict. Such schemes specify the components that are considered trusted, or else alternatively demonstrate how trust may be distributed across multiple components under an assumption that a certain proportion will not collaborate to violate the accuracy, or secrecy, of an election. Alternatively, where no satisfactory implementation of a set of secrecy and accuracy requirements can be obtained it may be necessary to relax the constraints so that an election may be conducted at all. Of course, such an approach does not preclude the later implementation of a system satisfying the stricter requirements.

2.3.1.4 Usability and Acceptability

For a voting system to successfully implement the requirements of a voting context, the system must be usable by those enfranchised by the electoral system. In the field of Human Computer Interaction (HCI), usability refers to the ability of a user to interact with a system in order to achieve desired goals.

ISO 9241-11 refers to usability as:

> "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

noting that not only is a usable system designed to allow a user to achieve desired goals (effectiveness and efficiency), but also that the user must be *satisfied* with the result. The usability of a system is not just the extent to which tasks are completed efficiently and quickly, but also the degree of ease and satisfaction with which a user interacts with that system. A particular factor relevant to voting systems for judging usability is the extent to which a user would consider using it again to repeat a given task. Maurer notes that systems which suffer from poor usability will be by-passed by users, employing alternative methodologies instead to complete their task [86]. In this sense, usability also incorporates the *acceptability* of a system to users - the likelihood that they will accept its use to accomplish a particular task rather than a parallel and potentially less efficient system.

The usability requirements of a voting context, then, are dependent on the capabilities of voters specified by the relevant electoral system's franchise. Given that a separate franchise may be specified for each round type in an electoral system, the capabilities of voters may vary across multiple rounds and within the rounds of voting themselves.

Factors which influence usability constraints for a voting system (with respect to voters) include:

Electoral complexity. The variety of choice which the electoral system presents to a voter. Electoral complexity is a function of the number of configurations of legal votes that may be cast (for a single vote); the total number of votes that may be cast in a round; the availability of "write-in" options where a voter may provide additional choices on a vote other than those specified at initiation; the number of discrete elections (races) that the voter is offered for decision at one time; and the number of discrete rounds

the voter may participate in. A voting system may be required to mask complexity in a voting system, if too much choice is considered a deterrent to participation. For example, voting systems employed for public elections in the United States provide a 'party ticket' option for voters who wish to vote for a single party's selection of candidates for multiple elections, rather than individually selecting that party's candidates on the system.

Literacy. A voting context may require a voting system to accommodate varying levels of literacy within the population of voters.

Physical capabilities of voters. A voting context may require a voting system to accommodate physical disabilities of voters. The precise disabilities accommodated and the manner in which the accommodation is made is context dependent. For example, the provision of DRE machines in polling places for public elections which support blind voters are mandated by recent federal legislation in the United States [58], whilst voters in the United Kingdom may either receive assistance or use a tactile template to mark a paper ballot [121].

Cost of participation. Norris notes (in a theoretical framework of participation) that the cost of participation in an election is a contributory factor for a voter deciding whether to participate in an election [102, 103]. High participation costs may result if a voter is required to purchase particular technology or travel to a distant location in order to vote. High costs of participation deter voter participation and thus have a detrimental effect on the usability of a voting system. A voting context may set limits on the acceptable costs of participation in an election.

Cost of implementation An organisation must usually commit at least some resources to conducting an election. One aspect of acceptability requirements are the costs an organisation is willing to accept in order to implement a voting system to fulfill the requirements of a particular context. In circumstances where all other requirements are deemed fulfillable, if the resultant costs are beyond the means of an organisation, other requirements (in terms of electoral system , secrecy, accuracy or usability) may

need to be relaxed in order to make the cost of conducting an election affordable to an organisation.

A voting system that successfully implements secrecy and accuracy constraints, but as a result is unusable by the participating voters is not at all useful as a decision making tool. As for the compromise between secrecy and accuracy discussed in Section 2.3.1, fundamental conflicts between accuracy, secrecy and usability may need to be resolved in favour of usability if a decision is to be made at all using the voting system and an implementation fulfilling all requirements is not known. For example, the use of remote voting technologies (postal or remote electronic voting, for example) may be necessary for geographically widely distributed populations. The use of supervised polling stations is impractical in such contexts, however desirable it is to employ them in order to achieve desirable secrecy requirements.

2.3.2 Instances of Voting Contexts

The previous section presented a framework for considering the variety of contexts in which voting takes place. This section describes a selection of voting context instances in order to illustrate the diversity of voting system requirements. It is not argued that the voting context types described here faithfully represent a single real world instance of a voting context. Rather the voting context types provide descriptions of classes of real world voting contexts.

The first voting context discusses characteristics of public elections and referenda. The second example discusses elections conducted in legislative and committee contexts, together with an illustrative case of system failure with respect to requirements. The third example discusses the restrictive requirements for secrecy in jury voting and the consequential difficulties for ensuring the accuracy of a resulting decision. The fourth example discusses shareholder voting, in which a voter may cast multiple votes (potentially for different candidates) and voters may be allocated different numbers of votes.

2.3.2.1 Public Elections

Public elections are perhaps the most commonly perceived type of voting context. Public elections are a feature of societies as a means of choosing legislators, executives and other public officials. Public voting contexts may also decide issues of public policy such as in *referenda* considered too significant to be decided by a legislator alone.

A diverse range of electoral systems are employed for public elections, although typically all enfranchised members of a population have equal voting capabilities.

Typically, public election voting contexts require that the association between voters and individual votes is kept secret. Secrecy requirements may also state that information regarding whether a voter participated in an election or not be kept secret.

In common with other voting contexts, requirements for accuracy are common for public elections. The nature of public elections makes demands on voting systems to ensure accuracy, including:

Authentication The large, diverse population of voters eligible to participate in public elections makes authentication of voters harder when compared to the small populations who typically participate in parliamentary and jury voting contexts. Authentication of voters typically requires some pre-constructed infrastructure used for authentication in other contexts. However, overly onerous authentication requirements may conflict with usability requirements by preventing voters from participating. The conflict between stronger authentication of voters and accessibility of voting systems is a controversial issue in the United States, where voter authentication has been perceived as a mechanism for limiting participation [91], whilst weak authentication has been shown to permit *personation* [52].

Voter interface The large electorate typically requires voting systems to be able to accurately record voter intentions from voters with a diverse range of physical and mental capabilities. Alternative approaches to this include providing voting systems with

flexible voting interfaces [2], or alternatively providing multiple parallel voting systems for a single context, with the intention that every voter is able to use at least one interface [42].

Vote storage, collection and tallying Public elections require that voting systems ensure (or at least provide re-assurance) that a tally is accurate with respect to votes cast, despite the requirement that the association between a voter and a vote is secret.

2.3.2.2 Legislative or Committee Motions

Parliamentary and committee voting share many common characteristics. Parliaments consist of a set of legislators, representing a larger body of people. A measure to be voted on will be presented before the parliament and may be discussed amongst the legislators. Once the discussions are completed a vote is conducted, in which all legislators are usually equal participants (other than a chairperson). Votes are most often conducted for or against the wording of a particular motion and as such a SMSP electoral system is employed.

Both the tally of votes and the association between votes and voters are published so that a decision may be acted upon and also so that the legislator is accountable to the larger body of represented people.

Since the association between votes and voters are not secret in legislative voting, ensuring the accuracy of a tally with respect to the intention of a voter is often considered trivial. This assumption is dependent on a voter being able to determine that their vote has been wrongly recorded prior to a decision being made on the basis of the election result. A counter example to the assumption that ensuring accuracy in "open" voting contexts is simplified compared to public elections is provided by the electronic voting system employed in the Knesset, the Israeli Parliament. Rules of voting require a legislator to be present in the chamber in order to cast a vote on a voting terminal. An incident arose in 2003 [99], where it emerged that one legislator was casting votes on behalf of another in contradiction of the rules. The accuracy of the tally of votes was thus violated at the authentication stage

of voting, since a voter is only considered eligible if they are present in the chamber for voting.

2.3.2.3 Jury Decisions

Jury voting is the most restrictive form of voting system considered here, in terms of the amount of information published concerning the result of the vote. Jury voting contexts characteristically employ a SMSP electoral system with just two options available - for or against a motion; the guilt of an accused, for example.

In contrast to public elections, the specific tally resulting from votes cast by jurors is not usually made public. Rather, a statement of whether the tally of votes for a motion reached a threshold (plurality, more than two thirds majority, unanimity etc.) is published. Such a restrictive secrecy requirement can have the advantage of protecting the value of a voter's choice in circumstances where voters are unanimous, as discussed in Section 2.3.1.

A consequence of such secrecy is that the accuracy of the tally of votes may be hard to determine. In some jury voting contexts, each of the voters may know the association between individual votes and voters but since the voters are usually a small subset of an interested population and are unable to prove the choice of other voters this is not considered a violation of secrecy. Some voting schemes have been proposed in which even voters do not know the association of votes and other voters. Such schemes produce proofs that a statement concerning a collection and tally of encrypted votes is accurate without revealing the value of individual votes of the tally [61].

2.3.2.4 Shareholder Motions

Shareholder voting contexts are similar to parliamentary elections in terms of secrecy and accuracy requirements. With respect to electoral system, a SMSP scheme is used as for parliamentary schemes to vote for or against a motion (approve an executive's salary and bonus, for example), but a voter's franchise is defined by the number of shares the voter

possesses. Each voter is provided with a number of votes proportionate to the number of shares they possess.

2.3.3 Summary: Voting Context Diversity

Much of the focus of voting scheme design has been on public elections [7, 25, 51, 74] because of the restrictive properties most public election voting contexts require of voting systems. These requirements typically combine (in some form) voting privacy and a tally accepted by candidates and voters for determining winners. The discussion has illustrated the diversity of requirements, both across a broad range of voting contexts and within the supposedly narrow range of public elections.

2.4 Requirements and Standards

In the previous section, the scope of voting contexts were elicited, together with an outline of several classes of voting contexts which exhibit similar properties. In this section, the next level down in the voting framework is surveyed. Voting system requirements models provide a mechanism for the capture of requirements expressed by a particular voting context. The requirements model may then be used to direct the design of a voting scheme which fulfills the necessary requirements of the voting context.

This section outlines efforts towards establishing requirements models for public election contexts in the United States and the United Kingdom. Public elections are chosen for the survey since the majority of efforts towards establishing voting system requirements have been for this context.

2.4.1 Voluntary Voting System Guidelines

S

The Voluntary Voting System Guidelines (VVSG) [38] and its predecessor the Voting System Standards (VSS) [48, 49] and earlier the Federal Election Commissions guidelines, together with several previous reports and studies compiled for the United States government [127, 128] provide a requirements model for the conduct of public elections in the United States. The documents provide a collection of requirements for the technologies and systems in use in the US public election context, together with a methodology to assess technologies and procedures against the standards.

The VSS were originally produced in 1990 by the Federal Election Commission (FEC) as the Performance and Testing Standards, to provide a voluntary nationwide standard for the production and testing of voting technologies and systems [48]. Legislation passed following the 2000 US Presidential Election [58] mandated that the VSS be updated, with control of the process passing to the Election Assistance Commission (EAC). A subcommittee of the EAC, the Technical Guidelines Development Committee, were tasked with developing a new standard and certification process for voting systems. The new document [38] is based on the 2002 Voting System Standards [49] which were adopted as preliminary standards for the EAC. The VVSG is divided into two volumes, specifying the standards which voting systems must comply with in Volume One (Performance Standards), and the mechanism by which voting systems are assessed in Volume Two (Testing Standards).

In the VVSG, performance standards of voting systems is divided into the following categories:

- Functional capabilities
- Hardware requirements
- Software requirements
- Telecommunication requirements
- Security
- Quality assurance requirements

- Configuration management requirements.

The functional capabilities provide a high level description of functions which the voting system should provide and may be regarded as the core of the VVSG. For example, a voting system must provide "security access controls" [38, Vol I. Sec 2.2.1.a] to prevent unauthorised access to a "critical components" of the voting system. However, the manner in which the security controls are to be implemented and what they must protect is left unspecified. Hardware requirements cover the quality of hardware components of a voting system, including detailed parameters of environmental conditions within which a voting system could be expected to operate. The software requirements apply to all source code developed by a voting system vendor, but not to externally procured software (i.e. operating systems, device drivers and procured middleware). The software requirements provide standards for development, organisation and documentation of the vendor's source code. Telecommunication requirements apply to communications typically between an election administrator and individual polling places. Security requirements provide standards for both physical security of voting devices in polling booths and the security of software employed on voting devices. Requirements are specified for the escrow of software used on voting devices to repositories specified by the EAC. The security requirements are intended to enforce the functional capabilities previously specified (secrecy, accuracy, usability etc). Quality assurance requirements define standards for testing of individual components of a voting system (including software installation) together with documentation to support the testing. The configuration management requirements provide standards for the manner in which a customer is migrated between similar versions of a voting system.

The outline above demonstrates both the breadth and detail of the VVSG requirements model. A difficulty identified by the VVSG is the trade-off to establish between high level generic requirements which may be applied consistently to a broad range of voting systems (incorporating high level statements which capture secrecy requirements, for example) and providing low-level, detailed requirements against which particular voting systems may be evaluated. High level requirements provide a general statement of the needs of a particular voting context, without directing developers towards particular solutions (and thus limiting

innovation). Conversely, for requirements to be testable they must be sufficiently detailed and implementation specific in order for tests to be repeated over time. Low level requirements thus provides a metric by which the success or failure of a voting system in a test may be consistently measured.

The VVSG attempts to resolve the conflict in the requirements approach in two ways. The VVSG categorises types of voting systems and where appropriate, specifies the applicability of detailed, testable requirements. This approach permits standardised tests of requirements to be established across classes of voting systems typically identified by the device used for vote casting or tabulation. For example, the requirements regarding Voter Verifiable Paper Audit Trail (VVPAT)s are only applicable to DRE systems that provide such a feature. The VVSG does not include a requirement as to whether a DRE should include a VVPAT, a decision which is left to local jurisdictions.

To further accommodate the diversity of potential voting systems within a single requirements model, the VVSG detail the procedure for production of a *testing plan* for individual voting systems as an agreement between an EAC certified testing laboratory and the vendor of the voting system [38, Vol II.]. The testing plan is developed with respect to the potential vulnerabilities of the specific voting system (with particular reference to the technology employed for vote casting and tabulation). Test plans are thus tailored to each individual voting system so that irrelevant tests are not included and the manner in which a vendor has mitigated known vulnerabilities for a particular system can be evaluated.

The VVSG are intended to provide a nationally applicable requirements model for the US public election context and is thus a necessarily substantial document. Even if local jurisdictions employ the VVSG, they are still expected to document requirements and standards for their own specific needs.

The approach to capturing and testing requirements adopted by the VVSG results in several disadvantages, including:

- The VVSG state requirements in terms of the voting technologies and procedures

that constitute a voting system, rather than in terms of the US public election context. Whilst the isolation of requirements from solutions is often difficult, the specification of requirements for technologies rather than the problem domain (i.e. the US public election voting context) is a consequence of the requirements and standards procedure being developed after most of the technologies targeted had already gained widespread use. A consequence is that the requirements document is quite substantial (more than 300 pages) and should new technologies be proposed, the requirements will need to be further extended in order to accommodate them.

- The VVSG attempt to apply the requirements established for the US public election context directly to a voting system, without consideration of an intermediate voting scheme as illustrated in Figure 2.1. Whilst this is a necessary consequence of a lack of formal voting schemes for the voting systems employed in the US context, the size and complexity of the VVSG illustrates the disadvantage of this omission.

- Whilst the adoption of a test plan development methodology for individual voting systems mitigates the difficulty of developing a uniform set of tests for all voting systems, a consequence is that individual voting systems may not be compared fairly with one another, depending on the agreement reached between testing laboratories and vendors.

- Brady has noted the danger of gross categorisation of voting systems in the context of making statistical assessments of a category of voting system's ability to record a voter's intention [11]. Similarly, a voting system may not be tested for a particular vulnerability because that vulnerability is thought to be present only in other categories of voting systems.

The difficulties of establishing a single requirements model for such a diverse voting context (with diverse established solutions) is illustrated by the unwieldy nature of the VVSG document. The diversity of the US context further suggests that a hierarchical requirements model may in fact be a preferable approach, with limited high level requirements

established at a federal level, together with separate documents for applying those requirements to particular technologies. The US public election context may also benefit from establishing formal voting schemes that may be evaluated against more concise requirements documents (together with any necessary assumptions) prior to implementation as a voting system.

2.4.2 Common Criteria

In her doctoral dissertation, Mercuri initially surveys some of the discrepancies that have arisen in public elections where DRE technologies have been employed [91]. Noting that such systems fail to follow identifiable requirements, she proposed adapting the Common Criteria (CC), a computer security assessment standard, to stating the requirements for, and assessing the features of Direct Recording Electronic (DRE) machines used in the US public election context [101]. She then assesses existing DRE systems against this requirements model, concluding that such systems are inadequately implemented with regard to the expected standards extracted from the CC.

To adapt the CC to a voting systems requirements model, Mercuri summarises topics with regard to voting systems for the purposes of security assurance. The resulting requirements document targets both the voting system and development and procurement factors, including the relationship between a product vendor and consumer. The topic areas include:

- Functionality - how a voting system is designed to function in accordance with requirements.
- Accuracy - how a voting system is tested to ensure not only that it is operating, but also that it is operating without errors.
- Confidentiality - preventing the linking of votes with voters.
- Integrity - ensuring that the assets of a voting system (primarily storage of votes) are protected.

EAL	Description
7	formally verified design and tested
6	semiformally verified design and tested
5	semiformally designed and tested
4	methodically designed, tested and reviewed
3	methodically tested and checked
2	structurally tested
1	functionally tested

Table 2.1: Common Criteria Evaluation Assurance Levels as summarised by Mercuri [91].

- Interface usability and availability.

These requirements are then assessed with respect to the seven Evaluation Assurance Levels (EAL) described in the Common Criteria. Table 2.1 summaries the seven EALs, with level 1 providing the most minimal assurance and level 7 describing a system that has undergone formal design verification and testing. Mercuri argues that, at minimum DRE based voting systems should be assessed against EAL 4 requirements (for legacy systems), whilst EALs 5 and 6 provide a more acceptable set of requirements (for new systems).

Mercuri's methodology provides a far more concise approach to evaluating voting systems than the VVSG discussed in Section 2.4.1, however, since the Common Criteria is used as the basis for assessment, the approach is only strictly applicable to software based voting systems, such as DRE machines. Whether Mercuri considers the methodology extensible to other voting systems, or whether she considers it necessary, is unclear. Mercuri's aim is to support her hypothesis and argue that electronic, software controlled technologies are unsuitable for use as voting systems given the conflicts that arise in requirements.

2.4.3 CESG Security Study (UK)

CESG is the commercial arm of the UK Government's Communications Headquarters (GCHQ). In 2002, CESG were contracted by the UK Office of the e-Envoy to conduct a security study of remote electronic voting (REV) in the UK, resulting in an initial document published for comment [18]. A revised document stating the UK government's security requirements was released once the comments had been incorporated into the final document [19].

The final document's approach to stating security requirements is as follows. Initially, assumptions about the context in which voting will occur is divided into domains with discrete responsibilities (registration, vote collection etc) and threats to REV in general are identified, both from internal and external attackers. A statement of fifteen security objectives (OS1-15)[1] is then made, describing the security properties that an REV system should implement in order to counter the identified threats:

1. Effective Voter Registration
2. Effective Voter Authenticity
3. Effective Voter Anonymity
4. Effective Vote Confidentiality
5. Effective System Identification and Authentication
6. Effective System Registration
7. Effective System Access Control
8. Information Integrity
9. Service Availability

[1]The technical requirements document uses the acronym OS for security objective, rather than SO. This work retains the original for reasons of consistency.

10. Information Availability
11. Service Protection
12. Operator Integrity
13. Open Auditing and Accounting
14. Third Party System Authentication
15. Public Verifiability

Finally, a set of requirements statements is provided for each of the security objectives. For example, for Voter Anonymity, requirements specify that an REV system will not be able to associate a vote with a voter under normal operating conditions.

The statement of security requirements as described above was incorporated in the UK government's [56] statement of requirements for the UK's REV pilots in 2002 and 2003, together with a statement of disability access requirements provided by Scope [133]. The statement of requirement provided a further 46 requirements for providers of REV systems covering the wider topic of managing the UK's public election context.

The UK government's approach to capturing requirements is thus substantially different to the approach adopted for the US VVSG described in Section 2.4.1. The UK statement of requirements is concerned primarily with REV systems (vote casting via the Internet, telephone network or digital television system, for example) rather than expressing requirements for the voting system as a whole. As such the requirements are mostly concerned with security issues, with relatively little documentation of usability standards (other than for disabled voters).

The statement of requirements also does not refer to the electoral system in use in the UK public election context. This is problematic since, although much of England and Wales continue to use electoral systems substantially similar to SMSP, Northern Ireland, and more recently Scotland, employ STV for local and/or national elections. The oversight

this highlights is illustrated by the voting scheme proposed by CESG in the original security study, which does not conveniently accommodate electoral systems in which the voter is required to express multiple, structured choices.

Unlike the VVSG, the UK statement of requirement does not provide a methodology for evaluating whether proposed schemes have fulfilled the requirements expressed for them, which is a consequence of the high level, concise form the requirements take. The lack of a proposed testing methodology in the CESG document makes evaluating whether schemes proposed for the UK context, fulfill the identified requirements. For example, the requirement for a vote to be associable with a voter pending judicial review is not fulfilled by a direct implementation of many cryptographic voting schemes whose objective is vote privacy, or even voter anonymity [19, requirement 3.2]. The requirements do however provide a high level basis for developing lower level more detailed, testable requirements for the UK public election context.

2.4.4 Summary

The preceding section has surveyed the major efforts towards establishing requirements models for the US and UK public elections contexts. A difficulty for all requirements models is how to resolve the conflict between providing low level, testable requirements and requirements which are sufficiently high level to permit multiple solutions. The VVSG approach results in a cumbersome and potentially uneven application of requirements to disparate technologies and procedures, whilst the CESG approach provides a high level statement of requirements without a methodology for testing schemes for suitability. Mercuri's approach of adapting and applying the Common Criteria [91, 101] provides a methodology for evaluating voting systems as software artifacts, but is less applicable to other types of voting systems. All three requirements models discussed here specify their requirements with respect to the technology that is expected to be employed, rather than with respect to the properties of the voting context for which a suitable voting system is to be deployed. To a certain extent, this approach may be inevitable, since many voting systems represent a

"facts on the ground" set of circumstances which have already been implemented without prior consideration of requirements. In such circumstances, CESG, Mercuri and VVSG may be viewed as an attempt to retrofit requirements to already deployed technologies. A desirable approach would be to consider the requirements of a voting context in isolation from expected technology in order to provide a framework for evaluation of future voting system proposals.

2.5 Voting Schemes

In this section, *voting schemes* are discussed prior to a consideration of existing voting technologies. Voting schemes provide the design for a voting system intended to fulfill the requirements of a given context. A single scheme may be implemented in a variety of voting systems, differing, for example, in the medium upon which votes are cast, communicated and tabulated.

The cryptographic research community has traditionally considered remote voting schemes as an example of a secure multi-party computation (SMPC), although more recent schemes that envisage a polling station setup move away from this view. An SMPC is a protocol between several participants, each of whom possess a secret value. The goal of the protocol is to globally compute some function over the secret values, without any participant learning any other participant's secret. The computation must be completed successfully and accurately despite the presence of faults within a sub-set of the participants. The possibility of external disruption caused by a malicious observer must also be anticipated.

Cryptographic voting schemes are typically modelled with respect to a malicious adversary, common to many cryptographic protocols outside the field of voting schemes, with varying well defined capabilities. In addition, cryptographic voting schemes are commonly designed to anticipate malicious behaviour by the participants in an election in order to violate the accuracy of an election as discussed in Section 2.3.1. Malicious participants include: voters attempting to vote twice, or claim that they have been cheated of their vote

and election organisers attempting to change the value of individual or sets of votes to their advantage. Given the focus on voting schemes for public election contexts in the cryptographic community, this section surveys the major efforts in this area. In particular, the survey describes recent interest in the potential for use of cryptographic voting schemes for polling station voting systems, rather than the more traditional interest in voting schemes designed for remote voting requirements.

2.5.1 Mix – Nets

The desire to communicate anonymously over computer networks has resulted in a number of cryptographic techniques by which a message may be forwarded to a recipient without including evidence of the sender. First proposed by Chaum in 1980 as a means of providing untraceable email [21], mix-nets are a commonly employed for voting schemes as a construct to replicate the anonymising effect of placing paper ballots into a ballot box.

Mix-nets presume the existence of a Public Key Infrastructure (PKI) for the purposes of distributing public keys. The choice of asymmetric encryption scheme has a consequential impact on the properties of a mix-net, with variations including decryption schemes using RSA and re-encryption mixes. Other variations of mix-nets provide for a secure anonymous service in the presence of failure of some servers [90]. This section outlines an RSA decryption mix.

Figure 2.5 illustrates an RSA decryption mix consisting of n mix-servers. Each mix-server computes two RSA key pairs and publishes both public keys. To prepare a message m for mixing, it is encrypted with each of the mix-servers public keys $K_{1,1}...K_{n,2}$ in reverse order. Each layer of encryption is accompanied by a random seed value $s_{i,j}$ for each layer, such that the message prior to mixing is of the form:

$$\{\{\{\{\{\{m, s_{n,2}\}_{K_{n,2}}, s_{n,1}\}_{K_{n,1}}, s_{2,2}...\}_{K_{2,2}}, s_{2,1}\}_{K_{2,1}}, s_{1,2}\}_{K_{1,2}}, s_{1,1}\}_{K_{1,1}}$$

This construct is sometimes referred to as a *doll*, since the layers of encryption are analo-

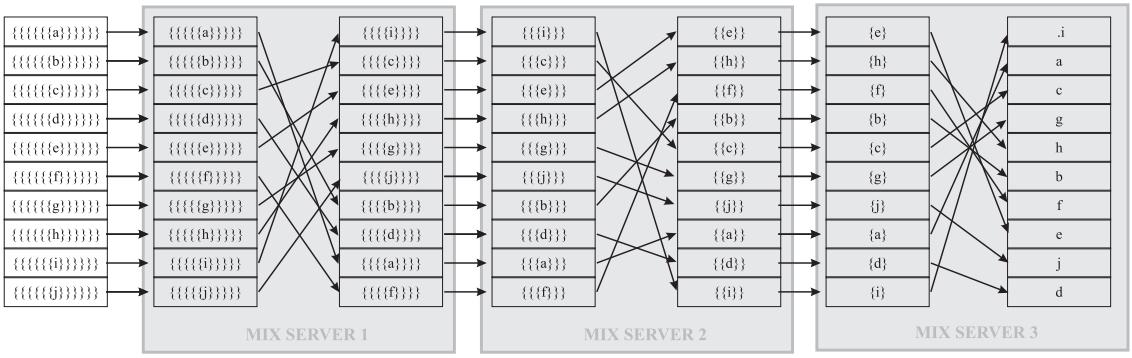


Figure 2.5: Architecture of a de-cryption mix-net anonymous channel. A mixnet consists of a sequence of *mix-servers*. A decryption mix server removes one layer of encryption from each message before and after mixing.

gous to multiple layers of a wooden Russian doll.

A batch of dolls are passed simultaneously to the first mix-server. The server removes the first RSA layer and seed from each doll, permutes the batch and removes the second RSA layer and seed. The dolls are then forwarded to the next mix-server which repeats the process, until all layers of encryption have been removed. Random partial checking may be employed to confirm that each mix-server (with high probability) decrypted each message accurately. In the technique, each mix server randomly reveals either the first or second decryption to an auditor.

Mix-nets are more commonly used as a mechanism for providing an anonymous channel rather than constituting a scheme in their own right. Mix-nets are used for digital signature schemes [51], the Chaum visual cryptography [22] and Prêt à Voter [24].

2.5.2 Homomorphic Schemes

Homomorphic public encryption schemes were first proposed by Benaloh as a mechanism for providing universally verifiable tallies [7, 8, 9]. Homomorphic voting schemes exploit a property of certain asymmetric encryption schemes, whereby given some operation on ciphertexts $\otimes$ and some operation on plaintexts $\oplus$, the following property holds:

$$E(a) \otimes E(b) = E(a \oplus b)$$

Thus decrypting the product of all available ciphertexts yields the sum of plaintext values.

The intutition behind such schemes is as follows. The scheme employs a Tallier and a set of Voter participants and assumes the availability of a secure bulletin board. Each voter encrypts their vote for or against an option (encoded as a single bit $b \in \{0, 1\}$) in an election using the public key of the Tallier. The voters also produce a zero-knowledge proof [90] that the vote is valid (i.e. the voter has not attempted to over-vote).

the voters publish their encrypted votes on a secure bulletin board. Once the period for voting has ended, the encrypted product of votes for each option may be universially computed (be computed by any participant or external observer). The Tallier then publishes a decrypted tally for each option together with a proof that the decryption is accurate. The proof prevents the Tallier from attempting to publish arbitrary results for an election. To prevent early partial tallies being computed by a corrupt Tallier, the Tallier is distributed across multiple domains which must collaborate in order to produce the decrypted sums.

2.5.3 Blind Signature Schemes

Blind signature schemes are perhaps the most widely implemented of electronic voting schemes due to their relative simplicity [30, 35, 76]. A multitude of variations and adaptations have been proposed, in order to improve robustness, for example [35], or to provide for a more flexible electoral system [67]. The scheme exploits a feature of some digital signature cryptosystems (RSA, for example) in which it is possible to add a ‘blinding’ layer of encryption to a message prior to signing by another participant [90]. When the blinding layer is removed from a message, a signature may be obtained for the underlying message. This technique thus allows a participant to obtain a digital signature for a message from a second participant, without the second participant learning the contents of the message.

A common analogy used for explaining blind signatures is to consider an interaction between two participants Bob and Alice (an authentication authority). Bob wishes to send the letter to Charles anonymously, but also wants to demonstrate to Charles he had a right to send the message. Bob thus needs Alice to let Charles know that the letter came from some approved person, but also does not want Alice to inspect the message. To achieve this, Bob places a letter he wishes to send to Charles into an envelope and seals it. Bob approaches Alice and identifies himeself. Alice then applies a stamp to the envelope with a unique imprint that cuts through the paper of the envelope and the letter. Later, Bob can remove the letter from the envelope and places it into a second which he addresses and sends to Charles. Charles can remove the letter from the envelope and check the imprint cut into the letter by Alice to determine authenticity.

The situation is analogous to one in which a voter authenticates to one authority (Alice), and then uses the authorisation obtained from that authority to register a vote anonymously with another authority (Charles).

The scheme envisages the separation of roles between voter authentication and vote casting, as in a conventional polling station environment. As such, two election authorities, a *Validator* (to validate a voter's vote) and a *Tallier*, (to tally validated, anonymised votes) are specified. Figure 2.6 illustrates the basic scheme. The voter encrypts their vote using their secret key $K_{V_{sess_i}}$ and applies a blind layer of encryption to obtain message m'. The voter signs the blinded, encrypted vote using their signing key K_{vot}^{-1} and sends it to the Validator who confirms the message is signed by a registered voter. The Validator applies their own signature to the blinded message using their signing key K_{val}^{-1} and returns the signature s'_{val} to the voter. The voter removes the blinding layer from the signature supplied by the Validator to obtain a signature s_{val} for the encrypted vote. The voter then forwards the encrypted vote and unblinded signature to the Tallier, who publishes a list of received encrypted votes. Once voting is complete, the voters send their secret keys to the tallier via an anonymous channel. The Tallier decrypts and publishes the votes for tallying purposes.

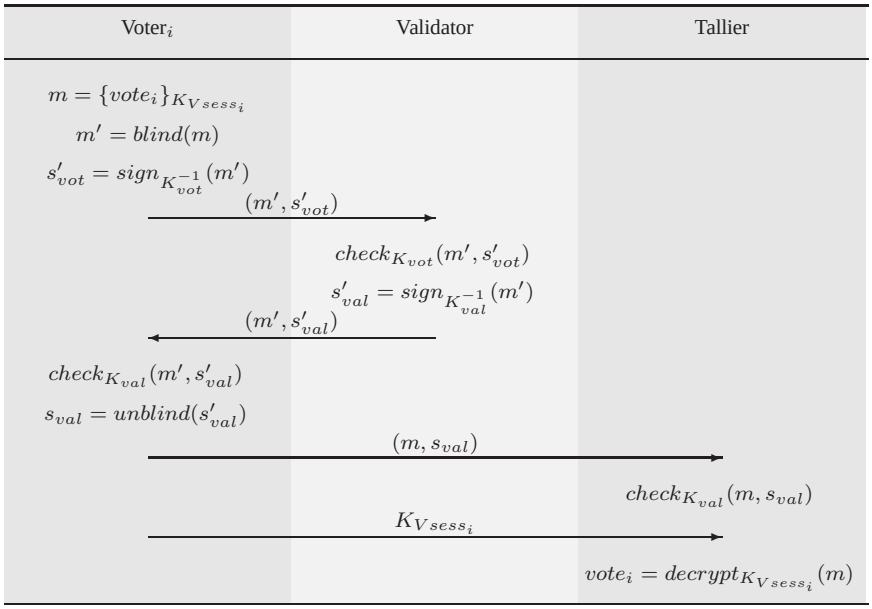


Figure 2.6: The Blind signature voting scheme as proposed by [51]. The voter encrypts their vote using their secret key and applies a blind layer of encryption. The voter signs the blinded, encrypted vote and sends it to a validator who confirms the message is signed by a registered voter. The validator applies their own signature to the blinded message before returning it to the voter. The voter removes the blinding layer of encryption and forwards the message to the tallier, who publishes a list of received encrypted votes. Once voting is complete, the voters send their secret keys to the tallier via an anonymous channel. The tallier decrypts and publishes the votes.

2.5.4 Hybrid Schemes

Since the 2000 US election and the passage of the Help America Vote Act HAVA 2002, interest has grown in the potential for voter verifiable paper audit trails (VVPAT). Both research efforts and campaigns by voting rights advocates in the United States have proposed that VVPATs be incorporated into Direct Recording Electronic (DRE) voting machines for use in US public elections [34, 57, 91]. DRE machines equipped with a VVPAT print a representation of a voter's choices on a paper ballot for inspection by a voter prior to those choices being finalised by the DRE. If the voter determines that the DRE has inaccurately recorded their choices on the paper ballot, they may choose to edit the changes on the machine and re-print the ballot. Once the voter is satisfied that the machine has accurately printed their choices, the paper ballot is committed to a secure ballot box, either by the DRE device, or by the voter. Should the voter handle the paper ballot prior to committment, then procedures, or mechanism are required to manage the potential for the voter to change the paper record. Such change might, for example, enable the voter to claim that the voting machine has attempted to change the electronic representation of their choices, without this being the case. In the case of a disputed election, the paper ballots are assumed to be the accurate record of a voter's choices and the implicit assumption is that paper is a trusted medium for vote storage.

In the cryptographic community, the proposals for VVPATs have spurred interest in the potential for providing *non-transferable* verification receipts, that is, some token which the voter may remove from a polling station and use to confirm that a vote has been included in a collection for tallying. The tokens are non-transferable because a voter is unable to use them to convince a third party of the choices represented by the receipt. Such schemes are termed *hybrid* in this work because of the presumption that an electronic voting device will be combined with some trusted medium (typically paper) in a voting system to produce an encrypted representation of their vote (an encrypted receipt).

To demonstrate to the voter that the encrypted receipt accurately represents their vote (without demonstrating how to decrypt the receipt), hybrid schemes commonly employ some

form of multi-round cut and choose protocol. Cut and choose protocols are a cryptographic construct in which one participant (a voting system, for example) is forced to commit to some value before being tested by a second participant (a voter, for example).[2] Cut and choose protocols force a voting system to decide whether to attempt to cheat a voter before a voter engages in a process which (with high probability) will detect the cheating.

Figure 2.7 gives the generic arrangement for hybrid schemes. Most hybrid schemes envisage a scenario in which a voter interacts with a voting device in a supervised polling station in order to produce an encrypted receipt of their vote. The interaction is arranged such that some additional secret is established between the voter and the machine that is non-transferable to an external observer once the interaction is complete. The receipt is provided to the voter in the form of a paper receipt and also published to a publicly accessible bulletin board. After leaving a polling station, the voter may confirm that the encrypted receipt of their vote has been published on the bulletin board. To obtain a collection of decrypted votes, the encrypted representations are passed through a decryption mix-net similar to that described in Section 2.5.1. The unencrypted votes may then be tallied as desired, but by using a mix-net to perform decryption, are not associable with the encrypted representations (unless all mix servers collaborate). Several examples of hybrid schemes are discussed below.

2.5.4.1 Chaum

The Chaum voting scheme employs visual cryptography in order to encrypt a graphical representation of a voter's choices [23]. The scheme is useful for voting in public elections in the US as it does not preclude the use of write-in options. The scheme closely follows that of the generic model for hybrid voting schemes illustrated in Figure 2.7, including the use of a RSA decryption mix. Explanations of the scheme are also provided by Bryans and

[2] Schneier describes the equal cake cutting metaphor from which the term for these protocols originates, in which one participant is able to cut a cake as they wish into two pieces, but the second participant is able to choose which half of the cake to eat. The first participant is encouraged to behave honestly and share the cake equally [129].

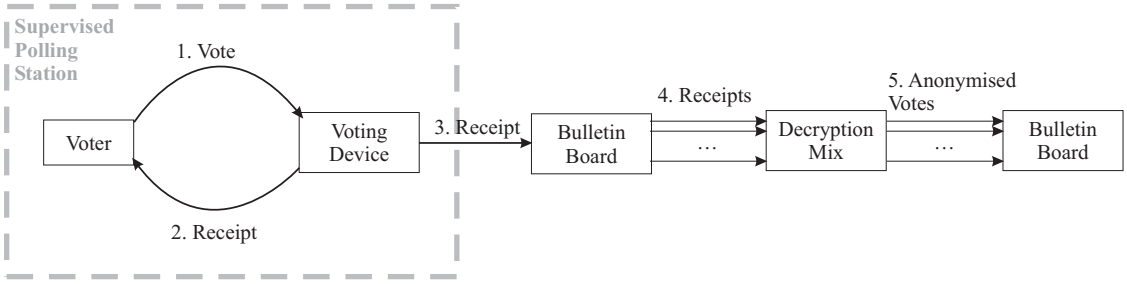
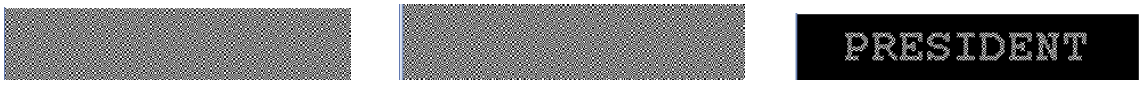


Figure 2.7: A Generic hybrid voting scheme, illustrating vote casting for one voter (steps 1-3) and receipt decryption and vote counting in steps 4 and 5. In step 1 the voter provides their choice to the voting device. The device responds with an encrypted receipt in step 2. The voter obtains some assurance that the machine has correctly encrypted their vote (through a cut and choose protocol, for example). Once satisfied, the voter removes the receipt from the polling station. In step 3 the encrypted receipt is published to a secure bulletin board where it's presence may be verified by the voter. In step 4, all published encrypted receipts are passed through a de-cryption mix to produce an anonymised batch of decrypted votes suitable for tallying (step 5).

Ryan [14] and by Karlof [75].

In the scheme, a receipt is provided to the voter as one layer from a two layer visual encryption of text printed as a graphic. Figure 2.8 is a reproduction illustrating the two layer paper ballot, taken from a prototype of the Chaum scheme prepared by the author. While the two layers of the ballot paper are overlaid, the plain text choices of the voter are evident. However, once the layers are separated, the plain text message is encrypted in both layers. Via suitable cryptographic techniques, the original vote is recoverable from either ballot paper layer as described below. The technique permits the voter to leave a polling station with one layer of the ballot paper or another, which forms an encrypted receipt of their vote. The layer kept by the voter is also retained electronically by the voting machine and posted to a bulletin board, as per the description for generic hybrid schemes.

To generate the two layers of the ballot paper, a representation is generated as white text on a black background. Each pixel of the ballot image is divided into four 'sub-pixels'. For each black pixel on the original image, a corresponding sub-pixel group on each layer of the ballot paper is printed:



(a) Layer L0 of the ballot paper. (b) Layer L1 of the ballot paper. (c) The two layers of the ballot paper combined to reveal the encrypted text.

Figure 2.8: The Chaum scheme two layer ballot paper. The illustrations were extracted from a prototype of the Chaum scheme implemented by the author. Chaum provides details of the scheme in [22].

$$\begin{array}{cccccccc} \blacksquare & \blacksquare & & \blacksquare & \square & \square & \blacksquare & \qquad \square \; \blacksquare \; \blacksquare \; \square \\ \blacksquare & \blacksquare & \longrightarrow & \square & \blacksquare & , \; \blacksquare & \square & \text{or} \quad \blacksquare \; \square \; , \; \square \; \blacksquare \\ B & & & L0 & & L1 & & \qquad L0 \qquad L1 \end{array}$$

such that when the two layers are combined a sub-pixel group of four black pixels is constructed. Similarly, for each white pixel of the original image, a corresponding sub-pixel group on each layer of the ballot paper is printed:

$$\begin{array}{cccccccc} \square & \square & & \blacksquare & \square & \blacksquare & \square & \qquad \square \; \blacksquare \; \square \; \blacksquare \\ \square & \square & \longrightarrow & \square & \blacksquare & , \; \square & \blacksquare & \text{or} \quad \blacksquare \; \square \; , \; \blacksquare \; \square \\ W & & & L0 & & L1 & & \qquad L0 \qquad L1 \end{array}$$

such that when the two layers are combined a sub-pixel group of two black and two white pixels is constructed. The result of the layer construction described above is that both layers consist only sub-pixel groups of the form:

$$\begin{array}{ccc} \blacksquare & \square & \qquad \square \; \blacksquare \\ & \text{or} & \\ \square & \blacksquare & \qquad \blacksquare \; \square \end{array}$$

To construct the two ballot layers described above, two RSA mixnet dolls are constructed using two sets of $2l$ pseudo random strings, with each string of length equal to half the

number of pixels in the original ballot image. The two sets of strings are then composed into a pair of single strings:

$$s_B = s_{b,1} \oplus s_{b,2} \oplus ... \oplus s_{b,2l}$$

$$s_T = s_{t,1} \oplus s_{t,2} \oplus ... \oplus s_{t,2l}$$

The bits of the two string are then arranged into a "checkerboard" one time pad matrix denoted:

$s_{B,1}$	$s_{T,1}$	$s_{B,2}$	$s_{T,2}$	$s_{B,3}$
$s_{T,3}$	$s_{B,4}$	$s_{T,4}$	$s_{B,5}$	$s_{T,5}$
$s_{B,6}$	$s_{T,6}$	$s_{B,7}$	$s_{T,7}$	$s_{B,8}$
...				

Similarly, the bits denoting the ballot image are arranged into a "checkerboard" matrix as illustrated:

$b_{T,1}$	$b_{B,1}$	$b_{T,2}$	$b_{B,2}$	$b_{T,3}$
$b_{B,3}$	$b_{T,4}$	$b_{B,4}$	$b_{T,5}$	$b_{B,5}$
$b_{T,6}$	$b_{B,6}$	$b_{T,7}$	$b_{B,7}$	$b_{T,8}$
...				

Note that the top-bottom arrangement of bits is reversed for the ballot image matrix. Next, a "ciphertext matrix" checkerboard is constructed from the ballot image matrix and the one time pad matrix, again consisting of top T and bottom B bits. The visual cryptography "overlay" operator is not closed, so the T, ith bit of the matrix is computed to satisfy the equation $c_{T,i} \oplus s_{B,i} = b_{T,i}$; the B, ith bit of the matrix is computed to satsify the equation $c_{B,i} \oplus s_{T,i} = b_{B,i}$. The complete matrix is thus a checkboard denoted:

$c_{T,1}$	$c_{B,1}$	$c_{T,2}$	$c_{B,2}$	$c_{T,3}$
$c_{B,3}$	$c_{T,4}$	$c_{B,4}$	$c_{T,5}$	$c_{B,5}$
$c_{T,6}$	$c_{B,6}$	$c_{T,7}$	$c_{B,7}$	$c_{T,8}$
...				

Finally, the two separate layers L_0 and L_1 are constructed from bits of the one time pad matrix and the bits of the ciphertext matrix:

$c_{T,1}$	$s_{T,1}$	$c_{T,2}$	$s_{T,2}$	$c_{T,3}$
$s_{T,3}$	$c_{T,4}$	$s_{T,4}$	$c_{T,5}$	$s_{T,5}$
$c_{T,6}$	$s_{T,6}$	$c_{T,7}$	$s_{T,7}$	$c_{T,8}$
...				

L0

$s_{B,1}$	$c_{B,1}$	$s_{B,2}$	$c_{B,2}$	$s_{B,3}$
$c_{B,3}$	$s_{B,4}$	$c_{B,4}$	$s_{B,5}$	$c_{B,5}$
$s_{B,6}$	$c_{B,6}$	$s_{B,7}$	$c_{B,7}$	$s_{B,8}$
...				

L1

The arrangement is such that when the ith bits of the matrix are overlaid, the ballot image bits are displayed:

$$c_{T,i} \oplus s_{B,i} = b_{T,i} \text{ and } c_{B,i} \oplus s_{T,i} = b_{B,i}.$$

During tallying, the layer of the receipt chosen by the voter, together with the corresponding 2 RSA dolls is passed through a decryption mix, with the seed strings $s_{b,j}$ and $s_{t,j}$ extracted from each of the $2l$ layers. It may be observed that applying the bits of each seed string to the receipt image using bit-wise exclusive or will reveal the original ballot image since, for the ith pixel in the top layer, say:

$$\begin{aligned} c_{T,i} \oplus s_{b,1,i} \oplus s_{b,2,i} \oplus ... \oplus s_{b,2l,i} &= c_{T,i} \oplus s_{B,i} \\ &= b_{T,i} \end{aligned}$$

and

$$\begin{aligned} c_{S,i} \oplus s_{t,1,i} \oplus s_{t,2,i} \oplus ... \oplus s_{t,2l,i} &= c_{T,i} \oplus s_{T,i} \\ &= 0 \end{aligned}$$

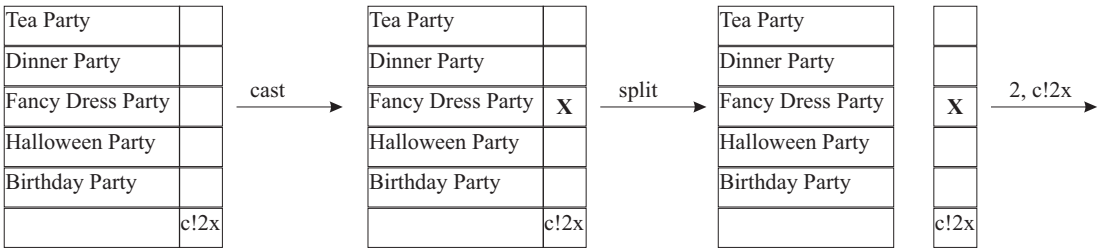


Figure 2.9: The Prêt à Voter scheme ballot paper [25]. The voter marks the selected candidate before separating the two columns of the ballot. The right hand side of the vote forms an encrypted receipt.

2.5.4.2 Prêt à Voter

The Prêt à Voter scheme was intially presented as a simplification of the Chaum visual cryptography scheme discussed in the previous section [15, 24, 25]. However, the scheme was later developed to provide an alternative mechanism for providing a voter receipt. The new mechanism has the benefit (for UK public elections) of leveraging the existing voter experience. However, the scheme precludes the use of write-in options for votes, which is necessary for the US context.

The scheme is derived from the layout of paper ballots common in the UK and elsewhere, with the added feature that the order of candidates is randomly permuted on the ballot paper. The permutation of candidates is encrypted in an RSA doll placed below the right hand column, as illustrated in Figure 2.9. The encryption of the permutation within the Doll is computed in a similar manner to the visual encryption seeds for the Chaum scheme discussed in the previous section. For the Prêt à Voter scheme, the random seed generated for each layer of the Doll is hashed using a publicly known function to generate a 'partial permutation'. The product of these partial permutations (modulo the number of candidates) is then applied to the candidate list on the left hand side of the ballot paper.

To cast a vote, the voter marks the ballot paper as normal and then separates the left and right columns. The right hand column is fed into a vote reading device and then retained as a receipt. The left hand side is discarded. The voting device forwards the Doll value and the position of the voter's mark on the ballot paper to a bulletin board where it may be

verified by the voter. Decryption and tallying is as per the generic hybrid scheme described in Section 2.5.4. Each layer of the RSA doll is decrypted, and the hash of the extracted seed value is computed using the same function as for preparation of the doll. The partial permutation is then subtracted from the position of the voter's choice. Once the Doll and vote position have passed through the complete mix-net, the voter's choice is aligned with the un-permuted location of their candidate's name.

Several variations to the scheme have been presented demonstrating considerable flexibility [25, 26]. An advantage of the scheme is that the voting device does not learn a voter's choice and thus precludes the possibility of the device leaking the association between votes and voters, a potential weakness of other hybrid schemes.

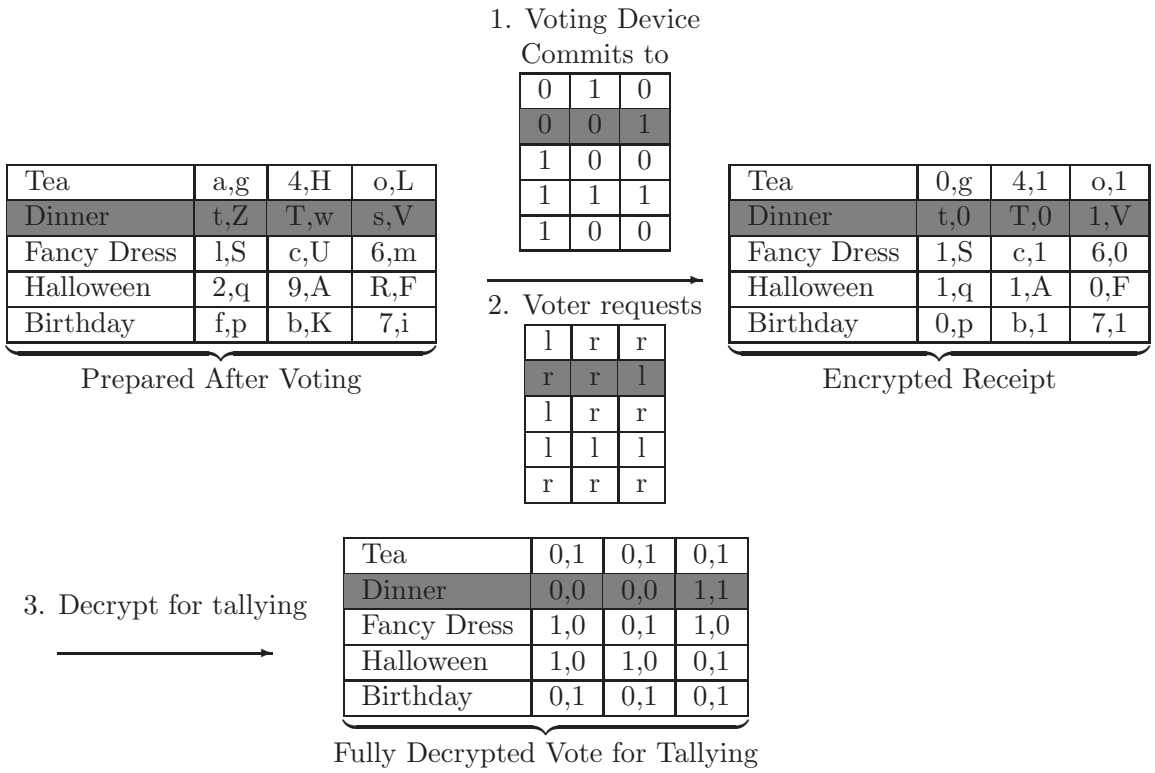
2.5.4.3 Neff/VoteHere

The Neff/VoteHere scheme [97, 98] is similar to the generic hybrid scheme described in Section 2.5.4 in which a voter interacts with a voting device in order to prepare a receipt for their vote.[3] In the scheme a vote receipt is represented as a set of bit pairs arranged in a matrix. Each row of the matrix corresponds to an option that was available for the voter to vote for.

Each bit pair consists of a pair of bits $b \in \{0, 1\}$ and initially all bits are encrypted under the El-Gamal asymmetric key scheme. Rows corresponding to options selected by the voter consist of encrypted bit pairs of the form $\{0, 0\}$ and $\{1, 1\}$, whilst rows of unselected options are of the form $\{0, 1\}$ and $\{1, 0\}$ as per Figure 2.10.

To verify the correctness of the receipt, the voting device commits to a bit value for each bit pair in the matrix. The voter then randomly chooses the left or right bit of each pair in the matrix to be decrypted, revealing whether the encryption represented a 0 or 1 bit value. For the row corresponding to the voter's chosen option, the revealed bit should equal the committed bit value of the voting device for that pair, whilst for non-choice options, the

[3] For a comprehensive description and analysis of the scheme see Karlof [75].



Tea	a,g	4,H	o,L
Dinner	t,Z	T,w	s,V
Fancy Dress	l,S	c,U	6,m
Halloween	2,q	9,A	R,F
Birthday	f,p	b,K	7,i

0	1	0
0	0	1
1	0	0
1	1	1
1	0	0

l	r	r
r	r	l
l	r	r
l	l	l
r	r	r

Tea	0,g	4,1	o,1
Dinner	t,0	T,0	1,V
Fancy Dress	1,S	c,1	6,0
Halloween	1,q	1,A	0,F
Birthday	0,p	b,1	7,1

Tea	0,1	0,1	0,1
Dinner	0,0	0,0	1,1
Fancy Dress	1,0	0,1	1,0
Halloween	1,0	1,0	0,1
Birthday	0,1	0,1	0,1

Figure 2.10: The VoteHere scheme ballot paper. The voting device prepares a bit pair matrix in which each row corresponds to a voting option. The voter's choice is highlighted on the matrix for illustrative purposes here. Initially, each bit in the matrix is encrypted as an El-Gamal ciphertext, with ciphertexts arranged into pairs. The ciphertext pairs are arranged such that the row of the voter's choice consists of encrypted $\{0,0\}$ and $\{1,1\}$ pairs, whilst the bit pair for all other rows consist of $\{0,1\}$ and $\{1,0\}$. In Step 1 in the diagram, the voting device provides a committment bit for each bit pair in the receipt. The voter then chooses randomly for the left or right bit of a pair to be decrypted in Step 2. Each bit decrypted in the voter's chosen option row should match the committment bit for that pair provided by the voting device (assuming the voting device did not attempt to cheat). After voting is complete, the receipts are anonymised and all remaining bits are decrypted to reveal the voter's choice indicated by a row of $\{0,0\}$ and $\{1,1\}$ bit pairs.

committment bit will equal the revealed bit with probability of $\frac{1}{2}$. The security of the verification process is thus parameterised by the number of columns k of bit pairs in the matrix, with probability $\frac{1}{2^k}$ that the voting device will be able to change a voter's choice undetected.

Assuming that the voting device has not cheated, the voter can now leave the polling station with their partially decrypted receipt, which will be published on a bulletin board, as per the generic hybrid model. For an attacker who did not observe the interactions between voting device and voter all rows on the receipt have equal probability for representing the voter's choice. During tallying the election authority can completely decrypt anonymised receipts in order to determine which bit pair matrix row corresponds to the voter's choice.

2.5.4.4 Remote Voting with Hybrid Schemes

Whilst hybrid schemes presume that some interaction will occur between the voter and the voting machine that an external observer cannot observe (as occurs in a supervised polling station, for example), adaptations to at least one suggest such schemes could be used for remote unsupervised voting [26].

2.5.5 RIES

The Rijnland Internet Election System (RIES) is a scheme designed to provide remote electronic voting for a water authority in the Netherlands [63]. The scheme is relatively simple compared to those discussed above, with only a single encryption and decryption step. In the scheme, an election authority generates a table consisting of all possible votes encrypted under DES, using a different DES key for each voter. Each voter is sent their DES key via a secure channel.

To cast a vote, a voter computes a Message Authentication Code (MAC) of their choice combined with a MAC of their own identity. A vote collector decrypts this information for

tallying, and after the end of voting publishes all the encrypted votes received along with an MD5 hash of the vote so that each voter can confirm both that only pre-declared votes have been published (to resist vote stuffing) and also that their vote has been published and correctly received.

2.5.6 Summary of Voting Schemes

The voting schemes discussed in this section provide only a sample of the diversity of approaches proposed. Variants to the schemes discussed here are also numerous. Other schemes, for example, include Riera (using mobile agents to perform mixing) [117] and Reynolds [116]. Remote, coercion resistant schemes have also been proposed to resist attacks such as vote-buying [74]. The purpose of this section was to demonstrate that voting schemes are designed for a particular context, with a particular electoral system and set of secrecy, accuracy and some usability requirements to be fulfilled. Voting schemes then, are placed appropriately in the framework described in Section 2.2, since they are targeted towards specific requirements, but are not by themselves implementations for use as a voting system.

2.6 Voting Systems and Technologies

In the framework presented in Section 2.2, voting systems are the implementation of the properties specified by voting schemes. Voting systems combine both technology and procedural activities surrounding the technology in order to conduct an election within the requirements specified at a higher level in the framework.

A number of attempts have been undertaken to catalogue and classify voting technologies, usually (but not exclusively) focusing on technologies used in public elections. Classification of voting technologies may be undertaken in terms of the location of vote casting (supervised or unsupervised), the mechanism for storing a vote tally (ballot or ballotless),

		Medium	
		Balloted	Ballotless
Location	Remote	Postal (Mail-in paper ballot), Internet, SMS	Online opinion polling software Show of hands
	Supervised	Paper ballot Optical Scan, Punch Card, DRE with VVPAT	Lever Machine, DRE,

Table 2.2: Voting technologies classified by location and casting medium. This classification is in contrast to other schema (see for example [53, pp64]), where priority is given to the medium of the ballot over the location of the voter.

the medium on which records are stored (paper, digital media etc.), the medium on which votes are stored (with the implications for the trustworthiness of the store itself) and the usability properties of the technology (convenience, availability etc.). This section describes the most prevalent technologies employed to implement voting schemes. Table 2.2 summaries the instances of voting technologies described below.

2.6.1 Ballots and Boxes

Paper ballots and other physical records are perhaps the oldest vote casting technology known. Ancient Athenians used saucer like objects to record votes for or against accused in jury trials [13]. Paper ballots were first used in Australian public elections in 1856 [100], for UK public elections in 1872 [112] and were first used in the US in New York and Massachusetts in 1888 [73].

In a typical voting system using paper ballots and ballot boxes, a voter authenticates themselves in a polling station. The voter is then provided with a paper ballot on which the choices for the election are presented, along with some instruction as to how to cast a valid vote. The voter marks the paper appropriately, which then becomes the record of the voter's choice. The ballot paper is then placed (along with others) in a secure ballot box, from which it cannot be retrieved until vote tallying begins. Paper ballots are typically counted by human counting clerks in the presence of both partisan and independent observers. The paper ballot votes may be recounted several times in this manner, if the result of the election is close, since the result of each re-count may vary. Recent technology has been used in the UK for public elections for the electronic counting of hand marked paper ballots [139].

Although they do not necessarily need to be used as such, paper ballots are typically associated with the use of ballot boxes to break the association between votes and voters, thus providing commonly employed secrecy properties.

Paper ballots are implicitly considered to provide a trusted medium on which votes may be stored prior to tallying. As discussed in Section 2.5.4, paper ballots may be used to provide a receipt for an otherwise electronic voting system because of their trusted nature. However, paper ballots cannot be used to constrain voters to cast a correct vote, so their use may violate accuracy requirements which specify accurate recording of valid votes by a voter. Further, the accuracy of a tally produced is uncertain, since the result of multiple manual recounts of paper ballots may vary.

Requiring a voter to attend a polling station in order to cast a vote in a supervised environment (and fulfill secrecy requirements) may violate convenience requirements in some contexts. An organisation may not have sufficient resources to provide polling stations conveniently for voters, such that inconvenience limits participation.

2.6.2 Postal or Mail in Paper Ballots

The use of paper ballots and ballot boxes discussed in the previous section may be extended to permit remote, unsupervised voting. Postal voting allows paper ballots to be marked in an un-supervised environment, with the paper ballot (prior to and after) marking to be sent via a supposedly secure channel (the postal service).

Postal voting varies the properties of supervised paper ballot voting by providing the potential for the association between votes and voters to be obtained by an observer, since voting does not occur in an isolated environment. In addition, postal voting presents greater opportunities to an attacker to violate the accuracy of a tally, either during vote casting (through coercion or vote buying) or vote communication (by intercepting uncast or cast paper ballots). However, postal voting provides greater convenience than polling station voting, since vote casting may be completed anywhere, and in a larger time frame than is usually permitted for polling station voting.

2.6.3 Lever Machines

By the late nineteenth century, the use of non-standard paper ballots had led to endemic attacks on the accuracy of tallies for public elections in the US. Non-standard paper ballots were produced by political party organisations in such a way as to prevent modification of the pre-printed choices for all races, giving rise to the term ‘party ticket’ [54, 73]. Although ballot papers would eventually become standardised and provided to voters by public authorities rather than partisan political parties, these improvements did not prevent attacks which exploited the *mobility* of ballot papers, i.e. the ease with which ballot papers could surreptitiously removed from a polling station and altered, facilitating attacks such as chain voting as discussed in Section 2.1.

Lever machines were intended to overcome the potential for chain voting. The devices store tallies of votes on internally secured mechanical counters. To cast a vote in a set of multiple races, a voter adjusts levers on the user interface of the lever machine to the

position corresponding to their selections. When the voter is satisfied with the configuration of the levers, a further lever is pulled to increment the correct internal counters. A detailed study of lever machines is conducted by Roth [119], with particular focus on usability issues.

Since the lever machine is ballotless, the potential for violating common secrecy requirements of public elections (the association between vote and voter) is limited to the vote casting period. However, several attacks have been identified which may violate the accuracy of tallies recorded using the lever machine. Mercuri notes that the internal mechanics can be tampered with either to initialise the counters for disfavoured options to a negative value, or to retard the incrementation mechanism, such that only a portion of votes for a unfavoured option are recorded [91]. Alternatively, a lever machine presents opportunities for violating accuracy during interaction with the user interface by a voter. An attacker may, for example, tamper with the labels for disfavoured options (or remove them entirely) so that a voter does not know how to configure the lever for a desired selection in a particular election.

2.6.4 Punch Card/Optical Scan

Automatic vote counting devices were first introduced into public elections in the United States as a means of increasing the speed of counting votes for public elections [96]. Initially, automatic vote scanning was conducted using punch card technology. Later, optical scan devices were used. In both cases, the introduction of automatic vote counting technologies was intended to improve the speed and efficiency of computing a tally and announcing a result, with the supplementary benefit of reducing costs [73].

The voting process is substantially similar to that of paper ballots, other than the manner in which choices are presented to a voter and the way in which a voter marks their choice on a card ballot. A voter marks the ballot in such a way that the mark can be read by the automatic counting device. The voter does this either by punching a hole through card, or

marking the card with special purpose ink.

Whilst automating vote tallying has no direct impact on other aspects of the vote casting process, the usability (and hence accuracy) of vote casting may be affected if the vote counting technology constrains the presentation of voting choices to a voter (on the card ballot for example) in an adverse manner. For example, the 'butterfly' layout of punch card ballots in the US 2000 General Election caused controversy because some voters were believed to have been confused into voting for the wrong candidate [12, 92]. The layout was necessary because all punch marks had to be placed along the spine of the card ballot for reading purposes.

The tallying process of automatic ballot counting is also less transparent than that of counting ballot by hand, since observation of the process by outsiders is not possible. External observers may need some mechanism to reassure themselves that the internal counting software has been correctly implemented, either through software verification of correctness [127], re-running the counting procedure, or partial manual recounts of some of the paper ballots [91]. The procedures surrounding the use of electronic counting technologies thus become important in determining whether the technology fulfills accuracy requirements in a particular context. More recent vote counting technologies are capable of scanning conventionally marked paper ballots [139].

2.6.5 Direct Recording Electronic Machines (DREs)

Direct Recording Electronic (DREs) machines were first introduced to public elections in the US in the 1980s [128]. The devices may be superficially viewed as having similar properties to a lever machine, although the use of software provides some quite different properties. Following the passage of the Help America Vote Act 2002 [58], polling places were mandated to be equipped with at least one DRE machine each in order to provide usable voting systems for blind and/or disabled voters.

In a typical vote casting process using DRE machines in the US, a voter enters a polling

station and authenticates themself to a polling clerk. Once authenticated, the voter is typically provided with a smart card which the voter inserts into a DRE machine in order to begin voting. The information written to the smart card may be used to configure the DRE machine when presenting choices to the voter, in circumstances where voters with different eligibility for voting are using the same system [77].

The DRE machine presents the voter with the election choices in which they are eligible to participate, typically on a touch screen monitor. The voter selects choices by pressing buttons on the screen which are labelled for their selection. DRE machines permit considerable flexibility in how election choices are presented to a voter. Typically, DREs machines prevent voters from casting *over-votes* (selecting more than the permitted options for an election) and warn the voter prior to permitting them to cast an *under-vote* (not selecting the maximum possible choices for an election). Further, DRE machines may be equipped to permit voters with physical disabilities to vote without (privacy violating) assistance.

DRE machines store electronic records of individual votes, rather than an aggregate as stored by lever machines. However, the voter is not able to observe the accurate storage of their vote in the same manner as placing a paper ballot in a secure ballot box. At the close of poll, the machines report a tally of votes, which are communicated to a central tallying location either via modem, an oral report from a polling clerk monitoring the DRE machine, or on electronic storage media physically transported to the counting location.

DRE machines may thus be vulnerable to violation of the accuracy of the tally at any point between vote casting and tallying. Procedural techniques to verify the integrity of software employed by DRE machines are the most common technique for ensuring the accuracy of voting tallies [49], although the task of guaranteeing the behaviour of software artifacts is considered to be intractable [141] and the difficulty is only increased if the binary instructions (rather than uncompiled source code) must be inspected. Ensuring that provided source code (where available) is a faithful representation of the compiled binary is a separate problem [140], although more recent results suggest that this problem may be manageable [144]. The use of Voter Verifiable Paper Audit Trails (advocated by Mercuri

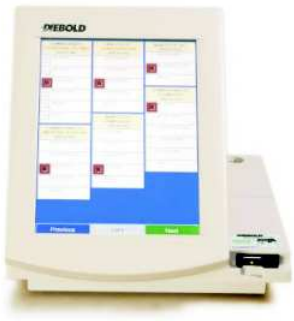
[91] and Dill [34] for example) has been proposed to remedy the lack of transparency of DRE machines. However, such add-ons risk eliminating the usability properties of DRE machines discussed above, since a disabled voter may require assistance to interpret the 'voter verifiable' paper ballot.

India and Brazil have also recently begun employing DRE machines for the conduct of public elections. In particular, Indian DRE machines reflect the requirements of the Indian voting context:

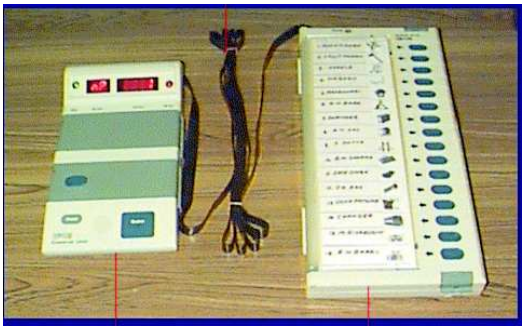
- the DRE machines are considerably simpler than those used for the US, reflecting the far fewer elections conducted simultaneously.
- robust design allow the DRE to be transported across India during the election period so that they can be re-used in several constituencies.
- the DRE machines are equipped with fail safe mechanisms which allow them to be quickly deactivated in the event of an attack on a polling station by partisan activists.
- the devices reflect the lower literacy rates of Indian voters, with candidates identified by small logos next to buttons on the DRE machine interface, rather than using complex touch screens [5].

Figure 2.11 illustrates two examples of DRE machines employed in US and Indian public elections respectively.

DRE devices are also employed in several legislative voting contexts, including the Scottish Parliament, the Israeli Knesset and the US Senate. DREs used in these contexts are only required to accept yes/no votes on motions placed before the legislature and are required to record the association between votes and voters.



(a) The Accuvote TS DRE machine manufactured by Diebold for use in public elections in the United States. The DRE is equipped with a smart card reader for voter authentication and a touch screen interface. The interface can display multiple elections simultaneously [33].



(b) The DRE machine and control unit employed for Indian parliamentary elections in 2004, manufactured by Bharat Electronics Limited and Electronic Corporation of India Ltd. Candidates are identified by logos labelling each button on the voting interface. The control device includes tamper resistance features to resist vote stuffing [66].

Figure 2.11: Examples of Direct Recording Electronic (DRE) voting machines.

2.6.6 Remote Electronic Voting Systems

Despite the later predominance of of cryptography in the design of remote (and later polling place) voting schemes, initial approaches to remote electronic voting lacked cryptography as a mechanism for ensuring secrecy and accuracy properties and employed the telephone network to provide a vote communication channel [104]. Modern interest in remote electronic voting systems began with proposals for cryptographic voting schemes as discussed in Section 2.5.

A typical remote electronic voting system envisages the use of the Internet or similar network for communication. A setup consists of one or more voting system servers and a larger number of client systems, all of which are able to undertake cryptographic computations on a realistic time scale. Some remote voting schemes envisage client devices with considerably less computational power in order to provide greater mobility of voting [117]. A typical remote voting scheme employs one or more server applications implementing

election system functionality and a *pollster* software artifact which must be distributed to all voters. The voters install the artifact on their client personal computer (PC). To cast a vote, the voter informs the pollster of their choice in the election and the pollster then interacts with the vote server in order to cast a vote on the voter's behalf. Depending upon the implemented scheme, the pollster may also obtain proof of the success or failure of vote casting and report the result to the voter.

Remote voting systems are commonly vulnerable to the same violations of secrecy requirements as postal voting using paper ballots. Certain systems however, may limit some of the attacks on voter secrecy by preventing *massive coercion* [74].

The accuracy of remote electronic voting schemes is typically dependent upon the correctness of implementation of the pollster artifact and the honesty with which the pollster reports success or failure to the voter. As has been noted, designs of cryptographic schemes refer to the act of 'voter verification' of a vote casting process [88], whereas in fact the voter merely observes the results of verification presented by the pollster. From the perspective of the cryptographic scheme, the pollster *is* the voter. Such cryptographic schemes and their implemented systems are thus better described as "pollster verifiable".

One proposed mechanism is the use of multiple system vendors for a single cryptographic scheme. In such circumstances, a voter is able to choose from a range of client software implementations which may interact with remote election authorities in an agreed manner. Further, the voter may be able to choose different vendors for different operations (voting and checking for example). Unfortunately, this proposal does not satisfy the concern that a voter must understand the operations that are being performed on their behalf if they are to determine whether they have been cheated or not, or alternatively, trust some third party's investigation. Using cryptographic schemes, a non-expert voter cannot be satisfied for themselves that their vote has been counted correctly.

In terms of usability properties, REV systems are typically similar to DRE systems, since their user interfaces are configurable to the needs and abilities of voters. The user interface may provide the same constraints on vote casting as DRE machines in order to prevent

spoiled or inaccurate votes (with respect to voter intentions) being cast. Careful implementation of an REV system user interface should also permit specialist information technology access devices to interoperate with the pollster artifact. Pollster applications designed for other voting devices such as Personal Data Appliances (PDA) and mobile phones may be less flexible in terms of the presentation of choices, since the layout of options is constrained by the screen size and functionality of the device's user interface.

The US military recently attempted to provide overseas personnel with a remote electronic voting system for the 2004 Presidential Election. The project was cancelled due to general concerns with regard to Internet security raised by researchers requested to comment on the system [69]. Critics of the report, however, noted that the SERVE system would have replaced existing systems such as postal voting, or sending votes by fax to a election administrator [118]. Such existing systems were either difficult to operate within the time constraints of an election, or were demonstrably less secure than the proposed SERVE system.

2.6.7 Summary of Voting Systems and Technologies

The preceding section has discussed the various technologies typically employed in the implementation of voting schemes together with (where appropriate) the procedures with which they are commonly associated. The discussion provides details of the technology's properties with respect to secrecy, accuracy and usability requirements.

2.7 Conclusions

This chapter has presented a framework within which the various research efforts into voting systems (across numerous disciplines) may be presented and compared. Whilst numerous studies have presented frameworks for technologies [2, 53], cryptographic voting schemes [16, 135] and the deployment of voting systems in particular contexts [91, 134],

this work is novel since it presents an overview of the various efforts into voting systems, together with an explanation as to how they interact. At the most abstract level, the notion of a voting context is introduced with several common classes of voting contexts portrayed. Voting contexts provide a series of requirements to be captured by a requirements model and standards which in turn define the necessary properties to be achieved by voting schemes. Finally, voting schemes are implemented using a collection of voting technologies (paper ballot, personal computer, dedicated DRE machine etc.) and procedures (voter authentication and paper ballot counting, for example). In the proceeding chapters, the framework presented is used to investigate the potential for deploying alternative voting systems which achieve the requirements of the United Kingdom's public voting context.

Chapter 3

Requirements for UK Public Elections

Overview

The preceding chapter presented a survey of the existing research efforts in the field of voting systems, structured as a hierarchical framework. This chapter discusses a set of requirements for the UK public voting context, establishing criteria against which alternative voting systems for that context can be evaluated.

3.1 Introduction

A common approach to defining requirements for voting systems is to seek a global list of properties which a voting scheme (which is then implemented by a system) must achieve, for example Gritzalis [53]. In some cases, functional requirements may be derived from these [65]. Typically, such approaches assume that new voting systems will be employed in a public election context, for which the requirements are broadly similar. Initially, high level statements as to the requirements for a voting system are identified. These may be extracted from International Treaties on the agreed conduct for public elections, for example [17]. Birch and Watt have gone as far as to suggest that particular voting systems which

employ electronic technologies or permit vote casting in a remote context are inherently in conflict with the high level requirements expressed in international treaties and law [10]. However, this global approach is typically in conflict with the diverse requirements for voting systems in different contexts, as discussed in the previous chapter. A global statement of requirements for public elections will have difficulty in coping with particular requirements in specifc contexts, such as the variety of electoral systems employed and the impact the choice of electoral system has on the privacy of a voter.

In this chapter, an investigation of requirements is conducted for a voting system for the *UK public election context* only. As will be realised as the chapter proceeds, the requirements for this context are complex. The chapter will produce a statement of requirements for a new voting system which seeks to fulfill the UK government's goal of improving the experience and convenience of voting, in addition to the requirements applied to existing voting systems. Given the UK government's desire to enable 'multi-channel' elections, an initial requirement of a new voting system is that it must operates alongside the existing UK voting systems.

Public elections in the United Kingdom (UK) are regulated by Acts of Parliament, predominantly Representation of the People Acts, for example [120, 121, 122], although acts relevant to electoral registration are passed under other guises, for example [44, 112]. Parliamentary acts specify *electoral rules* and the powers that government ministers may employ in the administration of elections. Ministers powers include the ability to vary rules in order to conduct pilots of new technologies [122].

A particular feature of the UK contexts is that there is no requirement to authenticate voters when they attend a polling station or request a postal ballot for voting (except in Northern Ireland). To compensate for the lack of authentication, the UK requires instead that voting systems implement a vote tracing mechanism. The mechanism permits illegally cast votes to be removed from a collection of votes when identified so that the tally can then be re-calculated [121]. Whilst this approach to requirements has been criticised, notably by Jackson [68], the UK government indicated that it intends future electronic voting systems

to also implement this requirement [18]. As such, many technologies which strictly enforce voting privacy may be unsuitable for UK elections, if they are required to operate alongside existing systems.

3.2 Convenience Requirements

In addition to the legal constraints on the adoption of new voting systems in the United Kingdom, the Government has proposed the use of new voting systems as a means of improving the convenience and the experience of participating in UK public elections. The Government and the independent Electoral Commission have proposed employing alternative voting systems as a means of improving participation in UK public elections; for some recent elections turnout has dropped below 20% [132]. Whilst the UK government acknowledges that multiple factors are responsible for a decline in turnout to elections, the increased inconvenience of participating in voting on polling day (by attending a polling station) is considered to be of significance. The postal voting system has already been modified to increase the convenience of voting and the UK Government is investigating further alternative channels which permit votes to be cast out with a polling station.

R1: The voting system must allow a vote to be cast from an unsupervised location.

In order for a new voting system to increase convenience it should not require a large number of steps in order to cast a vote. Large complex sequences of interactions are likely to deter voters from completing a transaction. Both of the existing voting systems in the UK require just two interactions on behalf of a voter (once registered) - a request for a ballot paper and the act of vote casting.

R2: The voting system must minimize the number of interactions required to cast a vote.

A particular difficulty of implementing new voting systems is the potential for disenfranchisement of portions of the electorate because the voting system requires the use of interfaces with particular devices (a touch screen terminal, for example). Voters who cannot use the particular interface require assistance in the polling station, thus violating privacy requirements. A mitigation strategy proposed by the charity Scope and the Royal Society for the Blind is that multiple channels are offered for vote casting, in order that all voters are able to utilise at least one channel [133]. This is in contrast to the strategy adopted for US public elections in which attempts are made to ensure that a single voting system can be employed by all voters without assistance. This suggests that a voting scheme should operate consistently over multiple voting channels.

R3: The voting system must allow vote casting to occur via a range of channels in order to increase accessibility for a range of voters.

Coupled with the previous requirement is the need to ensure that the range of channels employed for vote casting are affordable for voters. Norris notes that the direct *cost of participation* is a factor in determining whether a voter will participate in an election [103]. If multiple channels are to be employed for voting then the channels must be affordable for voters in order to avoid disenfranchisement.

R4: The voting system must not require a voter to possess special purpose equipment in order to cast a vote.

The above discussion describes significant requirements applicable to the implementation of *new* voting systems only. In order to motivate the adoption of further voting channels, new voting systems must be demonstrated to fulfill requirements beyond those of existing voting systems (polling station or postal voting). The adoption of new voting systems is unlikely to occur unless a substantial benefit can be demonstrated. Further to the above requirements, a new voting system must also fulfill the requirements of existing voting systems in terms of accommodating electoral systems and fulfilling secrecy and accuracy requirements. Each of these categories of requirements are discussed below.

3.3 Electoral System

Elections in the UK are conducted using a variety of electoral systems. Elections to the Westminster parliament are conducted using SMSP, with one election for each constituency [84]. Elections to the European Parliament since 1999 are conducted using the closed list system. Elections to the Holyrood Parliament in Scotland and the Welsh assembly employ a mixed simple plurality and closed list system, in which the representatives of political parties elected on the list system is influenced by the election of representatives for constituencies [125]. Elections to the Stormont assembly in Northern Ireland and local elections in Scotland and Northern Ireland use (STV). Local elections in England are conducted using a multi-member simple plurality system. The diversification of electoral systems is a relatively recent phenomenon and is one motivation for the investigation of new voting systems (electronic counting, for example) which would automate some of the new tasks [145, pp4]. Voting systems implemented for public elections in the UK will likely need to be suitable for each of these contexts in order to avoid unnecessary duplication.

As noted in the introduction to this chapter, the UK currently employs five electoral systems; referenda, SP, Closed List, STV and mixed-member. Given the types of electoral systems employed, several factors which would need to be considered in other voting contexts are not relevant here and so the requirements model assumes their absence:

- All electoral systems consist of only one round of voting. Consideration does not need to be made for transitions between successive rounds of voting.
- All voters participating in a election do so under a single franchise.
- All votes are of equal weighting, therefore weighting of votes or options does not need to be considered.

The diversity of electoral systems employed in the UK context requires a voting system to accommodate several types of proposal.

The referenda, SP, Closed List and STV electoral systems employed in the UK utilise two types of proposal: unordered and ordered i out of j selection of options.

3.3.1 Unordered Selection of Options

Referenda, SP, Closed List require a voter to select i unordered options out of j options on a proposal, where j is the number of available options and i is the maximum number of options that may be selected by a voter.

A proposal of this form may be denoted as:

- For Referenda, exactly two option descriptions are specified as “accept” or “reject”.
- For SP electoral systems each option description is of the form:

$$\{< \text{candidate} >, < \text{party} >\}$$

- For Closed List electoral systems each option description is of the form:

$$\{< \text{party} >, \{< \text{candidate}_1 >, < \text{candidate}_2 >, ..., < \text{candidate}_{S_j} >\}\}$$

  Where S_j denotes the number of candidates in the list.

A vote constructed from an unordered proposal is dependent on the option descriptions specified by the proposal and by the maximum number of options which may be selected. A vote is denoted as a *collection* of unordered selections from the available option descriptions on the proposal.

R5: A voting system must permit voters to express an unordered selection of options within some maximum as a vote in a Referendum SP or Closed List electoral system.

3.3.2 Ordered Selection of Options

An ordered selection of options is defined as i ordered options out of j options on a proposal where j is the number of available options and i is the maximum number of options that may be selected by a voter. The model of the ordered proposal type is identical to that for an unordered proposal except:

- the set of selections from a proposal must be treated as an ordered list of selections.
- For STV the maximum number of selections is equal to the number of options on a proposal for an execution of the electoral system.
- For the alternative vote electoral system used in the UK to elect the Mayor of London, a voter may select up to two options.

R6: A voting system must allow a voter to express a vote as an ordered selection of options within some maximum defined by the electoral system.

3.3.3 Mixed Member

In addition to the electoral systems which employ a single proposal type, the mixed-member electoral system requires that a voter be provided with two proposals, one for use in an SP electoral system tally function and the other for use in a Closed List electoral system, the result of which is affected by the results of several SP elections.

R7: A voting system must allow a voter to express two votes in a mixed member electoral system, as two unordered votes.

3.4 Secrecy Requirements

The introduction to this chapter noted the particular secrecy requirements which apply to the UK public election context. Due to weaknesses in the existing voting system infrastructure with regard to accuracy, the UK does not provide for absolute privacy of votes, in contrast to most other election contexts. This section discusses the particular secrecy requirements of the UK public election context.

3.4.1 Threat Model

The UK public election voting context implicitly employs two threat models for the voting systems employed. In both threat models, an attacker is assumed whose goal is to learn the association between a vote and a voter. The attacker requires this information to conduct other attacks, for example, vote buying or voter coercion, in which an attacker is able to improve the share of votes cast for a desired option. For polling station voting systems, the voter is assumed to be in collusion with the attacker, that is the voter will attempt to collaborate with the attacker to demonstrate their choice of option in order to gain some advantage. The paper ballot/polling station voting system is thus constructed with consideration to this threat, the system being designed such that the attacker cannot observe the voter's actions with the polling station and the voter cannot prove their choices to the attacker afterwards.

Conversely, a second threat model is employed for secrecy requirements of the postal voting system in which the voter is assumed to accept some responsibility for the privacy of voting. For remote voting systems, the voter is assumed to not co-operate with an attacker in order for a reasonable threat model for the voting system to be constructed. This more relaxed threat model is necessary since a voter employing a remote voting system is able to trivially violate privacy requirements by voting in the presence of the attacker. In order to fulfill other requirements of voting systems, convenience and mobility for example, the more relaxed definition of privacy may be employed in which it is assumed that the voter

simulates the conditions of the polling station during vote casting. In other voting contexts, in which the behaviour of the voter may not be assumed the polling station model may be the only appropriate threat model to adopt.

Section 3.2 discussed the motivation requirements of the voting system, that is, the need for the system to provide greater convenience and mobility for voting than the existing voting system employing paper ballots in polling stations or cast via the postal system. The implication for the voting system is that remote voting is anticipated as a solution to the motivation requirements and as such the remote voting threat model should be employed for the voting system investigated here.

Two particular aspects of secrecy are of interest for UK public elections - the association between votes and voter (voter privacy) and the secrecy of the result or partial result of an election prior to the end of voting.

3.4.2 Voter Privacy

As noted previously, a voting system which enhances convenience for voters must also operate alongside the existing UK electoral infrastructure and voting systems in order not to inconvenience voters who prefer existing voting systems. The existing infrastructure provides for only weak authentication of voters both during registration and later prior to voting. As such, the existing UK voting system employs a vote tracing mechanism, which under exceptional circumstances allows a vote to be associated with a voter by an election authority. The association is permissible when it is demonstrable that the identity used to cast the vote was fraudulent and as such the vote is invalid.

R8: An external observer of the voting system must not be able to associate a vote with a voter except when authorised by an election court judge, in parallel to the existing UK voting system.

The definition adopted is similar to that of the CESG security study statement of requirements [19]. The requirement excludes anonymity as a property of a potential voting system, since a requirement of UK public election voting systems is that a list of participating votes is published (the marked roll).

3.4.3 Tally Secrecy

A requirement of the UK public election context is that the aggregate of votes (tallies) are not published prior to the close of voting with the intention that those casting their votes later are not influenced by votes cast earlier during the election in their choices. For the UK, with multiple voting systems being employed to collect votes, all systems are required to prevent early disclosure of results. The following requirements of voting systems for the UK context are made:

R9: An external observer of the voting system must not be able to learn the value of a vote prior to the end of voting.

R10: An external observer of the voting system must not be able to learn the aggregate or partial aggregate of votes prior to the end of voting.

The requirements do not restrict observers learning the aggregate of votes once voting is complete and indeed, observers are not prevented from learning the value of individual votes provided that the association between votes and voters remains secret.

3.5 Accuracy Requirements

Section 2.3.1 discusses the scope of accuracy requirements for voting contexts. This work adopts the approach of Schneier in that ensuring accuracy in voting systems is considered as an end-to-end problem of the voting system, from voter intention to tallying of results.

The requirements for accuracy in the UK public election context with respect to existing voting systems are discussed below.

An initial requirement of accuracy is to ensure that votes are cast by eligible voters only. This requirement must be compatible with the existing UK voting system. The requirement therefore does not ensure that votes are cast only by eligible voters securely authenticated in some manner. Rather, that if votes *are* cast fraudulently and the fraud is detected, the invalid votes may be removed from the collection of cast votes and the tally recomputed.

R11: The voting system must permit a vote to be traced to a voter identity in conditions comparable to the existing UK voting system.

Related to the previous requirement, it is required that the list of voter identities used to participate in the election should be verifiable by both the owners of the identities and external observers. This does not violate the secrecy properties of the UK public election context which require voting privacy rather than voter anonymity.

R12: A list of voters participating in an election must be published after the announcement of results.

There is potential in the near future for the above requirement to be modified such that a list of participating voters is updated and published during vote casting. Discussion of this proposal have occurred in reports published by the Electoral Commission [43].

In order to ensure accuracy a voting system must record the intentions of a voter. This implies that the voter is able to verify in some manner that the voting system has functioned correctly in this respect. The two requirements to fulfill this purpose are:

R13: The voting system must accurately record the intentions of the voter, where those intentions are legal.

R14: The voting system should permit voters to confirm their choice at some point prior to final commitment to the vote.

The existing UK voting system permits visual inspection of paper ballots for those voters without visual impairments.

Once votes are collected, they must be stored such that modification is prevented prior to tallying. This requirement is necessary in the UK context because votes are not tallied as collected.

R15: The voting system must store all votes cast without modification prior to tallying.

Finally, the tally of votes must be accurate with respect to the store of votes cast.

R16: The tally of votes must be accurate with respect to votes stored.

3.6 Summary of UK Requirements

This chapter has surveyed the requirements for a voting scheme for the UK public election context in terms of the electoral systems which a scheme must accommodate, the secrecy requirements with respect to each electoral system, and the accuracy requirements with respect to each step of the voting process as modelled in Section 2.3.1. Further, a discussion is provided of the usability and acceptability requirements of the context, most notably the need for any new scheme and system to operate within the context of the existing UK public election infrastructure.

In summary, the requirements for the UK public election context are as follows:

R1: The voting system must allow a vote to be cast from an unsupervised location.

R2: The voting system must minimize the number of interactions required to cast a vote.

R3: The voting system must allow vote casting to occur via a range of channels in order to increase accessibility for a range of voters.

R4: The voting system must not require a voter to possess special purpose equipment in order to cast a vote.

R5: A voting system must permit voters to express an unordered selection of options within some maximum as a vote in a Referendum SP or Closed List electoral system.

R6: A voting system must allow a voter to express a vote as an ordered selection of options within some maximum defined by the electoral system.

R7: A voting system must allow a voter to express two votes in a mixed member electoral system, as two unordered votes.

R8: An external observer of the voting system must not be able to associate a vote with a voter except when authorised by an election court judge, in parallel to the existing UK voting system.

R9: An external observer of the voting system must not be able to learn the value of a vote prior to the end of voting.

R10: An external observer of the voting system must not be able to learn the aggregate or partial aggregate of votes prior to the end of voting.

R11: The voting system must permit a vote to be traced to a voter identity in conditions comparable to the existing UK voting system.

R12: A list of voters participating in an election must be published after the announcement of results.

R13: The voting system must accurately record the intentions of the voter, where those intentions are legal.

R14: The voting system should permit voters to confirm their choice at some point prior to final commitment to the vote.

R15: The voting system must store all votes cast without modification prior to tallying.

R16: The tally of votes must be accurate with respect to votes stored.

In the next chapter of this thesis, a class of pollsterless voting schemes is investigated with respect to their common properties fulfilling the usability and acceptability requirements of the UK context. The chapter also notes the flaws in existing proposed pollsterless voting schemes with respect to secrecy and accuracy which need to be corrected before the identified requirements are fulfilled.

Chapter 4

Pollsterless Remote Electronic Voting

Overview

This chapter describes voting schemes which adhere to the *pollsterless* property and discusses the benefits of employing pollsterless schemes for public elections. Two particular schemes are described, with the useful properties and flaws of both discussed. The chapter concludes by noting the potential for pollsterless schemes for public election if a suitable scheme could be identified which observes the properties of both the Malkhi et al and CESG schemes.

4.1 Properties of Pollsterless Schemes

The term *pollster* in reference to electronic voting schemes, was first noted by Malkhi et al by referring to the software and/or hardware artifact that participates in a voting protocol on behalf of the human voter [85]. The pollster is necessary to perform the cryptographic operations that are typical of most remote voting schemes which the human user is incapable of performing for themselves. Separately, Rivest has noted that from a protocol perspective, the pollster *is* the voter in remote cryptographic voting schemes, rather than

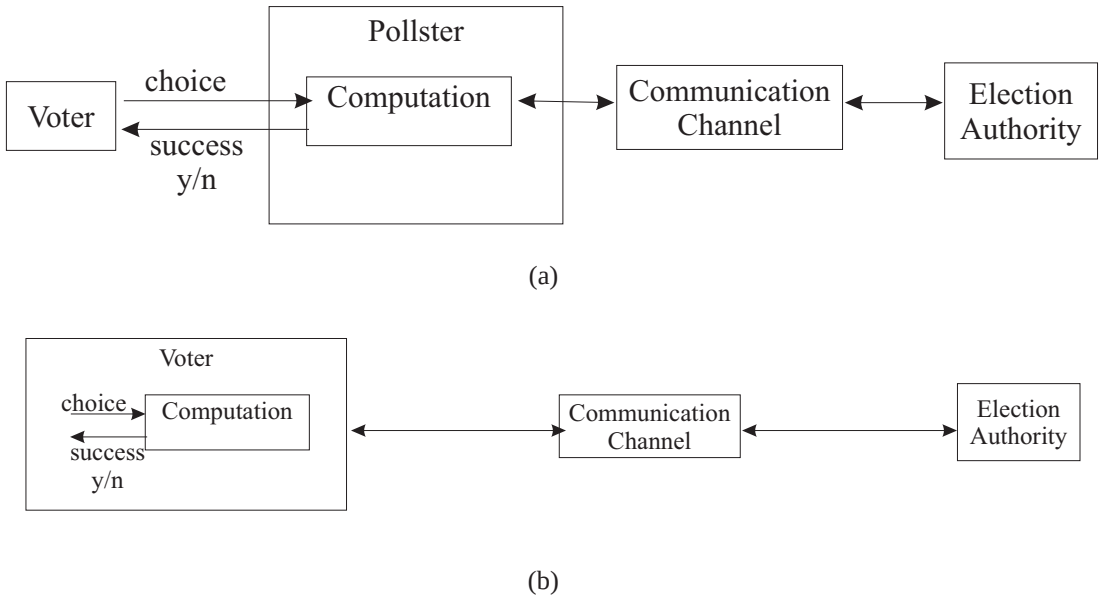


Figure 4.1: Pollster and pollsterless electronic voting schemes. Figure 4.1(a) illustrates schemes which employ a software artifact to conduct cryptographic computations on behalf of the voter. The voter submits a choice to the pollster which interacts with the election authority on behalf of the voter. Once the interaction is complete, the pollster indicates to the voter whether voting was successful or otherwise. Figure 4.1(b) illustrates a pollsterless scheme in which the voter performs computations directly, whilst the pollster relays messages between the voter and the election authority.

the user [88], comparing electronic voting via a computer to the practice of proxy voting using paper ballots. As such, the human voter is required to trust the pollster to record their wishes accurately and operate correctly on their behalf during the execution of the protocol. If given suitably detailed instructions, many voters may well be able to perform the necessary computations given time, However, such an approach would be unlikely to improve convenience for the voter.

Conversely, *pollsterless* voting schemes are designed to dispense with the need for the software artifact to perform computations entirely, through the use of computations for the client that are sufficiently simple that they can be completed by the voter directly. Figure 4.1 illustrates the difference between schemes which employ a pollster to perform computations and communication and pollsterless schemes where the voter interacts directly with a communication channel. Pollsterless schemes have several useful properties:

- The protocol can be executed on a variety of simple networked electronic devices. Cryptographic voting schemes assume the voter either possesses a dedicated hardware software artifact (provided by an election authority, for example) or a personal laptop or desktop personal computer on which special purpose software is executed in order to cast a vote. Pollsterless schemes may be implemented using a variety of devices for vote casting which lack the capability of performing cryptographic operations. Such devices range from relatively powerful mobile phones communicating via SMS text messaging, to the use of touch tone telephony in the home.

  Although pollsterless voting schemes remove the role of interpreting a voting protocol from the software intermediary to the voter, this does not necessarily mean that more sophisticated devices may be employed to improve usability or to address highly specific needs of particular voters. Indeed, the use of pollsterless voting schemes has the potential to allow more sophisticated devices to be used to improve usability for voters compared with cryptographic schemes. A far greater range of interfaces may be added to the scheme that do not perform any intelligent computation on messages received, but instead enhance the message understandability for the voter.

- Verification of the correct execution of the voting protocol can be performed directly without the need to assume the correct operation of the cryptographic pollster, if the protocol is designed to be voter verifiable. As discussed in Section 2.5, a common feature incorporated in cryptographic voting schemes is that the voter is able to independently verify that their own vote has been counted. However, as noted above, the human voter does not directly participate in cryptographic voting schemes, rather they relate their preferences to the pollster which acts on their behalf. Such schemes are thus better described as *pollster verifiable*, since the pollster will verify the correct execution of the protocol and then report back the result to the voter. The voter is therefore required to trust that the pollster software is itself operating correctly and reporting back honestly. This situation is particularly problematic where the pollster software is provided by the same vendor or organisation that implements the

election authority. A possible mode of attack on the system is for the pollster to be implemented to not report back errors. For *pollsterless verifiable* schemes, the voter directly verifies that the scheme's protocol has executed correctly without the need to trust the correct operation of software that may not operate in their interests. A counter argument to this problem is to advocate open protocols for voting systems in order to permit a range of client pollsters to be implemented and offered to voters. Although open protocols and public inspection of source code is to be encouraged, this approach does not mitigate the risk that a voter will be offered a corrupted pollster to operate on their behalf by an attacker.

- The limited capabilities required of the client voting device has the potential for improving the anonymity of a pollsterless scheme. Voters are not required to use devices associated with themselves for voting, instead using any suitable communication device from their own geographic location.

The advantages of pollsterless voting schemes (flexibility and mobility of voting channels together with the removal of a voter's dependency on the correct operation of software provided by the vendor), suggest that such schemes present considerable potential advantages over conventional cryptographic schemes. The schemes are of particular interest to the UK public election context, where the UK government wishes to increase turnout by improving the convenience of participation. However, the ability to leverage the potential advantages is dependent on the precise details of the schemes and also of their implementation.

Two proposed pollsterless electronic voting schemes are presented below. An overview is provided for the motivation of each scheme; that is the context for which the scheme is proposed, together with the mechanism by which votes are cast and aggregated. A discussion is then presented on the properties and associated flaws of the two schemes. The discussion illustrates the design considerations which influence the class of pollsterless voting schemes presented in the next chapter.

4.2 Malkhi et al's Scheme

Malkhi et al, who first proposed the notion of pollsterless voting schemes, suggested the use of *advanced check vectors* as a computational basis for their implementation. The technique employs the use of two two vectors V and B each held by a different participant, per secret s, known by both, for which $VB = s$. One participant may prove to the other that it knows s by revealing the vector it possesses.

An outline of the scheme is provided below, although the original paper is recommended for a fuller description [85]. The scheme proceeds in the three phases common for voting schemes; initiation, voting and tallying. The system assumes the prior establishment of *secure, anonymous channels* between voters and the election authorities.

The following definitions are introduced:

- The protocol participants: Dealer, Intermediary, and a Receiver. The Dealer is responsible for initialising the election by distributing credentials consisting of pairs of check vectors for each option. The Intermediaries act as voters by casting votes using credentials. Finally, the Receiver act as a Tallier of cast votes.
- A security parameter b, which specifies the lengths of Vectors employed in the protocol.
- A set of s meanings, denoted S, one for each candidate in an election. Let n denote the number of choices in the election.
- Pairs of voting vectors V_0 and V_1 both with meaning s, in which s refers to a voter's choice. Each voter is issued with a pair of vectors for each option available for the proposal.
- Pairs of check vectors, denoted B_0 and B_1.

Figure 4.2 illustrates the three phases of the protocol between the Dealer, Intermediary and Receiver.

4.2.1 Initiation

The Dealer delivers sets of pairs of vectors, $\forall_{1\leq k\leq n}\{V_{k,0}, V_{k,1}\}$, to each intermediary together with n secret meanings s (one for each vector pair). The Dealer also sends sets of pairs of check vectors $\forall_{1\leq k\leq n}\{B_{k,0}, B_{k,1}\}$ to the Receiver, together with n secret meanings s (one for each vector pair).

The work also provided the details of a scheme by which the setup may be conducted via an anonymous multi-party computation (AMPC), in which m dealers each only know an additive share of each of the coordinates of a generated vector V. The m dealers collaborate in the AMPC to simulate initiation as in the single dealer case, except that a single dealer cannot know the value of a complete V value.

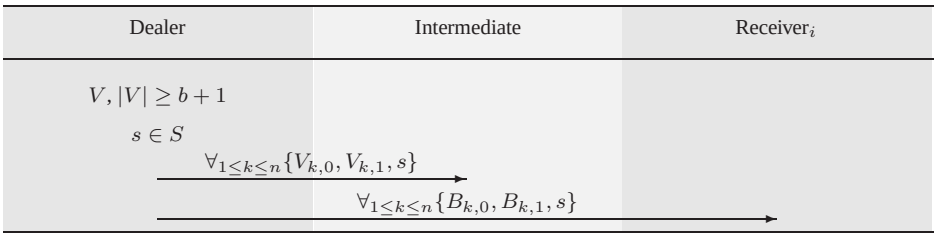
4.2.2 Pre-Voting Verification

Prior to the voting phase, the voter sends one of their voting vectors (chosen at random from the set of pairs of vectors for the election) to the Receiver. The Receiver then returns to the voter the Check Vector of the *neighbouring* vector to that sent. The voter then confirms that the product of the neighbouring vector and the check vector is equal to s. The revealed voting vector is then invalid for voting. The purpose of this check is to confirm that the Receiver is the appropriate entity to send a real vote vector to.

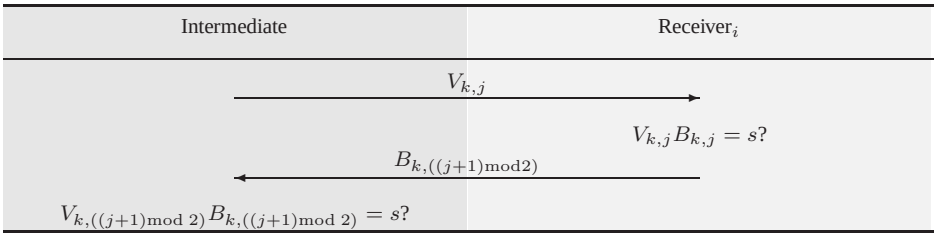
4.2.3 Voting and Tallying

In order to cast a vote, the Intermediary (the Voter) sends a Vector V to a Receiver (the Tallier). The Receiver computes $VB = s$, using the appropriate B vector for the received V vector.

Protocol Initiation:



Pre-Voting Verification:



Voting (assuming for same candidate as tested during verification):

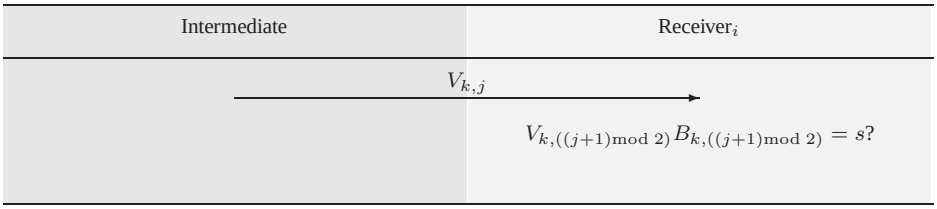


Figure 4.2: Initiation, pre-voting verification and voting of the Malkhi et al pollsterless scheme. A Dealer distributes vectors to Intermediates (Voters) and to a Receiver (the Tallier). The Intermediate may perform pre-voting verification using the spare credentials provided by the Dealer. Finally, the voter votes using the unused voting vector provided by the Dealer for desired secret s.

4.2.4 Comment

Whilst the scheme reduces the computational load for voters, there is still a considerable amount of computation for the voter to perform in order to verify that a vote has been correctly tallied. Commentary on the scheme within the published paper notes that the voter is required to perform a considerable amount of manual computation, even with the aid of a pocket calculator and that further refinements would be required prior to the scheme's practical use. In addition, the scheme cannot be argued to be truly voter verifiable, since the mechanism described provides a mechanism for the voter to determine authenticate the remote Tallier, but not to ensure that the Tallier is not corrupt.

Disputes, disruptions or delays may arise when voters are unable to perform the vector computation accurately, even though the correct check vector has been received. Pieters has suggested (based on pilots of another voting scheme implementation) that voter verification activity that result in a voter incorrectly perceiving an election authority as having cheated can reduce voter confidence in the result [110]. In this sense, voter verifiable voting schemes may in fact *reduce* voter confidence in the result of an election, if the verification process is complex and prone to error. The high occurrence of false positives during error detection suggests to external observers that the system is under sustained attack or is attempting to cheat at least a proportion of voters.

4.3 The CESG Study Scheme

In 2002, the then Communications and Electronics Security Group (now simply CESG)[1], published a security study of electronic voting, commissioned by the Office of the e-Envoy [18]. The initial study comprised a survey of existing works in electronic voting, a security requirements documents for electronic voting employed for public elections held in the UK and a proposed security mechanism for vote casting over multiple channels. Given the significance of this scheme proposed for UK elections, the main aspects are discussed

[1]The commerical arm of the UK Government's electronic monitoring agency GCHQ.

here, together with the corresponding flaws from the perspective of requirements for voting systems in the UK context. An overview of the scheme allows for comparison to be made with the modified CESG (mCESG) scheme presented in Chapter 5.

4.3.1 Voting Credentials

Generation of voting credentials is implied rather than well specified in the original CESG security study, although the structure of the credentials is detailed. The study does refer to the use of secure one-way hash functions for the purpose of generating voting credential values. Such one-way functions are of the form:

$$f_k : p \rightarrow c$$

where a publicly known function f is parameterised by a secret key k and applied to a plain text value p, resulting in a ciphertext c. The study suggests the use of a keyed cryptographic hash function to generate credentials. It is not clear from this choice whether the scheme is intended to use different key values for the generation of the various values of the voting credential, although this is assumed in the following description. An alternative approach not adopted in the study would be to use purely random values for the generation of credential values, in order to provide for unconditional secrecy.

Figure 4.3 illustrates the voting credentials envisaged for the CESG scheme. The credentials consist of a conventional polling card, currently delivered to all registered voters for UK elections. The polling card contains information on polling station location and the time and date at which the station will be open for voting. The polling cards are used to assist identification ,but not authentication, of voters in the polling station. In addition to the usual information, the polling card is supplemented by electronic voting credentials, consisting of a Voter ID (VID) value, a list of candidate identifiers, a corresponding list of Personal Candidate Identification (PCIN) values and a corresponding set of Expected Response ID (RID) values. To produce the credentials, an unpublished Candidate ID (CID)

John Doe
Voter ID Number: 1234567890123456

Candidate	Party	PCIN	Expected Response
Alice	AliceParty	3344	000999
Bob	BobParty	4455	111888
Charlie	CharlieParty	6677	222777
Dave	DaveParty	8899	333666
Intentionally Spoilt Ballot		1100	444555

Figure 4.3: Voting credentials delivered to the voter in the CESG scheme, taken from [18]. The added voting credentials consist of a Voter ID (VID); a set of candidates; a set of corresponding Personal Candidate Identification Numbers (PCIN) and a corresponding set of Expected Response IDs (RID).

value is generated once from the candidate's description.

For each credential, the VID value is generated using the voter's name and address as input data. Each PCIN value is generated from the corresponding CID and the voter's generated VID value. Each RID value is generated using the VID:PCIN concatenation as input data:

$$\begin{aligned} f_k(\text{candidate}) &\rightarrow \text{CID} \\ f_k(\text{voter}) &\rightarrow \text{VID} \\ f_k(\text{VID:CID}) &\rightarrow \text{PCIN} \\ f_k(\text{VID:PCIN}) &\rightarrow \text{RID} \end{aligned}$$

Credentials are assumed to be delivered to voters via a secure channel, with the example of printing the credentials on secure payroll stationary and delivered by post given in the study. Alternative channels may be the use of secure email integrated with a Public Key Infrastructure.

4.3.2 Vote Casting

The voter is able to begin vote casting using any available channel once the voting credentials arrive. To cast a vote, the voter sends a message consisting of their VID value and the PCIN value of their chosen candidate. Assuming the voter sends a correct message, an RID value is returned to them via the same channel as the vote message. The RID value is then compared to the RID of their chosen candidate to confirm that the vote has been received by the Election System. For example, consider that the voter chooses to vote for Alice using the credentials illustrated in Figure 4.3. To cast a vote, the voter composes the SMS message:

$$\text{Voter} \ : 012345678901234563344 \rightarrow \text{Election System}$$

and sends this to a Gateway number indicated on the credentials. The Election System then generates the RID value that corresponds to this vote in the same way as for the voting credentials and sends this back to the voter:

$$\text{Election System} \ : 000999 \rightarrow \text{Voter}$$

The voter then confirms that the correct RID value has been computed and received. Note that this step is necessary to ensure that the vote, likely sent on an insecure channel, is not intercepted or modified prior to receipt by the Election System. When this response step does not occur, or the RID values do not match, the voter contacts the Election System to cancel the interaction and is required to vote in a polling station instead. Note the implication of this fall–back measure is that the CESG scheme is intended to complement rather than replace the existing paper ballot/polling station voting system for UK elections.

4.3.3 Election System Architecture

Figure 4.4, extracted from the original security study document, illustrates the Election System envisaged for the scheme [18, pp. 54]. The system comprises a set of distinct inter-

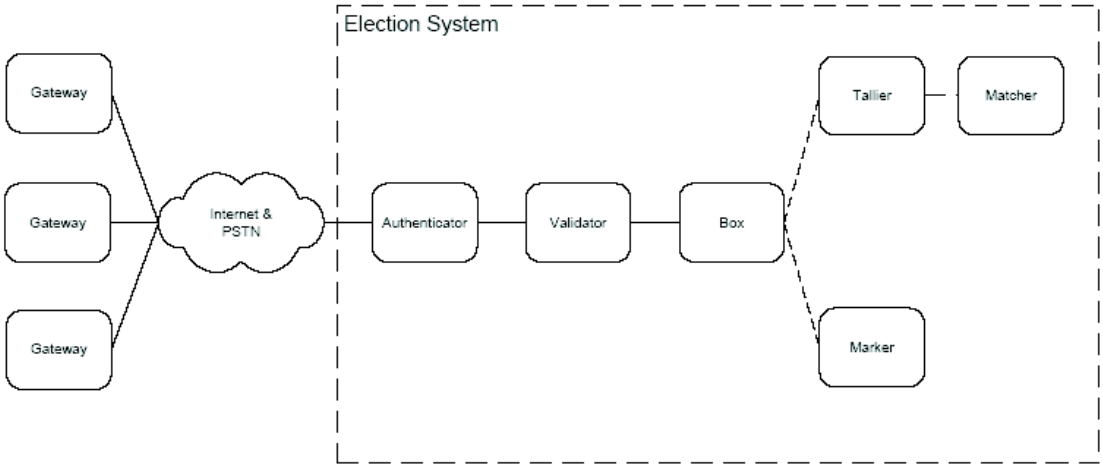


Figure 4.4: Architecture of the Election System proposed by CESG for vote collection and tabulation [18]. The diagram indicates the path of a vote from the voter, via a gateway to the Election System domain.

nal modules performing dedicated functions. Votes are collected from a series of hosting *gateways* representing voting channels (Internet, SMS or digital television for example) and forwarded to the Election System itself. To process votes, the Election System modules need the same secret key k used to generate the voting credentials. Whilst the study does not specify a participant responsible for generating credentials, it is implicit that since the Election System uses the key to process votes, the Election System is also responsible for generating credentials.

Votes are initially processed by an *Authenticator*, which, given a VID:PCIN ballot message, determines that for the VID substring of the ballot message was generated for a voter in the current election. If the ballot message is authenticated, an RID is generated for the whole ballot message using the same function as for the generation of credentials:

$$f_k(\text{VID:PCIN}) \rightarrow \text{RID}$$

and the RID is passed with the VID to the Validator module. If the vote is not authenticated, then an error message is generated and transmitted to the voter. The Validator determines

whether the RID value is valid for the provided VID value. If this is the case, the whole ballot message stored by the Authenticator and the generated RID value is passed to the *Box* module which acts as an electronic ballot box. If the RID generated is not valid, an error message is generated and transmitted to the voter.

On the close of poll, the Box module sends the contained vote message VID:PCIN and RID values to the *Marker* and *Tallier* modules. The Tallier recovers the anonymising CID values from the VID:PCIN concatenation. Given that the PCIN is the result of applying the one-way secret hash function to a concatenation of VID:CID values, this description implies that either the Tallier possesses a look–up table for obtaining CID values for corresponding PCIN values; or that for each vote, the Tallier applies the hash function to each VID:CID concatenation until the correct PCIN results. In either case, the Tallier then produces a tally of occurrences for each CID value and passes these to the *Matcher* module. The Matcher performs an association between anonymous CID values and candidate descriptions in order to obtain the tallies for each candidate. Again, the method by which the Matcher recovers the candidate descriptions is unclear, but the architecture implies that the Matcher is either originally responsible for the generation of the CID values, or that the association between CID and candidate description is provided to the Matcher by some external entity during the matching phase.

Simultaneously to the tallying process, the *Marker* module recovers voter identities from the VID values passed to it from the Box module. This list of voter identities is a requirement of the UK voting context in order for candidates to check that voters were not *personated* during the election.

4.3.4 Discussion

The scheme proposed by CESG was released for consultation as part of a wider study of the requirements for electronic voting for UK public elections. Whilst the consultation responses guardedly welcomed the requirements proposed, the scheme received a sub-

stantial amount of general criticism without identifying specific flaws in the scheme itself [46, 50, 93]. The responses also tended to concentrate their criticisms on the general notion of remote electronic voting itself, from a social perspective of maintaining polling station attendance, for example. Whilst these criticisms are valid, they are unfortunate in that the authors of the scheme are not provided with specific instances of flaws correctable through modification of the scheme itself.

Separately, a more detailed study of the scheme identified specific flaws and proposed corrections [138] resulting in the mCESG scheme described in Chapter 5. The flaws in the CESG scheme identified are described here to justify the significant adaptations made in the mCESG scheme.

4.3.4.1 Monolithic Election System

Figure 4.4 illustrates the architecture of the election architecture envisaged for the CESG scheme. In the diagram the functionality of the architecture is divided into distinct modules as described in Section 4.3.3, with the implied intention that each module only stores the necessary information to perform its task. However, the description of credential generation and ballot message handling in the study suggests that the credentials are generated by the Election System itself, implying that all modules have access to the voting credential information. Whilst the design of the Election System may modularise functionality, the separation of possession of information is not enforced. From the voter's perspective the Election System is a single monolithic structure regardless of the internal division of responsibility. This monolithic, necessarily trusted, architecture presents several possibilities for attack should the system become corrupted.

- Since the Election System knows the association between all voter identities, VID values, candidate descriptions, CID values and the relevant VID:PCIN ballot messages, a corrupt Election System is able to leak to an attacker the association between participating voters and cast votes. The privacy of a vote is dependent on the security

of a single domain.

- The practice of adding (stuffing) extra paper ballots to a ballot box in a polling station by insiders in collusion with particular candidates, allows results to be altered. A corrupt CESG Election System with possession of all the voting credentials of all the voters is able to add extra ballot messages using the credentials of those voters who do not participate in the election. Detection of such a practice would rely on inspection of the marked roll by voters who had not participated in the election, although such voters would have no evidence with which to demonstrate they had not cast the votes recorded on their behalf.

- As well as using the credentials of existing voters who do not participate in the election, an Election System which has control of the registration of voters may also add extra identities to the register and generate credentials for these 'fictitious' voters. This form of attack has already occurred in the UK in relation to the registration of non-existent voters for postal votes, and the use of the CESG system would automate this process for a corrupt election system.

The composition of multiple functions of the voting process into the single Election System domain consequently provides attackers with a single point of failure to be targeted. Voters are required to trust that the Election System both processes votes honestly and also maintains the secrecy of the votes that are cast.

4.3.4.2 Lack of Verifiability

A goal of the CESG scheme is to provide reassurance to the voter that their vote has been collected by the Election System. Whilst the protocol achieves this through the use of RID values sent to voters, there is no reassurance that the Election System then accurately processes the received votes by accurately translating the received VID:PCIN combinations into the correct candidate description. The RID values confirm only that the ballot message has not been intercepted by a third party.

The lack of *vote verifiability* introduces two further vulnerabilities for the CESG scheme.

- Most significantly, the voter cannot prove to either the Election System or an independent third party that they did not send a ballot message representing a particular vote to the Election System, or that they cast a vote at all. Further, the voter is unable to detect whether the Election System is behaving correctly or not, since the vote cast is not identifiable in the aggregation of results published by the Tallier module at the end of an election. This prevents the voter from usefully using the RID value received from the Election System, for example, to correct deliberate errors made by a corrupt Election System participating in ballot box stuffing.
- Similarly, an Election System cannot convincingly refute allegations that it received but did not process ballot messages sent by a malicious voter. This permits the malicious voter to undermine confidence in the result of an election by alleging that it cast a vote, received an RID from the Election System (which the voter is able to fake using the voting credentials) but was not entered on the marked roll list of participating voters. The CESG scheme is therefore vulnerable to manipulation by either corrupt voters or a corrupt Election System.

A common approach of cryptographic electronic voting schemes is to replace the reassurance obtained from the public counting of paper ballots with mathematical mechanisms that demonstrate to a voter that their vote has been included in the tally. As described, the CESG scheme does not provide this mechanism and as such the voter is dependent on the correct operation of the Election System, whilst the system is vulnerable to spurious allegations of corruption.

4.3.4.3 Electoral System Limitations

A feature of the CESG scheme is that it is intended for elections as conducted in England and Wales prior to 2002. As a consequence, the scheme does not address the added complexities of communicating a vote to an Election System using an ordinal electoral system

such as Single Transferable Vote, where voters are obliged to rank their candidates in order of preference, rather than indicate a single choice. A naive implementation of CESG for ranked votes would require a different PCIN value for each possible combination and ranking of candidates, resulting in

$$\sum_{k=0}^{n} \frac{n!}{(n-k)!}$$

potentially different values (all permutations of all subsets of candidates). Therefore, the CESG scheme is unsuitable for use in its original form in elections where ordinal electoral systems are employed. In the United Kingdom, this would include elections to the Stormont Assembly in Northern Ireland and to Unitary Authorities in Scotland from 2007.

4.3.5 Local Authority Pilots

During the 2002 and 2003 local elections in the UK, the CESG scheme was used by several vendors as the security mechanism for a variety of provided voting channels [42]. The use of the scheme was not mandatory, but was recommended by the Office of the Deputy Prime Minister's (ODPM) statement of requirement for the project [56]. Future pilots which had been planned for 2006 [105] in England and Wales are currently on hold due to government uncertainty regarding the benefits and costs of new voting channels [55]. The discrepancies concerning pilots of postal voting at local elections in 2004 may have influenced the government's decision to cancel all pilots [87], at least for the 2006 elections.

4.4 Conclusions

This chapter has discussed desirable properties of pollsterless voting schemes. Pollsterless schemes, which dispense with the need for a client software artifact to act on a voter's behalf (a pollster) are advantageous because simpler technologies may be employed for vote casting. In addition, if the scheme allows a voter to verify the presence of their vote

in a tally, then verification occurs without the need to trust the pollster to obey a voter's intentions. The two schemes described thus far achieve some of the desirable properties of pollsterless schemes. The Malkhi et al schemes provides verifiability, but the voter is required to perform vector calculations. The CESG scheme provides a simple voting mechanism, but which is however non-verifiable. A solution to this circumstance would be a pollsterless voting scheme which united the desirable properties of the Malkhi et al and CESG schemes.

Chapter 5

The mCESG Pollsterless Remote Electronic Voting Scheme

Overview

In Chapter 4 the notion of pollsterless remote electronic voting schemes was introduced. Existing approaches to pollsterless schemes were discussed along with identified flaws. In this chapter, the CESG scheme is formalised in order to provide a basis for modification and adaptation. A novel scheme is presented which corrects the flaws of the CESG pollsterless scheme by providing for voter verifiability and improvement to the protection of voter secrecy. The proposed scheme (modified CESG, or mCESG) retains the desirable properties of mobility and channel independence. Several adaptations of the mCESG scheme are also presented to illustrate its flexibility for implementation in a variety of voting contexts and that mCESG in fact represents a class of pollsterless voting schemes.

5.1 Introduction

The mCESG scheme is a novel remote voting scheme derived from a security mechanism for electronic voting proposed by the UK government's Communications and Electronics Security Group (CESG), the commercial arm of the GCHQ agency. The mCESG scheme provides additional desirable properties for UK elections not present in the original scheme, whilst retaining advantageous pollsterless properties.

The first section of this chapter provides a formalisation of the CESG scheme outlined in Section 4.3. As noted, the CESG scheme is under specified in terms of mechanisms for distributing voting credentials, with the implicit assumption in the original CESG Security Study that credentials are generated by a single domain, albeit using similar practices to those for distributing bank card credentials [18]. The formalisation provides a basis for correcting the flaws described in Section 4.3.4.

Following the formalisation, the basic version of the new scheme is described in two parts. In Section 5.3, the modifications to the scheme are presented from a voter experience perspective; that is the process of casting and verifying a vote by the voter is described. This provides an intuitive explanation of the verification process. In Section 5.4, the scheme is presented from a protocol perspective; that is the interactions between the voter and a distributed election authority architecture. The flexibility of the basic scheme is then demonstrated through a range of adaptations, illustrating that mCESG represents a new class of novel voting schemes.

5.2 Formalisation

This section describes the communication that occurs between the modules of the Election System and voters in order for initiation, vote casting and vote tallying to take place. Communication is assumed to occur via secure channels between the modules of the Election System. A secure one-way channel is assumed to exist from the Election System to the

voter during initiation, whilst further communication between voters and the Election System during voting and tallying is assumed to occur via un-secure channels with messages assumed to be vulnerable to interception and modification.

5.2.1 Notation

Prior to formalising the description of mCESG, a brief description of the notation to be used is necessary. In the proceeding sections, credential values are denoted as capitalised acronyms (CID, VID, PCIN, RID) when referring to values as they appear on a voting credential. Credential values are referred to from a protocol perspective they are denoted as lower case italicised acronyms (cid, vid, $pcin$, rid). Crytographic keys are denoted as K_{lab}, where lab is the label for the key. Value types are denoted as type writer font labels (`String`). Length parameters are denoted as len_{lab}, where lab is the label for the particular length value.

5.2.2 Initiation

Figure 4.4, taken from the original CESG security system, illustrates the Election System as several modules with specific roles. The study does not however, specify the process responsible for generating credentials. In this formalisation, a single additional module $Setup$ is assumed to be responsible for credential generation. To initialise the other modules of the election system $Setup$ requires the following parameters:

- *m* candidates each with a unique candName:`String`
- *n* voters each with a unique voterName:`String`
- secret government voter identification number generator key K_{vid}
- secret government candidate identification number generator key K_{cid}
- secret government personal candidate identification number generator key K_{pcin}

- secret government return identity generator key K_{rid}
- the number of digits len_{vid} of a vid value
- the number of digits len_{pcin} of a $pcin$ value
- the number of digits len_{rid} of a rid value
- the number of digits len_{cid} of a cid value

The $Setup$ module executes several functions to generate arrays of credential information. The CESG study proposed the use of a secure cryptographic 1-way hash function in order to generate voting credentials. Each credential value is thus generated using the following function (with the precise cryptographic algorithm left deliberately unspecified).

- **genHMAC(** input:`byte[]`, len_{output}:`int`, K_{input}:`byte[]` **):**`int`

  Computes a HMAC value for the specified input using the specified key.

Arrays of credentials are then generated by the $Setup$ module, using the following functions. In each case, the form of the array, the array identifier and the function (with arguments and type) are specified.

- let $cid_{1 \leq ij \leq nm}$ = **CID**

  genCIDs(candNames:`String[m]`, len_{cid}:`int`, K_{cid}:`byte[]` **):**`int[]`

  Computes a unique candidate identity number for each String of candNames.

- let $pcincid_{1 \leq ij \leq nm}$ = **PCIN-CID**

  permCIDs(CID:`int[m]`, n:`int` **):**`int[n][m]`

  Computes n permutations of the m candidate identity number values.

- let $vid_{1 \leq i \leq n}$ = **VID**

  genVIDs(voterNames:`String[]`, len_{vid}:`int`, K_{vid}:`byte[]` **):**`int[]`

  Computes a unique voter identity number for each String of voterNames.

- let $pcin_{\ 1 \leq ij \leq nm}$ = **PCIN**

  genPCINs(VID:`int[n]`, CID:`int[n][m]`, len_{pcin}:`int`, K_{pcin}:`byte[]` **):**`int[n][m]`

  Computes the non-unique personal candidate identity numbers between a candidate and a voter, such that

$$\text{genHMAC}(vid_i + cid_{ij}, len_{pcin}, K_{pcin}) = pcin_{ij}$$

- let $rid_{\ 1 \leq ij \leq nm}$ = **RID**.

  genRIDs(VID:`int[n]`, PCIN:`int[n][m]`, len_{rid}:`int`, K_{rid}:`byte[]` **):**`int[][]`

  Computes the non-unique return identity numbers between candidates and voters.

Using the above function definitions, generation and distribution of credentials proceeds as in Figure 5.1. $Setup$ generates an array of n vid values, and nm cid, $pcin$ and rid values. The **VID** array and key used for generating rid values is sent to the $Authenticator$ module for authenticating votes and generating rid values to be sent the $Validator$. The **VID** and **RID** arrays are sent to the Validator module for checking the validity of and rid value for a given vid. The **VID** and **PCIN-CID** arrays are sent to the Tallier, so that anonymous tallying of votes may be undertaken. Finally, the association between candidates and **CID** values and between voters and **VID** values is sent to the Matcher and Marker modules respectively so that candidates may be matched with CID values to produce a non-anonymous tally, and that a marked roll can be produced.

The diagram also illustrates initiation for a single voter. For all voters $1 \leq i \leq n$, the ith voter is sent as voting credentials, the ith vid value and the $i1...im$ $pcin$ and rid values.

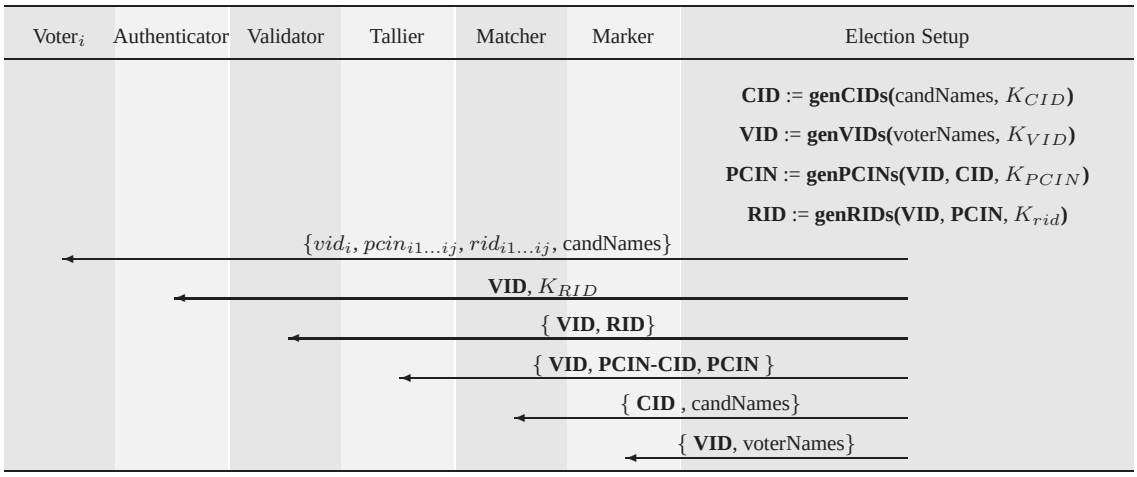


Figure 5.1: Initiation phase of the CESG Scheme. The figure illustrates interaction between the module of the Election System and a single voter. The ElectionSetup module uses four functions to generate arrays of hashed message authentication codes (HMACs) based on initiation parameters. These arrays are then distributed amongst the remaining processes of the domain in order for them to perform their specified tasks (authentication, validation) etc. Voter$_i$ receives values vid_i, $pcin_{i1...ij}$ and $rid_{i1...ij}$ from the arrays VID, PCIN and RID respectively, together with candNames to provide a set of voting credentials.

5.2.3 Vote Casting

As described in the previous section, the Authenticator has received the **VID** array and K_{RID} from the Setup module whilst the Validator has received the **VID** and **RID** arrays. In addition, the following function are specified for the Authenticator in order to process votes sent by voters.

- **genRID(** vid:`int`, $pcin$:`int`, K_{rid}:`byte[]`, len_{rid}:`int` **):**`int`

  Computes a non-unique return identity number between a candidate and a voter.

As for the functions used by the Setup module, **genRID** is constructed using the generic genHMAC function such that:

- **genHMAC(** $vid_i : pcin_{ij}$, len_{rid}, K_{rid} **):**`int`

Vote casting proceeds as illustrated in Figure 5.2, formalising the description provided in the original study [18] and in Section 4.3.2. The protocol has three termination points, either when vote casting is successful, when an incorrect vid value is received, or when an incorrect rid value is generated for the vid:$pcin$ value received. Note that the protocol does not have a separate termination state for when a voter receives an incorrect rid value for the vid:$pcin$ sent to the Election System, since remedying this failure was left out of the scheme in the original security study [18].

To cast a vote, the ith voter who chooses the jth candidate on their credential sends a concatenation vid_x:$pcin_y$ to a Gateway module. The Gateway forwards the vote to the Authenticator, which checks whether the vid_x value sent is contained in the set of vid values ($vid_x = vid_i$). If this is not the case, an error message is returned to the voter indicating they have entered their vid value incorrectly. If the vid_x value is within the **VID** array, the Authenticator computes $rid_y =$**genRID**(vid_x:$pcin_y$) and sends this and the vid

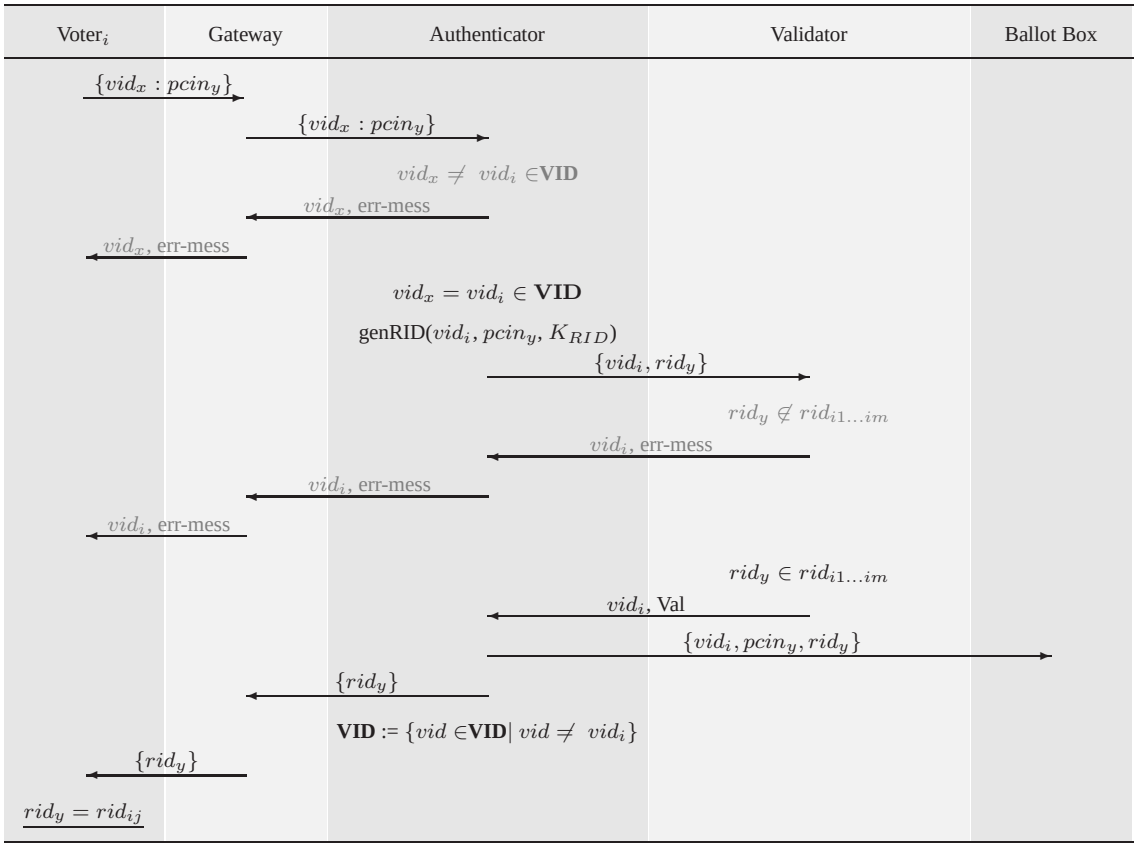


Figure 5.2: The voting phase of the CESG scheme. Successful execution of the vote casting protocol is illustrated in black, reaching termination and a vote is successfully collected. Faint messages in the protocol indicate early protocol termination sequences if the $\{vid : pcin\}$ combination does not contain a legal vid, or does not compute a legal rid.

value to the Validator. The Validator then confirms that the rid_y value is valid for voter i ($rid_y = rid_{i,j}$) . If the rid_y value is not valid, an error message is returned to the voter via the Authenticator. If the $rid_{i,j}$ value is valid, the Authenticator is notified, which then removes the vid_i value from the VID array and sends the rid_y value back to the voter. The vid_i, $pcin_{i,j}$ and $rid_{i,j}$ tuple is then sent to the ballot box for storage prior to tallying. The voter confirms that $rid_y = rid_{i,j}$ on their voting credentials.

5.2.4 Tallying

Once the deadline for voting has been reached, the tallying protocol is initiated. Recall that the Tallier is provided with the **VID**, **PCIN-CID** and **PCIN** arrays during initiation in order to compute a tally for each cid value. The Matcher module is provided with the **CID** and candNames array such that a tally for each candName can be computed using the tally for cid values computed by the Tallier. Finally, the Marker is provided with the voterNames and **VID** array in order to produce a marked roll of participating voters.

As for initiation and voting, several functions are defined to describe the behaviour of the modules of the Election System during tallying. For tallying, a function is specified for the Tallier, Matcher and Marker modules respectively, given p votes cast:

- **tally(** votes:`int:int[p]` **VID:**`int[n]`, **PCIN:**`int[n][m]`, **PCIN-CID:**`int[n][m]` **):**{`int, int`}`[m]`

  For each $vid : pcin$ combination received, the corresponding cid is obtained from cidpcin array and its tally incremented. The function outputs the tally for each cid.

- **match(** tallies:{`int, int`}`[p]`, CID:`int[]`, candNames:`String[]` **):**{`String, int`}`[]`

  Replaces each cid in the tally with the corresponding candName, revealing the result of the election.

- **mark(** $vid_{1...p}$:`int[p]`, register:{`int,String`}`[n]` **):**`String[]`

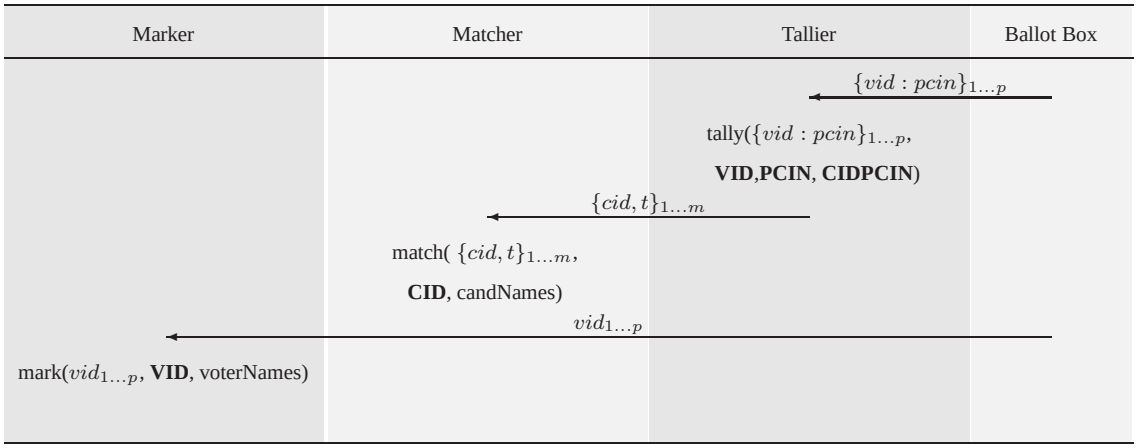


Figure 5.3: Tallying phase of the CESG scheme. The figure illustrates the sequence of messages and computation during the tallying and marking processes at the end of the election. The output of the tallying protocol is a list of candidate names with a corresponding tally (the election returns) and a list of voter names(the marked roll).

> *Outputs a list of voterNames corresponding to the recieved list of $vids$ that were used to cast votes.*

.

In contrast to the functions specified for initiation and tallying, the functions used for tallying are purely look-up functions, using parameters provided during initiation by the Setup module and votes cast during voting to produce a tally for each candidate and a marked roll of participating voters.

The protocol proceeds as per Figure 5.3. The BallotBox module sends the Tallier the p length array of vid:$pcin$ tuples received during voting. The Tallier computes:

$$\{cid, t\}_{1...m} = tally(vid : pcin_{1...p}, \mathbf{VID}, \mathbf{PCIN}, \mathbf{PCIN - CID})$$

and sends the resulting array to the Matcher. The matcher then computes the final tally by matching the cid values in the tally to the candNames:

$$\{candName, t\}_{1...m}\} = match(\{cid, t\}_{1...m}, \mathbf{CID}, candNames)$$

to produce a tally for the election. Separately, the Marker computes the marked roll:

$$\{voterName\}_{1...p}\} = mark(\{\{vid\}_{1...p}, \mathbf{CID}, voterNames)$$

5.2.5 Summary of Formalisation

The preceding sections formalised the CESG scheme described in [18] as a cryptographic protocol. An additional $Setup$ module was inserted into the Election System in order to provide a mechanism for accepting input parameters and initialising the system. The description formalised the modules of the Election System as discrete processes with a specified functionality and described the messages that passed between modules during the three phases of initiation, voting and tallying. The formal description provides a context for describing corrections to the CESG scheme to provide desirable properties, including vote verifiability and vote-voter non-association by the Election System.

5.3 Vote Verification

In this section a correction to the CESG scheme (mCESG) is described which provides for voter verifiability by committing the Election System to a receipt for a vote via a universally readable broadcast channel - secure electronic bulletin board.

5.3.1 Motivation

As noted in Section 4.3.4, the CESG scheme lacks both voter verifiability and undeniability. Voter verifiability and undeniability are considered useful substitutes for voting schemes

implemented using electronic media used for a public election context, since such voting systems are considered less transparent, and thus more vulnerable to abuse, than paper based systems. A voter verifiable voting scheme permits a voter to determine whether their vote has been counted in a tally of cast votes. Similarly, an undeniable scheme permits an election organiser to demonstrate that they did not receive a particular vote, or at least they did not attempt to convince the voter that a vote had been successfully included in the tally without this being the case. Schemes that lack undeniability are vulnerable to attacks on voter *confidence* in the result produced, since voters may claim *unrefutably* that their votes (which were in fact not cast) were illegally removed from the tally.

The CESG scheme is not voter verifiable since the rid value received by a voter indicates only that the Election System has correctly received their vote, not that the Election System will process the received vote accurately. Conversely, the CESG Election System cannot demonstrate that it did not receive a vote, return the correct rid value and then not include the vote in the tally, since the Election System can only demonstrate to the voter that it received their vote, and not that the vote was counted.

Given the other desirable pollsterless features of the CESG scheme, and it's otherwise suitability for UK public elections, it would be desirable to demonstrate a correction to the CESG scheme that incorporates voter verifiability and undeniability. The sections below describe a scheme which forces the Election System to publicly commit to voter's choices without revealing the association between votes and voters, or revealing a partial tally during the voting phases.

5.3.2 The Publisher

In order to adapt the CESG scheme to provide for voter verifiability and un-deniability, some mechanism must be employed that irrevocably commits the Election System to a vote in a manner which the voter can verify. To achieve this, a new *Publisher* module is added to the Election System. The publisher behaves in a similar manner to a secure elec-

tronic bulletin board, a common cryptographic construct. The publisher can be considered as an interface to a universally readable broadcast channel, to which messages may be written by processes with the appropriate capability. The Election System is provided with the additional capability of writing information to the Publisher, which is then universally accessible by voters, external observers and the Election System itself. The Election System is assumed to not have the capability of removing information written to the Publisher.

5.3.3 Verifying a Vote

Figure 5.4 illustrates the vote checking procedure from the perspective of the voter. Vote casting is identical to that in the original CESG scheme. However, the genRID() function is now modified such that:

- **genRID(** vid:`int`, $pcin$:`int`, K_{rid}:`byte[]`, len_{rid}:`int` **):**`int`

  Computes a unique return identity number between a candidate and a voter.

I.e, the function now generates a unique rid value for each vid:$pcin$ combination input argument for all credentials. Thus the rid value forms a unique association between a voter and a choice of candidate, in a similar manner to a vid:$pcin$ concatenation.

As before, voters are provided with a set of voting credentials consisting of a Voter Identification number (vid) and a set of Personal Candidate Identification Number ($pcin$) and (relabeled) *Receipt* Identification numbers (rid), one each for each candidate. To cast a vote, a voter prepares a message consisting of their own vid number and the $pcin$ number of their chosen candidate. This message is then sent via an available channel (such as an SMS message) to the Election System for processing.

Given a valid vid:$pcin$ combination, an rid value is published on a publicly accessible bulletin board as illustrated in Figure 5.4. The voter may then determine that the correct rid has been published for the vote they have cast. The election system sends a message

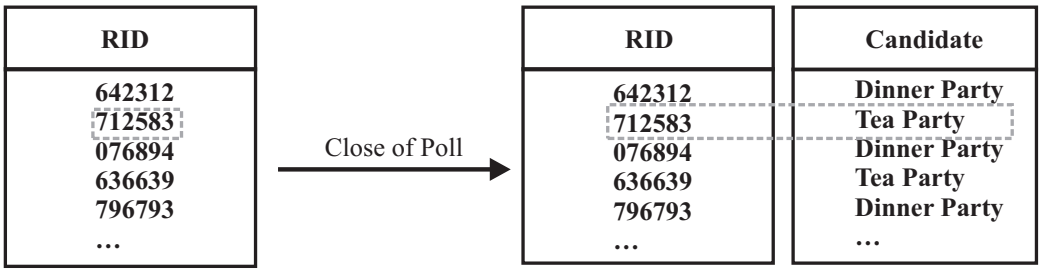


Figure 5.4: The mCESG secure, universally readable bulletin board. The lists of receipt numbers and votes committed to by the Vendor's Publisher module during the two phases of verification. In the first phase of verification, the voter confirms that the correct rid value occurs in the list under Receipt Number, prior to the close of poll. In the second phase of verification, the voter confirms that the correct candidate is published next to the rid value for their vote. The gray dotted boxes indicate the location of Alice's vote in the list.

to the voter indicating that their vote has been successfully processed, although the voter should consider this message to be informative only and not proof of receipt.

If the Election System publishes the wrong rid value for the voter's choice, the voter must contact the Election System via some other channel in order to have the incorrect rid value removed and cast a second vote, potentially via some other mechanism. The voter may take this action at any point until the end of voting. Conversely, the Election System may publish no rid value at all for a cast vote. In the circumstances where no relevant rid value is published after some latency period, the voter should re-attempt to cast their vote. If repeated attempts at vote casting do not result in a (correct or otherwise) rid value being published, the voter should assume that their vote is not reaching the Election System and should revert to the strategy described for a wrong rid value being published. Note that since voting is assumed to occur over insecure channels (as per the pollsterless property) the scheme's design deliberately accepts the potential for votes to be intercepted, say in a Denial of Service attack, but not to be interpreted or modified by an eaves-dropping attacker.

Assuming the correct rid value is published, the Election System is now committed to the rid choice of the voter publicly in a manner which the Election System cannot later de-commit from. However, at this stage, the Election System is not committed to processing

the voter's choice accurately. To effect this second commitment, once the close of poll has been reached, the Election System publishes the association between rid and candidates for each vote. This does not reveal the association between votes and voters, since the voting credentials are assumed to be a secret possessed only by the voter. At this stage, a voter can confirm that their vote has been processed accurately (i.e. that the correct candidate is associated with their rid) but not that the rid itself is correct, since this would violate the undeniability property.

The mCESG scheme thus achieves voter verifiability by publicly committing the Election System to a voter's choice that the voter can confirm with respect to their voting credentials. The credentials thus constitute a *receipt* with which a voter may request the Election System change the candidate name associated with a rid value on the bulletin board. The scheme preserves the secrecy of vote to voter association under the assumption that a voter does not reveal their credentials to a third party. Adaptations to the mCESG scheme which address the problem of vote buying or voter coercion with receipts are discussed in Sections 5.5.4 and 5.5.5. The scheme achieves undeniability by providing a voter with the ability to correct an incorrectly processed vote during voting without revealing the association between votes and voters. If the voter does not correct an rid value prior to tallying, the rid value is considered an accurate record of a voter's choice.

5.4 Revised Architecture

Although the modified system described in Section 5.3 is now both verifiable and undeniable, a single process, ElectionSetup, is still used to generate and distribute the credentials for casting and processing of votes. Such a design is vulnerable because (a) the process represents a single point of external attack and (b) voters must trust a single process not to violate the privacy of voting.

In addition, the use of the rid value as a unique secret shared between the Election System and the voter, requires that the association between an rid value and a voter should not

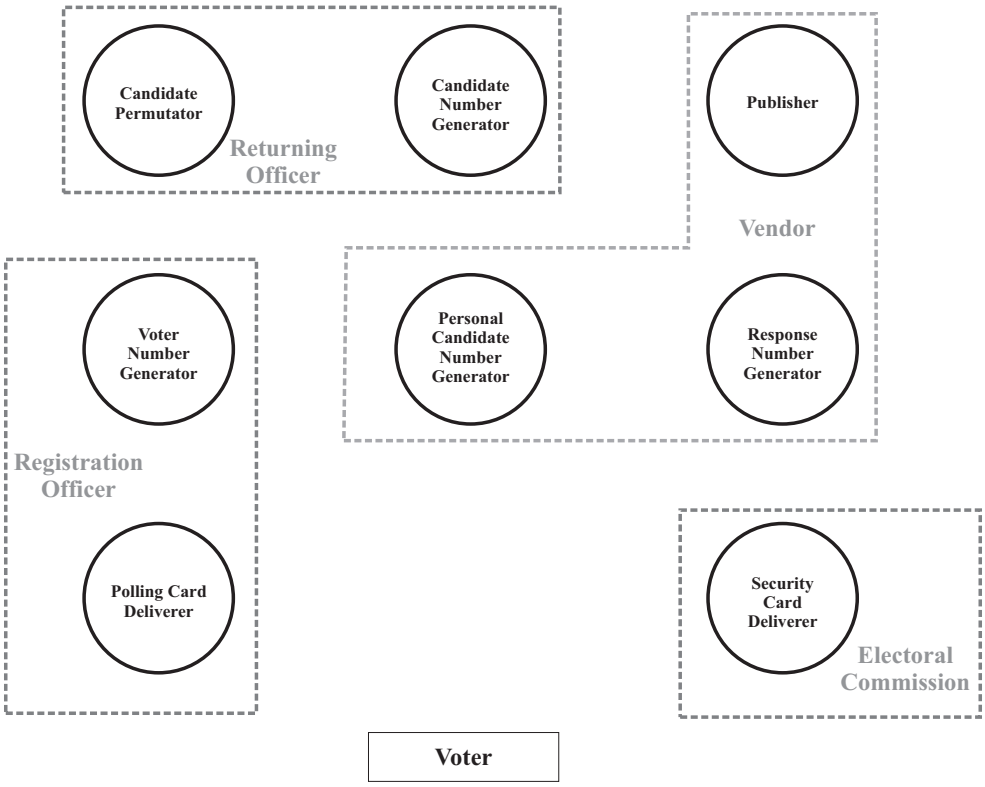


Figure 5.5: The distributed domains of the mCESG Election Authority. The monolithic structure of the CESG election system is divided into four autonomous domains. A Registration Officer domain is responsible for voter identities. A Returning Officer domain is responsible for candidate identities. A Vendor domain is responsible for generating voting credentials. An Electoral Commission is responsible for delivering the security card component of the voting credentials. The domain infrastructure is designed with respect to the existing UK voting system to minimise re-design of surrounding processes.

be known by any one process of the Election System. This requirement is complicated because if the rid value is to be delivered to the voter, then the delivering process must know the identity of the voter whilst at the same time possessing rid value material.

Figure 5.5 illustrate the redesign Election System, dividing it into four autonomous domains collectively known as the mCESG *Election Authority*. The design provides for increased protection for anonymity than the single ElectionSetup process in the original CESG voting system. In the revised scheme the Election Authority domain is divided into four domains, each under the control of an independent organisation. The *Registration Officer* domain is responsible for processing of voter information. The *Returning Officer*

domain is responsible for the storage of candidate information. The *Vendor* domain is responsible for generation of credentials for voting, collecting votes and publishing values to the secure bulletin board. The *Electoral Commission* domain provides a delivery function to prevent any one domain learning the association between rid values and a voter.

5.4.1 Initiation

The generation of credentials proceeds as illustrated in Figure 5.6. The key component of the process is the separation of the computation and delivery functions between different domains, preventing the domain that generates the rid values from knowing the identity of the voter to whom they will be delivered. This protects the anonymity of the voter based upon the assumption of non-collusion across domains. Communication between domains occurs via secure, authenticated channels.

The initiation parameters of the single monlithic Setup module of the CESG scheme is distributed as follows.

- The n voterName strings and vid generation key K_{vid} and length parameter len_{vid}. are initiation parameters of the Registration Officer domain.
- The m candidateName strings and cid generation key K_{cid} and length parameters (len_{cid} are initiation parameters of the Returning Officer domain.
- The $pcin$ and rid generation keys (K_{pcin}, K_{rid}) and length parameters (len_{pcin}, len_{rid}) are initiation parameters of the Vendor domain.

Further the functionality of the single monolithic Setup module is distributed such that:

- **genVID()** is a function of the Registration Officer domain.
- **genCID()** is a function of the Returning Officer domain.

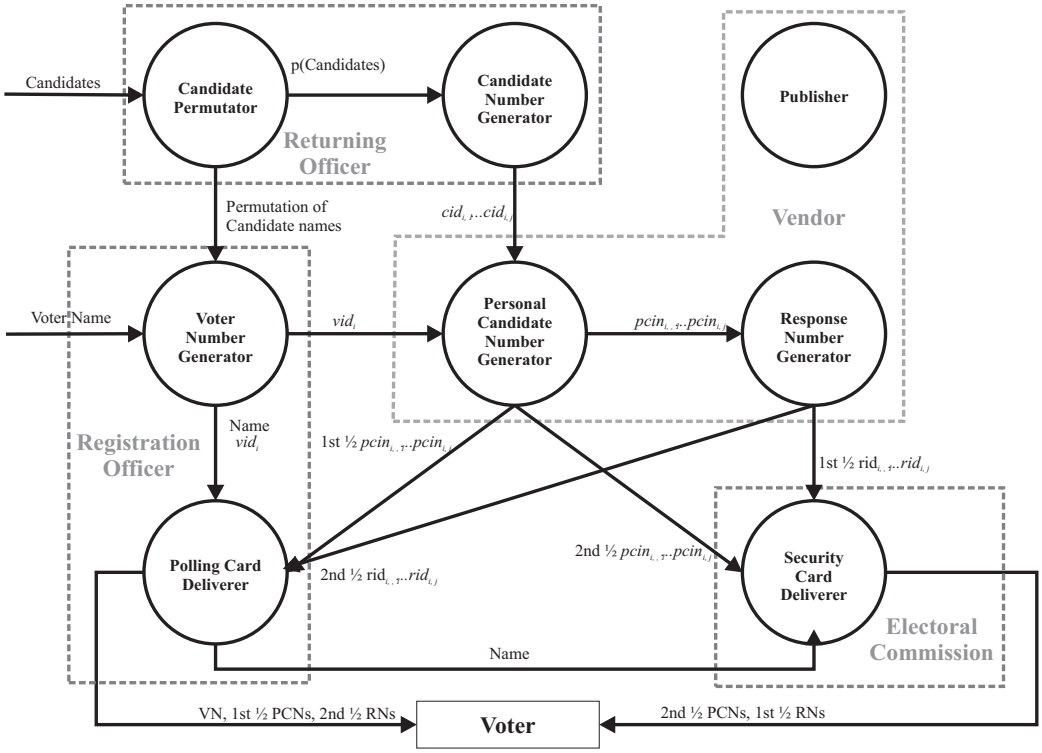


Figure 5.6: Initiation phase of the mCESG scheme. The figure illustrates the four domains of the Election Authority collaborating in order to produce a complete set of voting credentials. The Registration Officer domain generates a vid value for the ith voter and passes this to the Vendor domain. The Returning Officer domain generates a permutation of candidate and passes this to theRegistration Officer. The Returning Officer also passes a set of cid values to the Vendor domain. The Vendor domain uses the cid and vid values to generate a set of $pcin$ and rid values. Each of these two sets of values are divided into two sets of substrings which are delivered to the Registration Officer and the Electoral Commission who forward the credentials to the voter.

- **genPCIN()** and **genRID()** are functions of the Returning Officer domain.

To generate credentials, the Registration Officer generates a new Voter Identity value (vid) and passes the the new value to the Vendor. The Registration Officer also notifies the Returning Officer that a new voter has requested credentials. The Returning Officer generates a new set of Candidate Identity values (cid) for the Vendor. The Vendor then computes a set of Personal Candidate Identity values ($pcin$) and Receipt Identity values rid, one for each candidate. The Vendor then divides each $pcin$ and rid value in the set into two sub-strings. The division of values is denoted on Figure 5.6 as:

$$pcin_{1...len_{pcin}/2}$$

$$pcin_{len_{pcin}/2+1...len_{pcin}}$$

$$rid_{1...len_{rid}/2}$$

$$rid_{len_{rid}/2+1...len_{rid}}$$

The first sub-string of each value is sent back to the Registration Officer, whilst the second sub-string of each value is sent to the Electoral Commission. The Registration Officer passes the voter identity to the Electoral Commission. The Registration Officer then forwards the vid value and $pcin$ and rid sub-strings to the voter. The Electoral Commission forwards the $pcin$ and rid sub-strings it possesses to the voter. The initiation mechanism prevents any one domain from learning sufficient credential information to know the association between a vote and a voter.

To perform the generation of credentials, the specification of **genCID()** must be modified to ensure that a different set of cid values are generated for every voter. This is combined with a new function for the Returning Officer domain, which permutates the order of candidates:

- **permCandNames(** candNames:`String[m]`**):** `String[m]`

  Generates a random permutation of the candNames array.

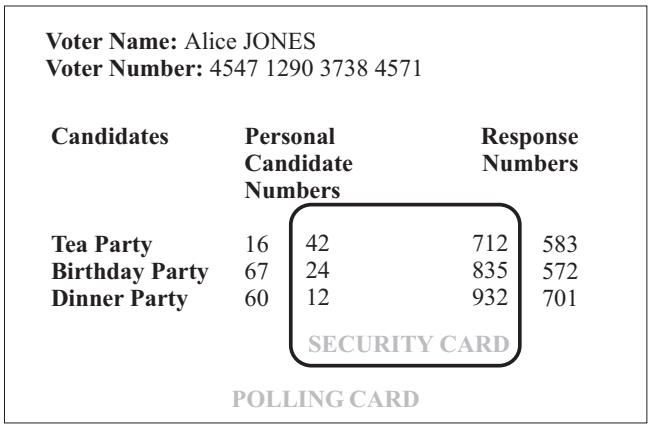


Figure 5.7: The completed voting credentials for a single voter in the mCESG scheme. The extra credential information consists of a voter number; a set of personal candidate numbers and associated response numbers for each candidate nominated in the election. The Polling Card is supplied to the voter by the Registration Officer domain. The Security Card is provided by the Electoral Commission domain.

An additional benefit of the re-design is that the voting system is resistant to *intelligent ballot stuffing* by the ElectionAuthority, again under the assumption of non-collusion. In order to perform ballot stuffing, a process needs to know a $vid : pcin$ combination, whilst to be intelligent, the process must know which candidate corresponds to which $pcin$ value. Although it is notable that the Vendor domains may commit *blind ballot stuffing* it cannot by itself commit intelligent ballot stuffing.

The effect of these modifications to the Returning Officer domain is to prevent a single voter from colluding with the Vendor to commit intelligent ballot stuffing. Without the modification, a single set of voting credentials could be used to match candidate names with the corresponding cid values.

A consequence of the revised scheme's initiation is that the voter receives their voting credentials as two separate messages. The revised mCESG scheme retains the assumption of the CESG scheme that voting credentials will be printed on secure stationary and sent to the voter using the postal system, under the assumption that this constitutes a secure, undeniable channel. The compiled credentials envisaged for the mCESG scheme are illustrated

in Figure 5.7. The credentials are divided into a polling card and a security card. As noted in Section 4.3, the polling card is a document already sent to voters participating in elections within the UK public elections context. The mechanism of splitting the credentials into two components could be explained to voters in the context of receiving credit cards and PINs via two separate messages in the post. The familiarity of security practices has been suggested by Randell et al to be important in establishing trust in a voting mechanism [114].

5.4.2 Voting and rid Checking

Vote casting proceeds as illustrated in Figure 5.8. The voter chooses a candidate and sends a vid:$pcin$ message to the Vendor via a Gateway domain as per CESG. the Vendor domain's generator module looks-up the corresponding rid value and sends this to the Publisher module, which writes the rid value to the universally readable broadcast channel (i.e. a secure bulletin board). In order to disrupt timing attacks, in which an external attacker observes the rid which is published subsequent to each vid:$pcin$ value received by the Vendor, the Publisher writes rid values to the bulletin board in randomly permuted batches. The voter receives the list of current rid values published from the bulletin board channel and confirms that the list contains the rid corresponding to their choice.

Note that at this stage the Vendor remains isolated from both the voter identities and the candidate identities, stored by the Registration Officer and Returning Officer domains respectively.

5.4.3 Tallying and Vote Checking

The production of a tally requires collaboration between the Vendor and Returning Officer domains, since in the mCESG initiation, the vote collection and candidate identities are stored in autonomous domains. The distribution of this function between the two domains prevents an early tally being published, in circumstances where one of the domains

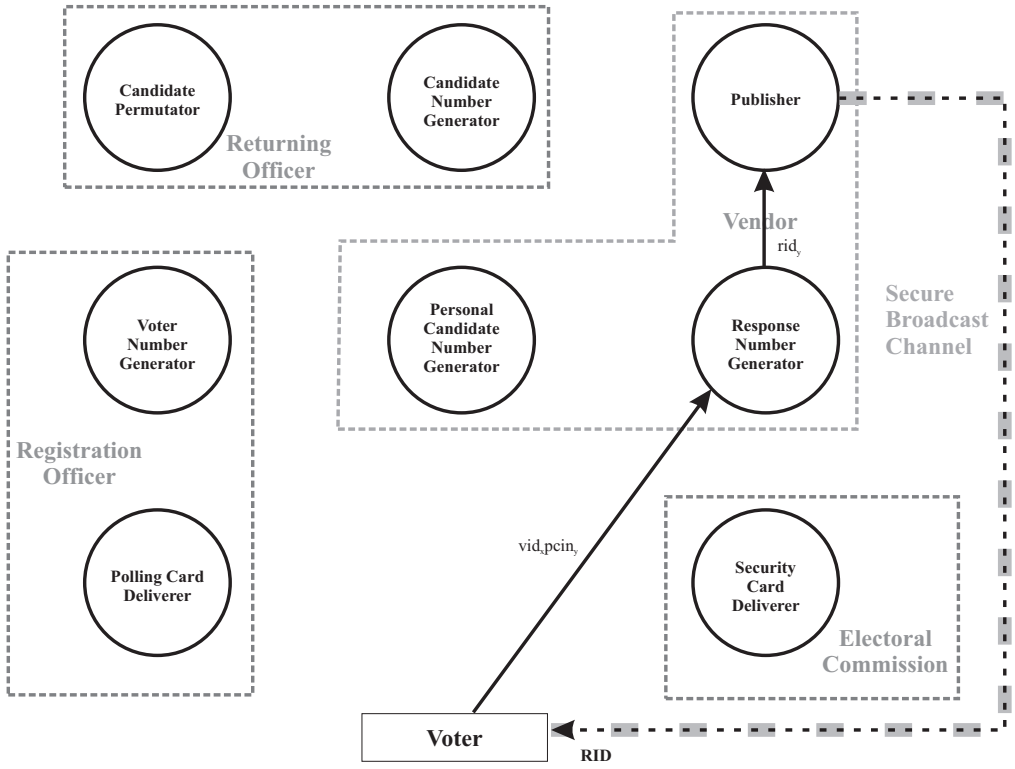


Figure 5.8: Voting and checking phase of the mCESG scheme. The voter sends a vid:$pcin$ message to the Vendor. The Vendor domain's generator module looks-up the corresponding rid value and sends this to the Publisher module, which writes rid values to the bulletin board in randomly permuted batches. The voter receives the list of current rid values published from the bulletin board channel and confirms that the list contains the rid corresponding to their choice.

is corrupt.

Tallying proceeds as illustrated in Figure 5.9. The RID generator module converts all published rid values into their cid form, by look-up of the values provided during initiation. The cid values are then sent to the Returning Officer, who produces a list of candidate names corresponding to the cid values through a similar look-up process of generated values. This array of candidate names is then returned to the Vendor, which forward the list to the Publisher module. The list of candidate names is then published alongside the list of rid values already written to the bulletin board. The voter accesses the list of rid values and candidate identities and determines whether the candidate identity published corresponds with the candidate on their voting credentials next to the rid value as published on the bulletin board.

5.5 Adaptations

The previous section discussed a modification of the CESG scheme to provide for the desirable properties of voter verifiability, undeniability and anonymous credential generation in order to prevent the association between votes and voters being revealed. With the modified (mCESG) scheme described, several further adaptations are possible which demonstrate the considerable flexibility of the scheme. The adaptations are presented separately from the mCESG scheme, since they also add extra complexity, or restrictions on the scheme's functionality which may not be desirable in certain voting contexts, such that they will not be used. This section illustrates that the mCESG scheme is *configurable* to different voting contexts, where different requirements for voting scheme properties prevail.

5.5.1 Multi-member Electoral Systems

A limitation of the mCESG scheme thus far described is that the voter is only able to indicate a choice for a single candidate from a proposal. This limits the range of electoral

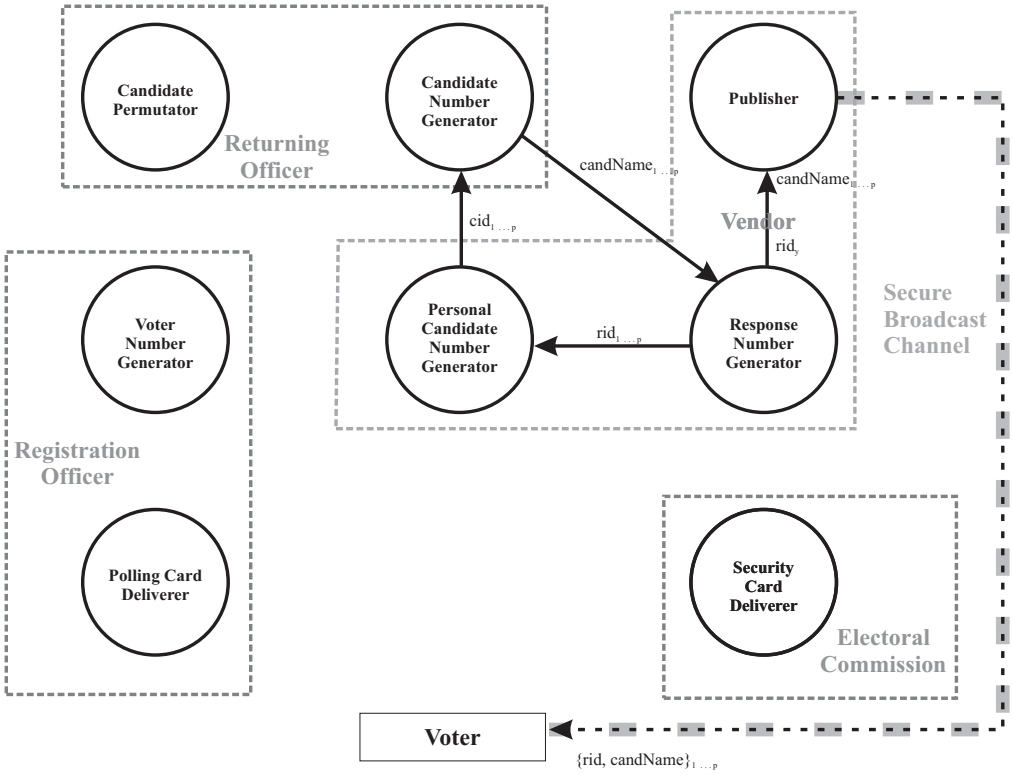


Figure 5.9: Tallying phase of the mCESG scheme. At the end of voting, the Vendor domain sends a list of cid values for the votes cast during the voting phase to the Returning Officer domain. The Returning Officer returns a corresponding list of candidate names to the Vendor domain. The voter can then determine whether the correct candidate is published next to their rid value and that the tally of results reflects the list of candidate names published.

systems for which implementations of the scheme can be used. In particular, multi-member simple plurality schemes are not accommodated.

A simple generalisation of the scheme to facilitate multi-option votes would be to permit votes to indicate multiple choices for a single vid. Vote message construction can be altered so that several candidates can be indicated by including all their *pcin values*:

$$vid_i : pcin_j : pcin_k ...$$

However, this approach is problematic, since an external observer of an unprotected channel down which vote messages are sent may be able to alter voting messages by removing $pcin$ values. The benefits of this attack are limited, since the attacker is unable to determine which candidate they are removing from the message. Similarly, if the voter checks the bulletin board to determine the correct rid values have been published, they will discover the vote message has not been received and processed correctly by the Vendor domain. However, the attack is still disrupting, since the voter may perceive that the Vendor domain is attempting to cheat them. As an additional protection for the vote during communciation to the Vendor domain, the voter is provided with an extra set of credential values - Check Sum Numbers (CSNs) which the voter appends to the vote message. The Check Sum Numbers are generated and distributed by the Vendor domain on the polling card half of the voting credentials as illustrated in Figure 5.10.

For an election in which Alice Jones would use the credentials illustrated, to cast a vote for the Tea Party's two candidates, she would send the message:

$$\underbrace{4547129037384571}_{\text{VID}} \quad \underbrace{1642}_{\text{Candidate 1}} \quad \underbrace{9130}_{\text{Candidate 2}} \quad \underbrace{8965}_{\text{CSN}}$$

If the vote message is received correctly, the voter will view the rid values for both candidates displayed on the bulletin board as for the basic scheme. This adaptation does not permit ordinal votes to be cast where the voter may rank candidates. The next section describes an ordinal adaptation to the mCESG scheme voting credentials.

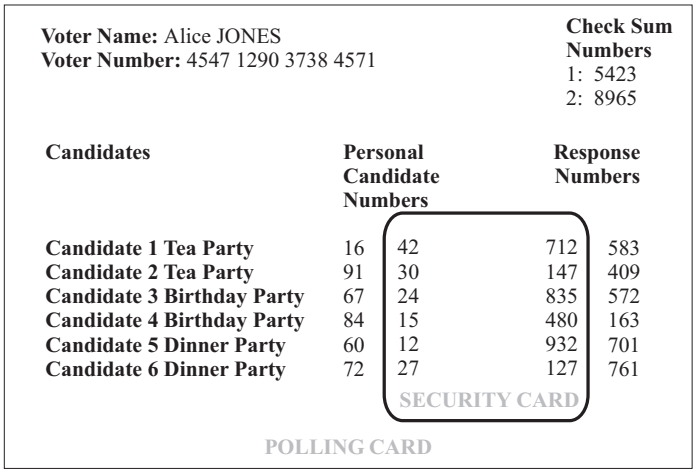


Figure 5.10: mCESG scheme voting credentials for the Multi Member Simple Plurality electoral system adaptation. The Voting credentials are modified to permit ordinal (ranked) voting for electoral systems such as Single Transferable Vote (STV). The credentials are modifed from Figure 5.7 to include *check sum numbers*, which enable a voter to indicate how many choices they have selected .

5.5.2 Ordinal Electoral Systems

Ordinal electoral systems introduce additional complexity for a voter, since they are required to rank the candidates in order of preference, rather than select the most preferred alone. The original mCESG does not manage this complexity well, since a voter would need to be presented with a PCIN value for every possible permutation of candidates on their voting credential in order to prevent information leakage from the vote during communication. In this section, an adaption of the mCESG scheme to ordinal electoral systems is presented. The adaption does not increasing the size of the voting credential provided to the voter.

To permit ranked votes, the voting credentials are modified as illustrated in Figure 5.11. *Preference numbers* (PNs) are incorporated into the PCINs and the RIDs on the voting credentials. PNs consist of random digits associated with each possible rank a voter may wish to associate with a candidate. The preference codes are inserted at a random location for each voter in order to prevent their identification during transmission. In Figure 5.11 the preference codes for PCINs are inserted at index one, whilst the preference codes for

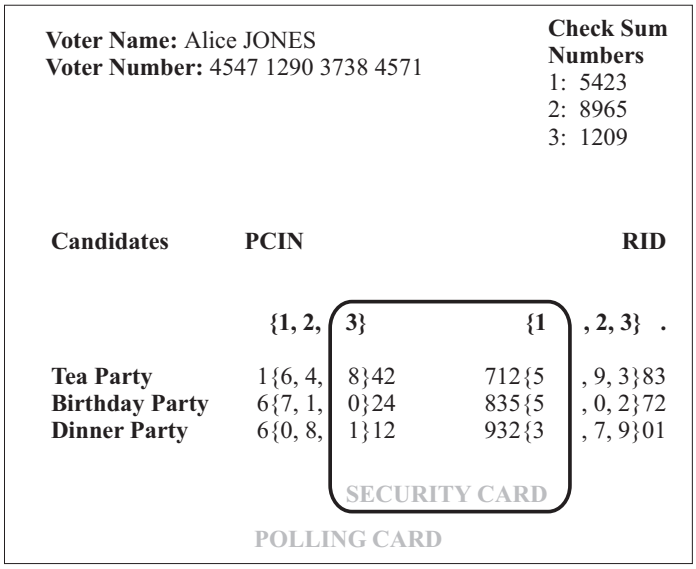


Figure 5.11: mCESG scheme voting credentials for the ordinal electoral system adaptation. The Voting credentials are modified to permit ordinal (ranked) voting for electoral systems such as Single Transferable Vote (STV). The credentials are modifed from Figure 5.7 to include *preference codes* which indicate the preference to be associated with a particular candidate.

the RIDs are inserted at index three. As for the multi-member scheme described in the previous section, Check Sum Numbers are used to indicate how many candidates for the voter has selected.

To cast a vote, the voter sends a message similar to that described in Section 5.3. However, the voter must choose a rank for each candidate voted for, by choosing exactly one preference code. For example, should the voter, Alice, wish to vote for the Birthday Party as first preference and the Dinner Party for second preference, they would send the following message:

$$\underbrace{4547129037384571}_{\text{VN}}\underbrace{6\overbrace{7}^{1^{\text{st}}}24}_{\text{Birthday}}\underbrace{6\overbrace{8}^{2^{\text{nd}}}12}_{\text{Dinner}}\underbrace{8965}_{\text{2 candidates}}$$

During the first phase of the verification process, the voter would expect to see the RIDs for each candidate they voted for as before, but also containing the correct RIDs. From the example above, the voter would expect:

$$835\{5\}72\ 932\{7\}01$$

on the bulletin board. During the second phase of verification, the candidate associated with each rank of the vote is published in association with the RID, for example:

$$835\{5\}72\ 932\{7\}01$$ 1st: Birthday Party 2nd: Dinner Party

Note that the construction of the adapted voting credentials does not require any re-configuration of the Election Authority. The extra information may be added by the Vendor to the anonymous Candidate Numbers supplied by the Returning Officer.

5.5.3 Two Step Vote Casting

A common feature of voting systems is to separate voter authentication and vote casting, particularly for public election contexts, where the electorate is particularly large. An advantage of this separation is often that the process of ensuring vote secrecy (in some form) is easier to manage. The separation is often formalized in schemes which incorporate authentication mechanisms, for example [51].

Several studies typically associated with public elections have suggested that authentication is a necessarily discrete step in the voting process, Ikonomopoulos for example [65]. A consequence of the common separation is a *voter expectation* that all schemes will follow this mechanism. This may not in fact always be true and is dependent upon the voting schemes design and the manner in which it fulfills secrecy and accuracy requirements for a given voting context. Several authors have noted that if a system is to be accepted by users, it should meet pre-conceptions as to its functionality, whilst elsewhere it has been suggested that this condition applies to voting systems as well [14, 25, 114]. That is, new voting systems which incorporate familiar functionality from previous technologies or

Figure 5.12: The two step adaptation of the mCESG scheme illustrating interaction between the voter and the Vendor domain of the Election System. The voter sends the vid value only to the Vendor, which responds with a tok nonce for the voter. The voter then appends the $pcin$ value of their chosen candidate to the tok and sends the complete message to the Vendor for processing.

procedures are more likely to be accepted by voters than systems which require unexpected usage.

For the mCESG scheme, authentication and voting occur in a single step, which may prove unexpected and therefore unacceptable to voters. During demonstrations of the scheme, a common voter mistake was to attempt to send their VID value to the Vendor before entering a PCIN to complete the message (see Chapter 6). To cope with possible user acceptability concerns with the mCESG scheme, it is possible to adapt the vote casting mechanism in such a way as to provide for a two step authentication and vote casting mechanism. [1]

Figure 5.12 illustrates the scheme adaptation with respect to interaction between the voter and the Vendor domain of the Election Authority. The voter sends the vid value only to the Vendor, which responds with a token tok nonce for the voter. The voter then appends the $pcin$ value of their chosen candidate to tok and sends the complete message to the Vendor for processing. To construct the token, the Vendor generates an additional key K_{TOK} and uses additional function employing the generic genHMAC() function:

- **genToken(** vid:`int`, K_{token}:`byte[]`, len_{token}:`int` **):**`int`

  Computes a unique token for the two step mCESG adaption.

[1] This adaptation to the mCESG scheme was suggested by James McKinna, but is included here because of it's relevance to the topics of the thesis. The formalisation of the adaptation is the author's own.

A consequence of the two-step adaptation is that whilst the security of the scheme is unaffected, the complexity (from a voter's perspective) is increased, but the scheme may be more acceptable to voter's with pre-conceptions as to the schemes functionality.

5.5.4 Receipt Free Scheme 1

A valid criticism of the mCESG scheme is that it provides a receipt to voters. The voting credential is assumed to be a secret held by the voter who is responsible for its security. As such, voters are potentially vulnerable to being coerced into revealing their vote. To prevent this attack, many other voting schemes are designed to be *receipt–free* [8]. Receipt free, voter verifiable, voting schemes provide voters with the ability to convince themselves only that their vote has been counted honestly based on messages received from an Election Authority. In receipt free schemes, the voter is unable to *transfer* the proof that their vote has been counted in a certain way to a third party (e.g. an attacker).

The goal of the adaptation described here is to replicate the notion of receipt–freeness in practice in current UK systems. Any modification to the mCESG scheme must still provide re-assurance to voters that their votes have been correctly counted.

For simplicity, the receipt–free adaption is described with respect to the original mCESG scheme, although combination of receipt–freeness with the ordinal electoral system variation is feasible. The key to the receipt–free scheme is to separate the association between voters and chosen candidates in the response schemes. To achieve this, a voter is assigned a single, unique Personal Response ID (PRID) on their voting credential. Each candidate on the voting credential is assigned a smaller, non–unique Candidate Response ID (CRID). Figure 5.13 illustrates the modified voting credential. Note that the responsibility for generation and delivery of both new types of response number may still be split between the various domains of the Election Authority.

The procedure for casting a vote is the same as in the original mCESG scheme – the voter sends a message of the form VID:PCIN. Figure 5.14 illustrates the receipt–free verification

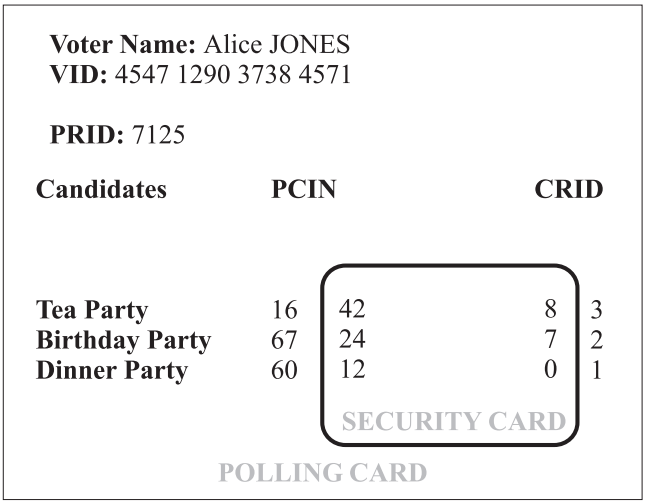


Figure 5.13: Receipt free voting credentials. Note the RID values of the original credentials illustrated in Figure 5.7 are now explicitly divided into a single Voter RID and a set of Candidate RIDs.

procedure, which is now split into three phases. Prior to the close of poll, the voter is only able to observe their PRID on the bulletin board. This commits the Election Authority to acknowledging receipt of votes without at this stage publicly committing to the voter's choices. At this stage, any voter may demonstrate to another participant that they have taken part in the election, but not how they voted. This is comparable to the current UK voting system, where the identities of participants in an election are published after the close of poll in a marked roll [121, Sch. 1 R. 57].

After the close of poll, the second verification phase occurs. In the isolated presence of polling officials, the nominated candidates in the election and their agents the Election Authority reveals the one–one association between PRIDs, CRIDs and candidate identities. This process commits the Election Authority to the associations to the candidates, but not publicly. If desirable, a trusted participant in the election process (the Electoral Commission, for example) could receive an escrowed copy of the associations to prevent the Vendor and Returning Officer changing the associations later.

Having observed the complete set of associations, the candidates are now permitted to select a small number to be published on the bulletin board. Initially, only the association

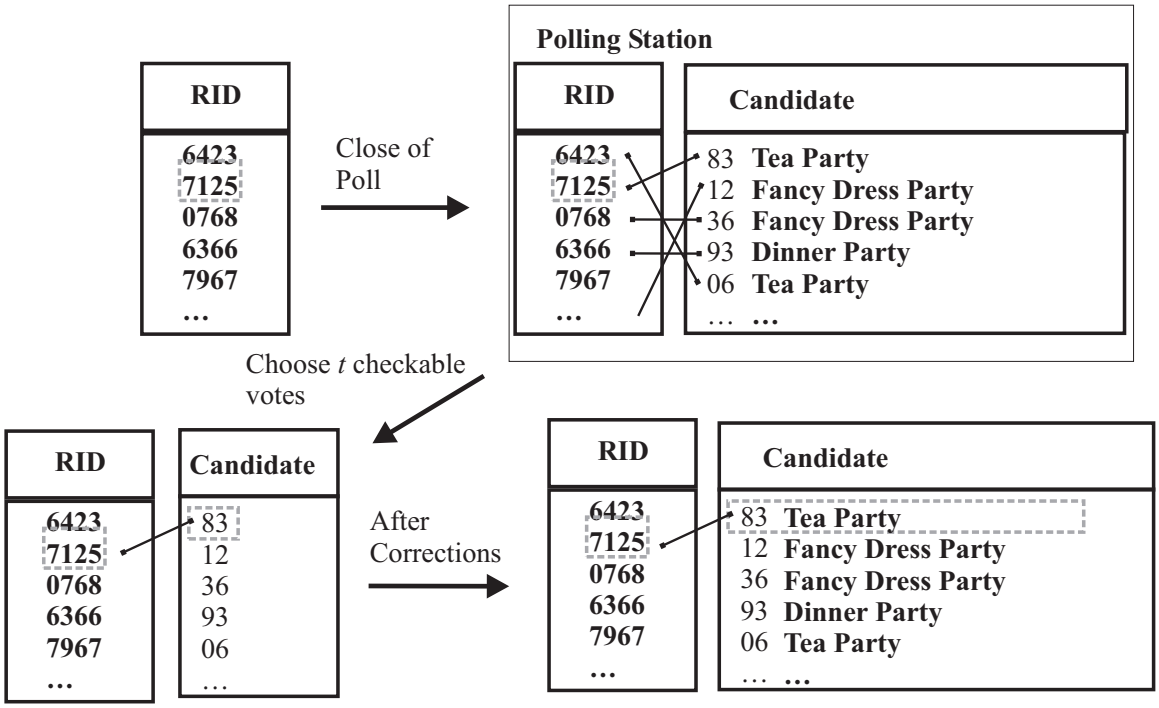


Figure 5.14: The transitions that occur in the published list of response numbers during the phases of verification in the receipt–free adaption of the mCESG scheme.

between the chosen personal RIDs and candidate CRIDs is published. A period of time is then permitted for voters to re–check the bulletin board and, if published, confirm that the association between their PRIDs and CRIDs is correct. This is similar to the initial phase of the original mCESG scheme, except that only a sub–set of voters, selected blindly by the candidates, are able to verify that the correct association was made for their vote.

Assuming no objections are raised to the published associations, verification proceeds to the final phase for the election. The Election Authority publishes the association between all candidate response numbers and candidates. The sub–set of voters who were permitted to verify the association between their RN and their candidate RN may also now verify the association with their chosen candidate. The Election Authority cannot cheat at this stage since it has already committed to the complete one–one associations to the candidates prior to the selection of votes to be verified. This approach may be considered an example of a *cut and choose* protocol and is similar to the *parallel testing* approach advocated for use in the United States and Ireland, where random electronic voting machines are removed from

active polling on polling day and tested for accuracy alongside the remaining machines [80, 134].

5.5.4.1 Selecting the Security Parameter

The significant parameter for the receipt–free voting scheme is the proportion of voters who are able to verify their vote in the tally. Keeping this proportion small limits the number of voters for whom the scheme is not receipt free (those who are able to verify their vote), whilst if the parameter is too small, the probability of the Election Authority cheating undetectably increases.

Denote t as the number of voters permitted to verify their vote out of V voters, such that $t \leq V$. Assuming all permitted t voters follow the verification procedure and that the Election Authority attempts to change n votes, the probability of detection may be defined as:

$$p_d = 1 - \prod_{i=0}^{n-1} \left(1 - \frac{t}{V-i}\right)$$

For small n, small t and large V this may be approximated to

$$p_d = 1 - (1 - t/V)^n$$

By example, consider a typical UK parliamentary election where 50,000 votes are cast and where an Election Authority will attempt to change sufficient votes to overcome the majority of the legitimate victor. As few as $t = 1000$ verifiers, would be required to act as verifiers to provide a high probability of detecting cheating when the number of mis–assigned votes was greater than 200. This would provide a random coercible population of just 2% of the electorate for an attacker. The value of t could be chosen at the start of the verification process, in agreement between the candidates and election officials.

5.5.5 Polling Station Scheme

Section 5.5.4 described an adaptation to the mCESG scheme which provides a receipt free voter verifiable vote checking mechanism for most voters. In some contexts, however, providing a receipt-free voting scheme for all voters such as in certain public elections contexts where remote unsupervised voting is not permitted, is considered a more significant requirement than providing a convenient remote voting system to enable higher participation.

In such circumstances, the mCESG scheme may be adapted to incorporate vote casting in a supervised polling station environment. The use of a polling station with the scheme provides a period of time in which secret information may be transferred from the Vendor domain to a voter which is not visible to an external observer. The secret information may be used by the voter to confirm that the Vendor domain has correctly processed their vote without being able to prove the secret information to an external observer, since no receipt with the secret from the Vendor domain is provided to the voter.

Figure 5.15 illustrates the setup for the polling station adaption of the mCESG scheme. The voter enters the supervised voting environment, i.e. a polling station, and authenticates themselves. The voter is provided with credentials of the same form as the mCESG scheme and enters the booth from where they are able to observe a presentation of the contents of the bulletin board. The voter votes in the same manner using the provided voting device (Step 1). The Vendor domain receives the vote via an anonymous channel and forwards the rid to the bulletin board, where the voter observes it from within the polling booth. If the voter is satisfied that the correct rid has been published, they exit the polling booth, deposit the credentials in a ballot box and exit the polling station. Later, the voter confirms that the correct candidate name has been published next to the rid value they previously viewed. If an incorrect rid value has been published, the voter may make a complaint to the Vendor domain, requesting that their voting credentials be recovered from the ballot box for inspection.

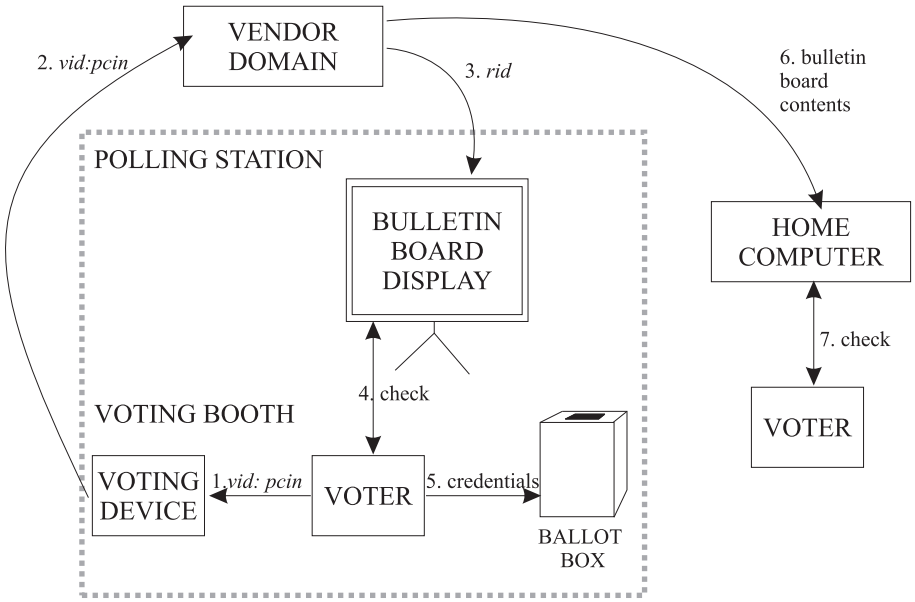


Figure 5.15: Polling station adaptation of the mCESG scheme. The voter enters the supervised environment, aquires their voting credentials and casts a vote on the voting device (1). The voting devices sends the $vid : pcin$ vote to the Vendor domain (2), which posts the rid value for the vote on a bulletin board visible within the polling station (3). The voter checks that the correct rid value has been posted on the bulletin board (4) and then deposits the voting credentials in a secure container (5). The voter then leaves the polling station. Later, the voter can check that the correct candidate has been posted on the bulletin board for the rid value of their vote (7,8). However, unlike the original mCESG scheme, the voter cannot use the voting credentials to convince an attacker that the rid on the bulletin board is for their vote.

For some voting contexts, it may be considered desirable to separate the credential information from the voter's identity, prior to providing the voter with the credential document, if the security of the ballot box is uncertain. This process, whilst not preventing correction of an rid-candidate association on the bulletin board, protects the anonymity of the voter. This process also does not prevent the voter requesting a correction to the bulletin board via a proxy in order to protect their anonymity.

The use of a polling station for vote casting reduces the convenience of the mCESG scheme in order to provide a receipt free vote verification mechanism. The use of the polling station scheme may be necessary in contexts where the threat of voter coercion or vote buying is considered greater than the potential for low participation due to inconvenience of attending a polling station. A potential compromise between the original scheme and the polling station adaption would be to provide both remote channels and polling station environments over which vote casting may be undertaken. This compromise may be effective in circumstances where otherwise coerced voters are able to take advantage of the additional security of the supervised environment. The precise choice of receipt free scheme will depend on the requirements of the voting context in which the scheme operates.

5.5.6 Receipt Free Scheme 2

Section 5.5.4 describes an adaptation of the mCESG scheme which is receipt free for most voters, leveraging the involvement of candidates in the checking procedure. The adaptation is problematic since voters do not know prior to tallying whether they will need to check their votes for correctness. Similarly, Section 5.5.5 describes a polling station adaptation to the mCESG scheme which provides receipt freeness to all voters, at the cost of not providing the useful properties (mobility, convenience) of a remote voting scheme. This section discusses an adaptation to the mCESG scheme which provides a pollsterless remote voting scheme which is receipt free. The disadvantage of the scheme to be presented is that voters are required to vote n times in order to be assured with probability 1-1/2^n that their vote has been counted accurately.

The intuition for the scheme adaptation is that voters engage in a multi-round cut and choose protocol with the Vendor domain. The cut and choose protocol commits the Vendor domain to either cheating the voter or processing their vote honestly, before the Vendor learns if the voter wishes to decommit from and then check the value which the Vendor has committed to. The Vendor is committed to the value not revealed to the Voter by interactions with other, autonomous domains of the Election Authority. The last vote cast by the voter (and not subsequently decommitted from) is taken as the voter's choice.

The receipt free scheme adaptation described below thus takes its inspiration in particular from the Neff cut and choose techniques and the Prêt à Voter scheme's use of permutation of candidates described in Section 2.5.4. The adaptation applies the cryptographic cut and choose techniques of those schemes to the basic mCESG scheme.

The adaptation to the scheme does still retain the *pollsterless* property of the basic mCESG scheme. However, voters are required to be able compute Chinese addition[2] of one time pads and encrypted rid values in order to be able to identify their rid on the bulletin board when the Election Authority decommits from it. This requirement is greater than the essentially computationless (from the voter perspective) mCESG scheme, but less than that for conventional cryptographic protocols or the Malkhi et al scheme.

5.5.6.1 Voting Credentials

The voter receives a set of credentials as illustrated in Figure 5.16. The credentials are similar to those for the basic mCESG scheme. However, rather than receiving a single PCIN and RID value for each candidate, the voter receives N pairs of these values for each candidate.

Voting is similar to that for the basic mCESG scheme. The voter chooses a candidate and sends their VID number and one PCIN value for that candidate to the Vendor Domain.

[2] Additions of values are not carried to the left-ward column of digits.

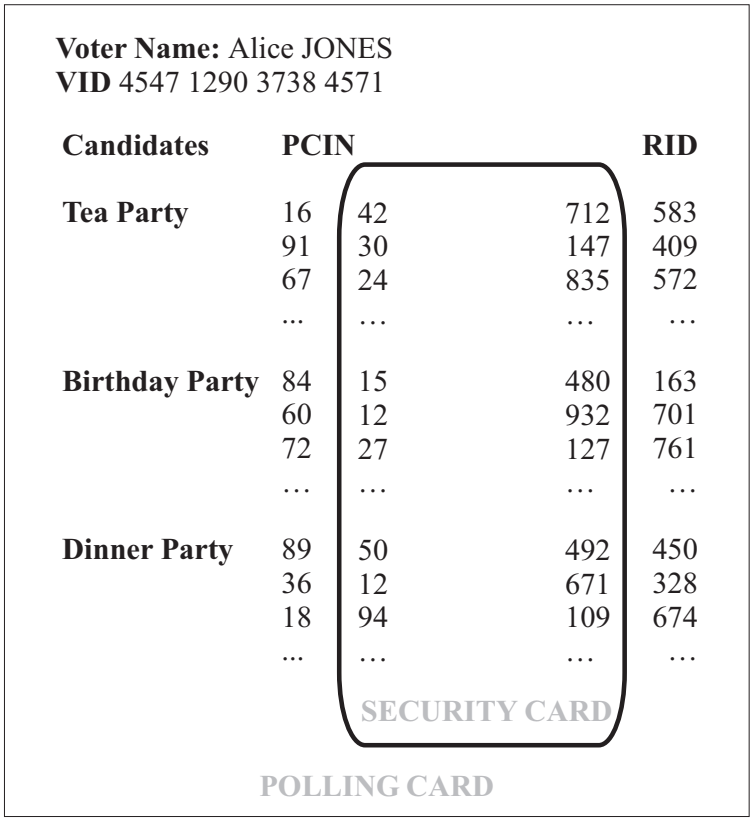


Figure 5.16: Voting credentials of the cut and choose receipt free adaptation of the mCESG scheme. The voter is supplied with N pairs of PCIN and RID credentials per candidate.

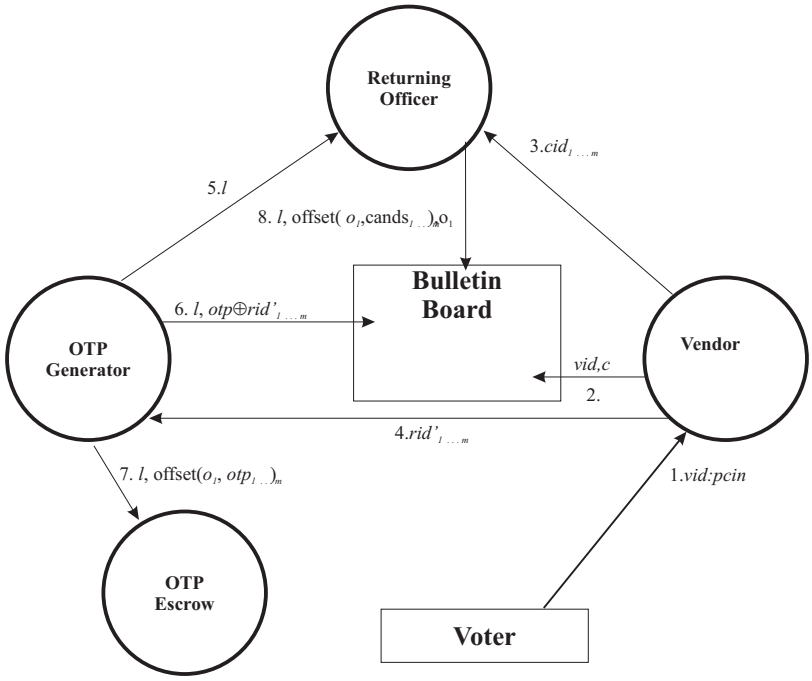


Figure 5.17: Initiation of the cut and choose mCESG scheme adaptation. The domains of the mCESG scheme interact to produce on the bulletin board a one time pad encrypted rid value, a set of m-1 encrypted values and a permutation of candidates against the rid and random values.

5.5.6.2 Vote Processing

To process $vid : pcin$ messages received in the adaptation of the mCESG scheme, the Election Authority incorporates two further domains denoted *One Time Pad (OTP) Generator* and *One Time Pad Escrow*. Figure 5.17 illustrates the processing of vote messages by the re-organised domains, omitting the Registration Officer, whose role is unchanged. Vote processing is then as follows.

1. When a vote message is received the Vendor domain, the corresponding rid value is calculated.

2. A set $m - 1$ random values of length len_{rid} is selected. The calculated rid value from step 1 is appended to the set and the new set is then denoted $rid'_{1...m}$. The set is then randomly permuted and sent to the OTP generator. The result is that the OTP Generator is unable to determine which member of $rid'_{1...m}$ is a genuine rid value.

3. The Vendor domain sends a set of cid values to the Returning Officer, such that if the voter used the kth $pcin$ value generated for the voting credentials, then the kth cid value generated for each of the candidates is passed to the Returning Officer. The unused kth voting credentials are now invalid for further vote casting. The Returning Officer thus does not know which cid value an rid value has been generated for.

4. The OTP Generator informs the Returning Officer which position on the bulletin board to write details into.

5. The OTP Generator generates a *one time pad* otp values and xors these against each rid' value. The OTP Generator writes the resulting cipher texts to the bulletin board.

6. The OTP Generator sends the otp values to the OTP Escrow, but not the position on the Bulletin Board for which they were used.

7. The Returning Officer offsets the list of candidate identities by a random value o_1 and writes both this value and the permuted candidate identities to the bulletin board in the lth location specified by the OTP Generator.

8. The Vendor domain announces it has received a new vote message for a particular vid value and sends the current count of vote messages for that vid value to the bulletin board. This prevents the Vendor domain 'hoarding' vote messages to see if the voter will decommit votes.

At this stage in the protocol, the voter has registered a vote on the bulletin board, with their receipt number for the vote encrypted under a one time pad and hidden in a permutation of invalid receipts and votes. Figure 5.18 illustrates the state of the vote list area of the bulletin board after the voter first casts a vote, assuming that the voter has used the credentials to cast a vote for the Birthday party using the 1st $pcin$ value.

	otp	$\oplus$	$otp \oplus rid'$	$\oplus$	rid'	=	Candidate
Offset = 1		$\oplus$	601474	$\oplus$		=	Tea Party
		$\oplus$	129023	$\oplus$		=	Birthday Party
		$\oplus$	376740	$\oplus$		=	Dinner Party

Figure 5.18: State of the bulletin board after vote casting in the cut and choose adaptation of the mCESG scheme. The diagram illustrates the lth entry on the bulletin board after the Election Authority commits to a vote cast by a voter using the credentials illustrated in Figure 5.16.

5.5.6.3 Decommittment and Checking

Prior to the close of poll, the voter may choose to decommit from a previously cast vote, confirm that the domains of the Election Authority did not attempt to cheat them and commit to a new vote message. To do this the voter waits until their previous vote was acknowledged (by the increase in vote count for their vid) and sends a new vote message to the Vendor domain. The Vendor domain then requests that the OTP Generator indicate which position on the bulletin board stored the previous vote. The OTP does this and writes the otp values to the Bulletin Board. The voter is then able to decrypt each of the $otp \oplus rid'$ values, identify the genuine rid and determines that the correct candidate is offset by the amount published by the Returning Officer from the rid value. The new vote message can then be processed as normal. Figure 5.19 illustrates the state of the Bulletin Board after the voter decommits from the vote recorded on the bulletin board in Figure 5.18.

5.5.6.4 Tallying

Following the end of voting, the choice of each voter needs to extracted from the bulletin board without either violating the receipt freeness property of the scheme or permitting the domains of the Election Authority to decommit from voter's choice (and thus violate the accuracy of the final tally). Figure 5.20 illustrates the interaction between the domains to yield the votes cast. For each committed vote at the end of tallying, the Vendor domain indicates the position of the genuine rid value. The OTP Generator then indicates the

	otp	$\oplus$	$otp \oplus rid'$	$\oplus$	=	rid'	Canddidate
Offset = 1	568909	$\oplus$	601474	$\oplus$	=	169373	Tea Party
	126798	$\oplus$	129023	$\oplus$	=	245711	Birthday Party
	756803	$\oplus$	376740	$\oplus$	=	480163	Dinner Party

Figure 5.19: State of the bulletin board after a vote is decommitted in the cut and choose adaptation of the mCESG scheme. The diagram illustrates the lth entry on the bulletin board after the Election Authority decommits to a vote cast by a voter using the credentials illustrated in Figure 5.16.

location of the vote on the bulletin board. The OTP Escrow decrypts the non-genuine rid values for the vote to demonstrate to the Vendor domain that the OTP Generator has not attempted to cheat. The genuine rid value remains encrypted under it's otp value to prevent the voting credentials being employed as a receipt.

5.5.6.5 Summary

The scheme described above demonstrates the incorporation of techniques employed for cryptographic voting schemes into a remote pollsterless voting scheme in order to yield a receipt free adaptation. However, the scheme adaptation does imply some considerable extra complexity for the voter. The voter is required to undertake multiple rounds of voting to gain confidence that their vote is being recorded accurately. In addition, the voter must be able to perform chinese addition in order to identify their vote on the bulletin board. It is noted that pollsterless schemes are intended to limit the computation required of the voter. However, the adaptation described here reflects both the flexibility of the basic mCESG scheme, together with the compromises that must be acknowledged when selecting to use particular adaptations.

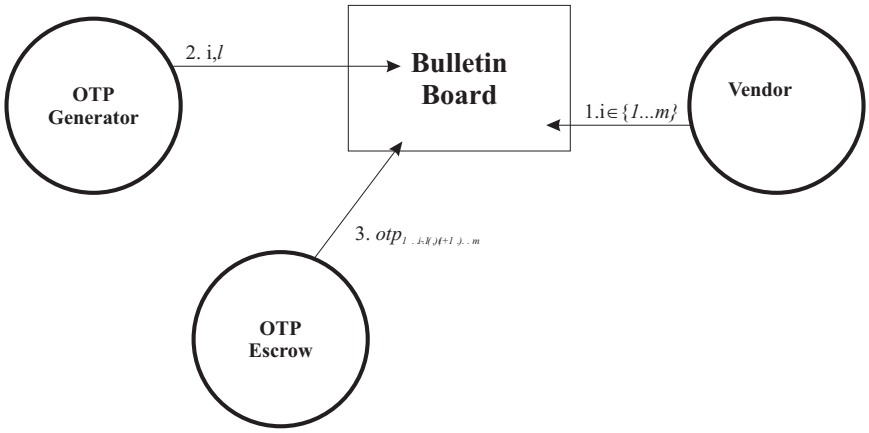


Figure 5.20: Tallying phase of the cut and choose adaptation to the mCESG scheme. The Vendor domain commits to the location of rid values within uncommitted vote records on the bulletin board. The OTP Generator also commits to a location for each vote the Vendor has now committed to. The OTP Escrow reveals the random values for each vote to demonstrate to the Vendor domain that it has not been cheated by the OTP Generator.

5.6 Conclusions

This chapter has presented a novel class of pollsterless remote voting schemes by substantially modifying and correcting a flawed existing scheme. The mCESG scheme retains useful pollsterless properties of the CESG scheme whilst introducing extra useful properties including voter verifiability and undeniability. Further, the monolithic Setup module of the CESG scheme formalisation was re-designed to provide protection of the association between voters and votes within an Election Authority functionality distributed across autonomous domains. A range of further adaptations to the basic mCESG scheme were presented illustrating that mCESG represents a novel class of pollsterless remote voting schemes.

Chapter 6

Evaluation of the mCESG Scheme

Overview

This chapter presents an evaluation of the mCESG scheme discussed in the previous chapter. To present an evaluation of the mCESG scheme, a prototype of the basic mCESG scheme is implemented. The implementation decisions describe in Section 6.2 illustrate the distinction between a voting scheme and a voting system as discussed in the framework proposed in Section 2.2. The evaluation considers the mCESG scheme using several approaches including an evaluation of the scheme with respect to requirements discussed in Chapter 3, a threat analysis of the scheme from a system implementation perspective, similar to the analyses of 'hybrid' schemes discussed in [75, 124] and a user acceptance study of the scheme employing videotaped activity scenario directed focus groups.

6.1 Introduction

The previous chapter described the mCESG pollsterless remote voting class of schemes as a correction to the flawed CESG scheme [18]. Whilst the CESG scheme incorporated desirable properties of pollsterless REV schemes, the mCESG scheme provides voter ver-

ifiability and a distribution of setup parameters across autonomous domains. This chapter is divided into sections as itemized below, providing an evaluation of the mCESG scheme as proposed in the previous chapter. This chapter comprises several aspects:

- An implementation of the basic mCESG scheme as a demonstrable system. The implementation is necessary in order to conduct a user-acceptance study and an analysis of the scheme from a system perspective.
- An evaluation of the mCESG schemes with respect to the requirements described in Chapter 3.
- A user acceptance study using videotaped scenarios and focus group response elicitation similar to Little et al [82]. The user acceptance study also notes informal observations of user actions during live demonstrations of the system as a precursor to further user acceptance evaluation.
- A threat analysis of the CESG scheme in terms of potential for collusion between autonomous domains of the Election Authority.

The work presented here is not intended to provide a complete formal evaluation of the mCESG scheme's suitability for implementation in the UK public election context. Rather, the evaluations presented are exploratory, illustrating known aspects of the UK requirements context which the schemes satisfy and identifying potential issues that must be considered in future adaptations to the mCESG scheme prior to implementation.

6.2 Prototype mCESG Scheme Implementation

This section describes the development of a prototype implementation of the mCESG pollsterless remote voting scheme as a remote electronic voting system. An initial step in the evaluation process of the mCESG *scheme* was to develop a voting system which could be employed for the various evaluation exercises and in particular, the user acceptance study.

The prototype was developed in Java, since this language provides convenient support for interactions within the Election Authority and between the voter and the election authority and is a common choice for software development projects. There were several implementation issues to be considered with respect to the prototype mCESG system which impact the evaluation studies described in later sections of this chapter. The design considerations are discussed below.

6.2.1 Election Authority Implementation

Ideally, the four domains of the election authority should be implemented by independent development teams in order to mitigate the risk of inter-domain collusion which violates the purposes of task separation. However, for the practical purpose of implementing a prototype architecture for each domain, a single implementation is sufficient. Initially, a generic election authority domain was implemented to conduct the secure (permissible) communication between domains. Secure communication was implemented using the Secure Socket Layer implementation provided in the `javax.net.ssl` package of the Java language SDK. Message handling was left un-specified in the generic domain implementation. Each domain of the election authority implemented specific message handling functionality for that domain's purpose. In order to communicate, domains were required to mutually authenticate. Thus prior to an execution of the system, each domain needed to be provided with the public key certificate of the domains to which it will send and receive messages. This operation was deliberately left as a manual operation such that certificates will be exchanged via courier or similar prior to initiation of communication.

The Registration Officer, Returning Officer and Vendor domains are required to generate voting credential values using one-way hash functions. To implement this functionality, a utility generator module which accepted arbitrary strings and generated hashes represented as integer strings of required length was implemented. Generation of credential values was implemented using the `javax.crypto` framework of the standard Java SDK. The credential generation function was implemented independent of cryptographic hash algo-

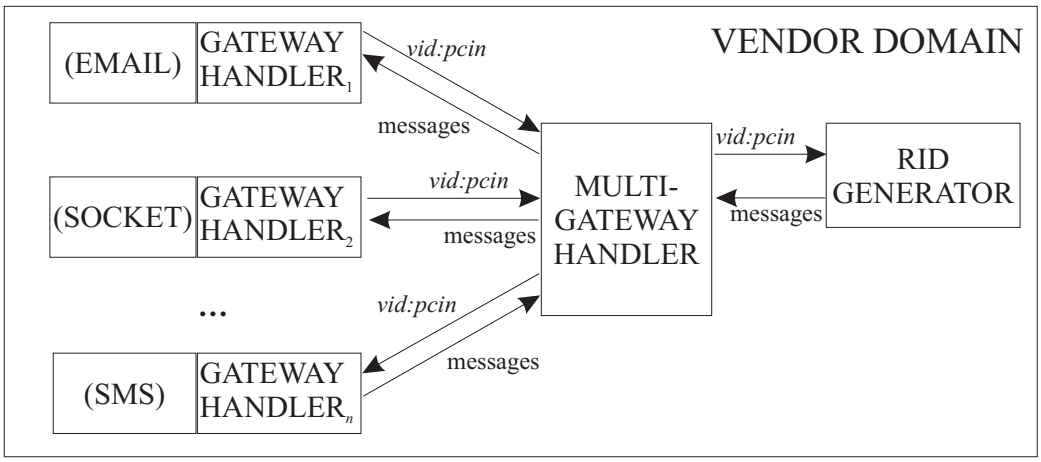


Figure 6.1: Gateway and Vendor domain interaction of the prototype mCESG system. A gateway listener harvests votes from individual gateways.

rithm. The MD5 message digest algorithm was employed during development and testing, although since MD5 is not a keyed algorithm this choice would not be appropriate for an implementation of the scheme employed for live elections.

6.2.2 Provision of Available Voting Channels

To demonstrate the pollsterless property of the mCESG voting scheme, the Vendor domain was implemented to collect votes from arbitary gateways. The particular gateways used to collect votes could be specified during system configuration without modifying the Vendor domain implementation. Figure 6.1 illustrates the architecture adopted for the Vendor domain. The vendor initiates a gateway listener module with which available gateways register.

The gateways implemented for the prototype were:

- A TCP socket listener. This gateway was most useful for early testing of the Vendor domain functionality, since provision of a Socket gateway for demonstrations would require voters to interact with the socket listener. To simulate large scale voting, a *VoteBot* module was also implemented to collect credentials generated by the election

authority and cast random votes on their behalf. The VoteBot interacted with socket gateway in order to send votes back to the Vendor domain.

- Email - a simple POP server.
- Bluetooth serial port - A gateway which listened for serial connections on a port used by a bluetooth adaptor on the gateway node. The gateway forwards received messages to the socket gateway described above. The gateway was useful for live demonstrations of the mCESG prototype system. A client user interface was implemented for a PDA which simulated the functionality of a mobile phone interface. The client user interface was implemented using the SuperWaba SDK [59].
- SMS messaging - implemented using Application Programming Interfaces (APIs) for a Nokia PCIMIA GSM phone card developed for the GLOSS project at the University of St Andrews[32]. Text messages could be sent to the gateway node via the phone card from any SMS enabled mobile phone.

The Vendor domain interacts with the gateways via the listener module, which in turn interacts with each type of gateway through a standardised interface. Thus, from the perspective of the Election Authority, the underlying channels through which votes are collected is transparent.

6.2.3 Credential Generation and Delivery Format

The implementation of the mCESG scheme required the choice of a secure, authenticated channel for communication of the voting credentials to a voter from the domains responsible for delivery. The system was designed to permit re-configuration of secure credential channels without modification to the mCESG scheme. Channel implementation was undertaken such that the same channel type could be used by either domain responsible for credential delivery. Three channels were chosen for implementation, only one of which constituted a secure authenticated channel:

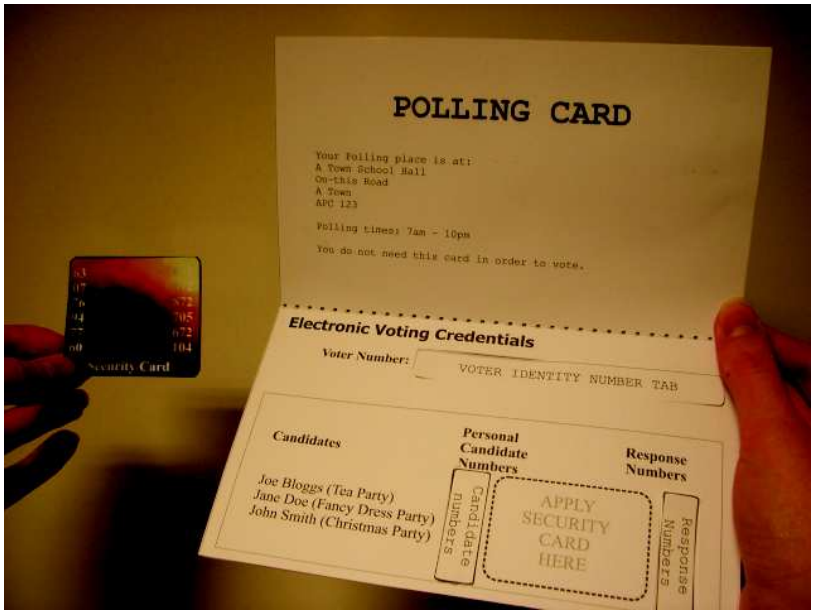
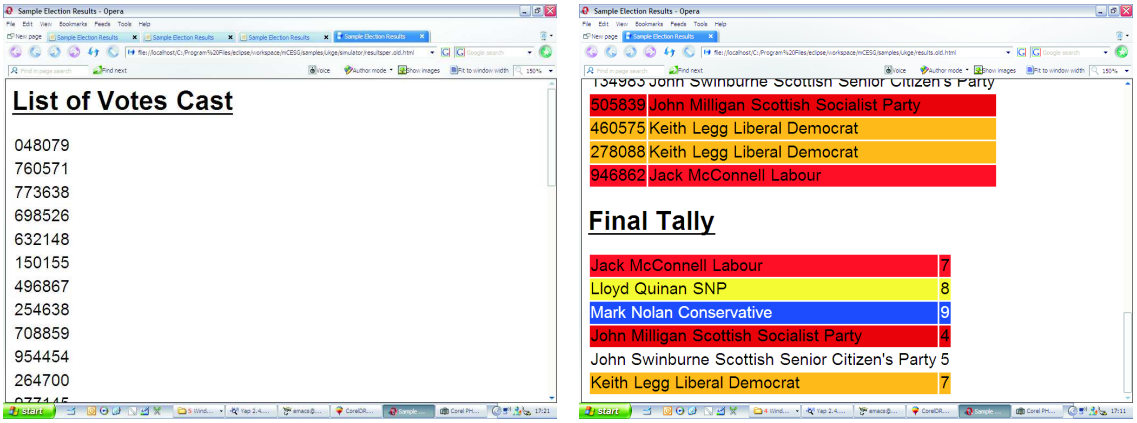


Figure 6.2: Secure stationary mock-up of the mCESG voting credentials. The credentials are printed to card and then modified to convey the impression of secure stationary, similar to that used for payrolls. The security card is modifed to give the appearance of a plastic card.

VoteBot delivery channel: This was implemented to send credentials to the VoteBot node implemented to simulate a large number of voters. The channel was implemented using TCP sockets and enabled testing of the prototype against a large number of votes cast without employing a larger number of testers. The VoteBot received votes from the delivery channel and after a random delay period, cast a random vote constructed from the credentials.

Email delivery channel This was used to conduct convenient demonstration elections without excess waste of printed credentials. The email delivery channel is appropriate for use in elections where security of credentials is less important than convenience in order to facilitate participation. Voters were required to provide email addresses during registration if this configuration was to be usable. Such a setup is useful for demonstration elections, for example, like election of class representatives within a university. The email delivery medium could be coupled with the email voting channel described in Section 6.2.2



(a) During Vote Casting (b) After Tallying

Figure 6.3: The mCESG prototype implementation bulletin board. The figure illustrates the bulletin board as used during demonstrations both during vote casting and after tallying.

A printed delivery medium This was used for demonstration of the scheme during live demonstrations where the security of the delivery channel needed to be emphasised. The printed credentials were then modified to give the appearance of payroll stationary. Figure 6.2 illustrates the mocked-up credentials used in the user acceptance study.

Recall that the prototype system was implemented for evaluation purposes. For the user acceptance study described in Section 6.4 and for live demonstrations, the printed delivery format provided usable props which conveyed the purpose of the credential delivery in a secure, authenticated form.

6.2.4 Bulletin Board

To implement the bulletin board of the mCESG scheme, a simple web-page generator was employed. The web-page listing all votes cast during the election was placed in a universally readable location on the node hosting the Vendor domain.

Figure 6.3 illustrates the bulletin board web page employed for the demonstrations of the

scheme. When the election authority generates the list of votes cast after tallying, each row of the tally on the web-page is colour coded by the candidate represented, allowing a manual tally of votes to be computed more easily.

6.2.5 Hardware Configuration

Two configurations of the mCESG prototype implementation were developed. An initial configuration of the system employed a single node to host all four domains of the election authority and a single gateway. The gateway chosen listened for serial port connections over which a PDA connected to the PC via Bluetooth. A software client on the PDA represented a mobile phone interface to simulate employing SMS messaging to cast a vote. The single platform configuration allowed convenient development, testing and demonstration of the system.

A second configuration of the mCESG prototype system was developed using five nodes to host each of the four election authority domains and two gateways. In the second configuration, two gateways were hosted on a single node, providing both an SMS and an SMTP gateway. As per the design of the mCESG scheme the two gateway hosts forwarded messages to the Vendor domain separately. Since the domains of the election authority were now operated on separate hosts, a procedure for transferring the public key certificates for each domain was implemented.

Note that the prototype implementation was not modified between deployment in the two alternative configurations. The configurations were also dynamic, such that additional gateways could be initiated on further nodes without modification of the system itself. Configuration of the Vendor would be modified to accommodate the additional gateway. The configuration exploits the flexibility of the mCESG scheme design.

6.3 Requirements Analysis

The purpose of this Section is to evaluate the mCESG scheme and its adaptations with respect to the requirements discussed in Chapter 3 for the UK public election context. The Section discusses the extent to which the prototype system fulfills the requirements identified in Chapter 3.

1. **The voting system must allow a vote to be cast from an unsupervised location.**

   The prototype implementation of the mCESG scheme demonstrates that voting may be undertaken from remote locations, using simple networked devices.

2. **The voting system must minimise the number of interactions required to cast a vote.**

   To *cast* a vote, the voter must interact with the election authority once. The two step adaptation to the scheme introduces an extra interaction such that a voter requests voting credentials, authenticates and then casts a vote in order that the *experience of voting* is comparable to that in the existing UK voting system. To *verify* a vote, the voter must interact with the Vendor domain of the mCESG scheme two further times.

3. **The voting system must allow vote casting to occur via a range of channels in order to increase accessibility by a range of votes.**

   The prototype implementation of the mCESG scheme demonstrates that votes may be cast over multiple channels. The channels implemented are SMS, email, Bluetooth serial port (for simulation of SMS) and TCP socket (for testing purposes). Demonstrations of voting were conducted using a PDA device communicating over Bluetooth, whilst the user acceptance study used an SMS channel for voting.

4. **The voting system must not require a voter to possess special purpose equipment in order to cast a vote.**

   The simple protocol of the scheme permits votes to be cast over a range of channels. Votes may be cast using a mobile phone equipped with SMS messaging, or from an

email account. No special purpose equipment are required for this purpose.

5. **A voting system must permit voters to express an unordered selection of options, within some maximum, as a vote in a Referendum SP or Closed List electoral system.**

   The basic mCESG scheme permits a single option to be selected as a preference. The adaptation to the scheme described in Section 5.5.1 permits a voter to express a vote as several options selected from a proposal. The size of the vote is linear in the number of options selected.

6. **A voting system shall allow a voter to express a vote as an ordered selection of options within some maximum defined by the electoral system.**

   The adaptation to the basic mCESG scheme described in Section 5.5.2 permits a voter to express a vote as several ordered options selected from a proposal. The size of the vote is linear in the number of options selected.

7. **A voting system shall allow a voter to express two votes in a mixed member electoral system, as two unordered votes.**

   Provision of credentials for the two separate SP votes as implemented in the basic mCESG scheme may be employed to accommodate a mixed member electoral system. The credentials may still be delivered as for the one SP electoral system.

8. **An external observer of the voting system must not be able to associate a vote with a voter except when authorised by an election court judge, in parallel to the existing UK voting system.**

   The secrecy requirements described in Section 3.4 adopts the threat model associated with postal voting for the UK context, that is, a voter will not cooperate with an attacker in order to demonstrate how they voted. The mCESG scheme fulfills this requirement, in that, providing that the voter does not share their credentials with an attacker, the attacker will not be able to learn the choice a voter makes. The credentials remain a secret shared between the voter and collectively the domains of

the Election Authority. This property holds even if the voter's vote is intercepted during communication to the Election Authority, as opposed to the existing postal voting system.

9. **An external observer of the voting system must not be able to learn the value of a vote prior to the end of voting.**

   This requirement refers to the inability of an external observer to learn a partial ongoing tally of results prior to the end of voting. If an observer could learn partial results, voters who had not yet participated may be influenced differently from voters who have already cast their vote. The mCESG scheme maintains the storage of votes and the candidate identities they correspond to separately until after tallying. The tallying operation itself requires cooperation between the Vendor and Returning Officer domains, such that a partial tally of results cannot be revealed without collusion between these domains during tallying.

10. **An external observer of the voting system must not be able to learn the aggregate or partial aggregate of votes prior to the end of voting.**

    The fulfillment of this requirement follows from the previous. Further, since all candidate identity values stored by the vendor are unique, the Vendor is not able to produce an anonymous tally without the collusion of the Registration Officer. An anonymous tally is of use to an attacker since results from successive elections may change only marginally, enabling an observer with access to a partial tally to associate each tally with a particular candidate.

11. **The voting system must permit a vote to be traced to a voter identity under parallel circumstances to the existing UK voting system.**

    Under normal operation a vote cannot be associated with a voter because voter identities are stored by the Registration Officer domain and not used for the processing of votes. However, in circumstances where the Vendor cooperates with the Registration Officer, a vote cast using a particular set of credentials may be identified and removed from the bulletin board of the mCESG scheme. In circumstances where several votes

are identified as being cast fraudulently, votes may be removed anonymously (if desirable) from the bulletin board, since the Returning Officer may indicate to the Vendor the VID values of votes to be removed, rather than the identities of the voters themselves.

12. **A list of voters participating in an election must be published after the announcement of results.**

    The mCESG scheme specifies that the Vendor domain provide the Registration Officer domain with a list of VID values of votes cast. The corresponding identities of voters are then published by the Returning Officer, without linking individual votes to voters.

13. **The voting system must accurately record the choice intentions of the voter.**

    The prototype implementation of the mCESG voting scheme does not permit voters to spoil their votes, that is record a vote which is not valid for a candidate. The scheme does provide a voter with the ability to cast an incorrect vote by sending the wrong candidate number to the Election Authority. The scheme does however provide voters with the opportunity to check that the correct receipt value for their candidate has been published prior to votes being tallied.

14. **The voting system must permit voters to confirm their choice at some point prior to final committment to the vote.**

    The scheme does however provide voters with the opportunity to check that the correct receipt value for their candidate has been published and later that the correct candidate is published next to that receipt value after vote casting is complete.

15. **The voting system must store all votes cast without modification prior to tallying.**

    The accurate storage of votes prior to tallying is dependent upon the implementation of the secure bulletin board assumed for the mCESG scheme as a secure authenticated broadcast channel. If the bulletin board is not secure then the Vendor domain

is able to publish and then revoke receipt values prior to tallying. The prototype implementation of the voting scheme itself does not implement the bulletin board in a secure manner. However, Section 7.2.1 discusses how the bulletin board may be implemented in a distributed manner within the existing UK voting system infrastructure to prevent revocation by the Vendor.

16. **The tally of votes must be accurate with respect to votes stored.**

    The mCESG scheme publishes the values of individual votes permitting external observers to verify the accuracy of the corresponding tally with respect to the rules of the relevant electoral system.

6.4 User Acceptance Study

This section describes a user acceptance study conducted as part of the evaluation of the mCESG prototype system. The study was undertaken in conjunction with psychologists at the University of Northumbria's Psychological Aspects of Communications Technology (PACT) laboratory. Design of the videotaped scenario described in Section 6.4.3 was undertaken by the author, whilst the organisation of focus groups and analysis of results was provided by psychologists at the PACT laboratory. The author also participated in the categorisation of focus group participants and the conduct of focus groups themselves under the supervision of psychologists at the PACT laboratory. As this thesis has discussed and this study illustrates, the investigation of voting systems requires interdisciplinary expertise.

6.4.1 Motivation

A substantial amount of work has been undertaken into user-perceptions of remote electronic voting (REV) systems. A study for the UK Office of the e-Envoy investigated user perceptions towards electronic voting systems in general, noting that introducing new technologies into democratic structures met with only modest enthusiasm, the use of electronic

voting was seen as more relevant than electronic participation systems [27]. In addition the study found anecdotal evidence to suggest that voters were more interested in e-voting once the various channels had been discussed. Oostveen investigated voter's understanding of the security properties of voting systems [108]. The study noted that voters are willing to accept statements from voting client pollsters that their vote has been successfully collected without requiring demonstrable evidence to support the statement [108, 109].

The study of the mCESG scheme presented here is believed to be novel, since there has not been a published study that investigates voters' acceptance of pollsterless voting scheme which permit highly mobile voting (voting can take place on any connected device and in any public location) and also permits voters to confirm that their vote has correctly contributed to a tally of votes. In addition, we are not aware of previous uses of scenario-directed focus groups for evaluation of voting schemes, although 'think aloud' techniques [143] have been employed to evaluate the interfaces of DRE machines [6].

Whilst the desirability of receipt-freeness has been asserted as a desirable property for cryptographic voting schemes, that desirability has not been tested, and it is noteworthy that the existing UK remote voting system, postal voting, permits a voter to construct a receipt for their vote (by photocopying the paper ballot, or transferring the paper ballot to an attacker) and the system is used satisfactorily and regularly for UK public elections.[1] The study presented here investigated whether the voter is able to understand why the information presented to them constitutes evidence that their vote has been counted and also whether the provision of evidence is considered valuable by voters. The study therefore constitutes an *exploratory* evaluation which establishes qualitative results based on the responses of participants, rather than a *validation* evaluation, which would place a greater emphasis on quantitative data.

[1] Disputes have arisen from the use of postal voting in the UK, including Hackney in 1998 and Birmingham in 2004 [87]

6.4.2 Demonstration

As a preliminary exercise before conducting the full user acceptance study, the mCESG prototype implementation was employed in live demonstrations. The exercise provided an opportunity to identify issues that would be raised in the scenario directed focus group exercises described below.

The mCESG prototype was configured to the single node version described in the previous section, using the Bluetooth connected PDA to simulate mobile phone SMS telephony functionality. The bulletin board was displayed on an overhead projector in a laboratory, such that users could cast a vote and observe the results in one location. The VoteBot module of the prototype was employed to simulate a larger number of voters for each user.

The demonstration occurred over two days, the first day to members of the School of Computer Science at the University of St Andrews and the second to members of the public invited to the School for an open day. Users were provided with a brief explanation of the motivation for the system, emphasising the inconvenience of attending a polling station, and an explanation of how to vote. Each user was provided with a mocked up, pre-assembled voting credential and invited to use the PDA to cast a vote. The bulletin board displayed on the projector could then be monitored for checking purposes. The users were free to discuss the voting system with demonstrators.

One particular phenomenon from the live demonstrations was the tendency of users to attempt to send their VID value to the election authority by itself, rather than concatenated to a PCIN value. The explanation for this behaviour is that a user in the UK voting context expects voting to be a two-step process, with authentication followed by choice expression. The motivation for the two-step adaptation to the mCESG scheme described in Section 5.5.3 is now clear. An aspect of this potential for two step voting is that the number of interactions to vote increases, that is the complexity increases from the voter's perspective, although the adaptation aids usability.

6.4.3 Study Design

The user acceptance study was undertaken within a broader investigation by the PACT Laboratory of psychological aspects of online privacy and trust. The study employed videotaped scenarios in order to direct focus group discussion to elicit responses.

The initial objective of the study was to develop a videotaped scenario which captures the issues described in the previous section with respect to the prototype mCESG system as implemented. To begin this process a storyboard consisting of three scenes divided into thirteen images and captions was developed. The three scenes illustrate three phases of an election in the UK from a voter's perspective - registration, vote casting and tallying. The registration phase is unrelated to the prototype mCESG system itself, but is included to provide the focus groups with a complete scenario. The registration phase illustrates the voter filling her personal details (name, address etc) into a web-form. The second, vote casting scene, covers the voter receiving and compiling voting credentials as described in Section 6.2 and the casting of a vote using SMS messaging on a mobile phone as the communication channel in a public location. The voter also uses a computer located in an office to complete the first vote checking phase during this scene. The final scene of the scenario illustrates the online vote tallying and checking procedure. Appendix A illustrates the storyboard that was developed for the mCESG scenario.

Once the storyboard had been finalised, a script for the scenario was generated, describing the voter's behaviour and actions during the three scenes. The script was then passed to a media production company, which reduced the volume in order to complete the three scenes within a shorter period of time. The revised, summarised script was then approved before being filmed by the production company employing professional actors.

The procedure for initiation and conduct of the focus groups is as described in [83] and summarised here for completeness. 304 participants from the Newcastle upon Tyne region were divided into 38 focus groups (ranging in size from 4 to 12 people). Participants were categorised in terms of:

- Age
- Gender
- Disability
- Level of educational achievement
- Technical stance (technically knowledgeable and also attitude towards technology use).

Participants were allocated to focus groups as a result of this categorisation in order to encourage discussion. Prior to attending the focus group, participants were provided with information as to the project's objectives.

Each focus group session lasted ninety minutes and covered four different scenarios (e-voting, shopping, health and finance), of which the e-voting scenario was first. The scenarios were shown to the focus group first, followed by a discussion on each of the topics, directed by a moderator who was a member of the PACT laboratory. Each focus group was tape recorded and the ensuing conversations later transcribed. The transcripts then underwent qualitative analysis and open coded, identifying several categories of opinion.

6.4.4 Results

Table 6.1 summarises focus group responses to the videotaped scenario which they viewed. The focus groups were aggregated into three classifications by the PACT psychologists - non-technical experience, technical experience and a separate disabled group. The non-technical and technical groups were further sub-divided according to level of education (low and high) reached. The categories listed for responses are grouped in terms of social trust/security and privacy issues.

6.4.4.1 Social Issues

Exclusion Refers to the potential for some societal groups to be unable to use the voting system.

Social Interaction The desirability of communal properties of polling station voting systems.

Social/Moral consequences. Whether the mCESG system would trivialise voting or reduce sense of responsibility for the democratic process.

Convenience Whether the scheme permits voters 'with busy lives' to participate in voting.

Encourage young voters Whether the participants thought the viewed system would improve participation amongst younger voters.

Mobility The advantage of not having to attend a polling station to vote, which is related to convenience.

Motivation Whether the voting system viewed by participants would reduce the likelihood of participation, which is related to the question of social/moral consequences.

6.4.4.2 Trust

Security That the system does not appear secure, and therefore reduces trust.

Verification Whether the ability to verify a vote as having been counted was appreciated and trusted.

6.4.4.3 Privacy Concerns

Informational Refers to whether participants were comfortable with personal information and voting intention being processed electronically.

Topic	Technical		Non-Technical		Disabled
	Low	High	Low	High	Participants
Social Issues					
Exclusion	-	-	-	-	-
Social Interaction	-	-	-	-	-
Social/Moral Values		-	-	-	
Convenience	+	+	+	+	
Encourage young voters	+		+	+	
Mobility	+	+	+	+	+
Motivation		-	-	-	
Trust					
Security	-	-	-	-	-
Verification	-	-/+	+	-/+	
Privacy Concerns					
Informational	-	-	-	-	-
Physical	-	-	-	-	-
Tracking/Anonymity	-	-	-	-	-

Table 6.1: Results of the mCESG user acceptance study. The table categories positive and negative reactions to videotaped scenario of the mCESG scheme from focus groups. Focus groups are categorised according to technical experience and level of educational achievement, as well as including separate information on a group of disabled participants. Reactions are grouped by social, trust and privacy issues. A '+' indicates the focus group gave a positive response on a category. A '-' indicates that the group gave a negative response on a category. '+/-' indicates that both positive and negative issues were discussed by the group. No symbol indicates that a topic was not raised by a group.

Physical Whether voting in public locations was a concern in terms of privacy, which is related to the desirability of mobility and convenience.

Tracking/Anonymity Refers to concerns as to whether a voter's choices could be tracked via an electronic voting system.

The results illustrate a mixture of reactions to the scenario, from positive, to mixed and negative, with some groups not raising some of the issues at all. As discussed in the design of the study, the conversation between participants was not heavily constrained by the

discussion moderator. As such, the recurrence of themes across groups is in itself, interesting, since this suggests the system raises similar issues from all participants. The videotaped scenario elicited positive responses primarily for the usability aspects of the voting scheme, notably the mobility and convenience, although all focus groups noted concern about whether some groups would be excluded from voting by the system. This perhaps reflects the fact that the scenario did not suggest that multiple voting channels were envisaged, of which mobile phone voting was just one. Participants also raised concerns about the 'behind the scenes' processing of personal information and the security of the infrastructure. The occurrence of these topics is interesting, since the scenario did not discuss directly how voter information was handled to ensure privacy and security, but instead focused on usability and verifiability aspects. The concerns raised by the participants suggest that the implementation of voting schemes will need to be accompanied by explanation as to the reasons voters should accept voting systems as secure.

In addition to the responses categorised as positive and negative, several other topics were raised with respect to the voting system which can be considered to be assertions as to the desirable properties for a voting system, rather than a specific comment on the system proposed

Transparency The inner workings of the voting system should be demonstrable, it shouldn't be possible to mask inner workings. This was a desire raised by the high-education/technical focus group.

(De-)Centralisation The control of the voting system should be de-centralised to prevent abuse. The raising of this issue suggests an intuitive public understanding of dependability issues and the importance of distributing trust.

Control and choice An issue raised by several focus groups was the importance of users *retaining control of the right to choose who to vote for.* The discussion of this issue amongst focus groups is interesting from the perspective of pollster/pollsterless voting schemes. As discussed in Chapter 4, pollsterless, verifiable voting schemes permit a voter to determine (if the voter understands the verification mechanism)

directly that their choice has been reflected by a voting system. Conversely, cryptographic voting schemes require the voter to give their choice to a pollster which votes on their behalf, and thus the voter does not directly retain control of their choice. The discussion of this issue in the context of a pollsterless voting scheme, therefore suggests potential for future research on the topic of vote verifiability and voter trust.

6.4.5 Summary

The user acceptance study presented in the preceding section was undertaken to explore responses to the mCESG scheme prototype implementation and also investigate voter attitudes to the use of a vote verification mechanism for pollsterless voting schemes. provided results which suggested both positive and negative responses to the videotaped scenario viewed by participants. Participants expressed serious concerns about the security of electronic storage of personal information, including political choices. Conversely, the results of this exploratory study suggest the participants appreciate the potential for a convenient and mobile voting systems. Most interestingly, the study provides evidence that the ability to verify that a vote has been counted is both understood and appreciated.

6.5 Threat Analysis

This section discusses some potential threats to the mCESG prototype system, resulting from both the design of the scheme itself and also the implementation choices discussed in Section 6.2.

6.5.1 Domain Collusion Analysis

Table 6.2 summarises the potential for attacks should two domains choose to collude with one another. The table also includes *blind vote stuffing*, a possible attack should the Vendor

domain alone choose to behave maliciously. The types of attack possible under collusion for an attacker in control of two domains are described below, together with the steps in the vote casting process which is attacked, as discussed in Section 2.3.1 and illustrated in Figure 2.3.

False Voter Registration The attacker is able to use the initiation procedure to generate credentials for non-franchised voter identities. The attack occurs on the *Initiation* phase of the accuracy model described in Section 2.3.1. The attack is made more difficult to perform in the prototype implementation since a list of participating voters is published for review. The list permits checks to be made on the eligibility of voters to participate in the election.

Blind Vote Stuffing The attacker is able to cast extra votes but is not able to tell who the extra votes were cast for. This is an attack on *Vote Casting*. The attack is unreliable since:

- A large number of stuffed votes will need to be cast, raising the possibility of detection.
- The attack provides all candidates with an equal opportunity of winning, assuming stuffed votes are cast uniformly for all candidates.
- The lack of anonymity in the scheme enables voters to challenge when votes have been cast on their behalf.

Intelligent Vote Stuffing The attacker is able to cast extra votes and is able to determine the candidate being voted for. This is an attack on *Vote Casting*. The attacker uses credentials of non-participating voters to add extra votes to the final tally. The attack is more powerful than the Blind Vote Stuffing, since the attacker may target votes on their preferred candidate. However, unless the attack is combined with Early Tally Leak, the attacker does not know how many extra votes to cast.

Early Tally Leak The attacker is able to obtain an on-going tally of results. This is a violation of secrecy in the UK public election context, rather than accuracy.

	Registration Officer	Returning Officer	Vendor	Electoral Commission
Registration Officer	Register extra voters	None	VS, Intelligent BBS	VS, Intelligent BBS
Returning Officer		None	Intelligent BBS Leak early tally	None
Vendor			Blind BBS	None
Electoral Commission				None

Table 6.2: The table illustrates potential attacks that may occur under circumstances where one domain or two domains of the Election Authority choose to collude to perform an attack. The table denotes blind ballot box stuffing (Blind BBS) where an attacker is able to cast extra votes, but not know who those votes are cast for; violate secrecy (VS) where an attacker is able to determine the voter ↔ rid ↔ candidate association; and intelligent ballot box stufffing (Intelligent BBS) in which an attacker is able to cast votes whilst knowing the value of those votes.

Voter Privacy Violation Permits an attacker to determine the choice of candidate a voter made.

The CESG election authority was deliberately distributed into autonomous domains in order to prevent the attacks discussed above from occurring. With the exception of Blind Vote Stuffing and False Voter Registration, the attacks described require the collusion of two domains in order to operate and the limitations of the no-collusion attacks are described above. The distributed domain approach yields better properties than the monolithic Election Authority proposed for the CESG scheme, since collusion is required for the more serious attacks.

It may be noted that collusion between the Vendor and any other domain in the election authority is a particular source of vulnerabilities. Section 7.2 in the next chapter examines potential adaptations to the Vendor domain in order to mitigate this potential threat.

6.5.2 Denial of Service

The mCESG prototype implementation is vulnerable to both internal and external Denial of Service (DoS) attacks. A DoS attack prevents some service operating, typically through the prevention of access to some necessary resource. The target and consequences of a DoS attack varies in the mCESG prototype implementation. This section describes the potential attacks.

Internal DoS attacks refer to domains of the election authority which do not function as intended. Internal DoS may occur during:

Initiation During initiation, all the domains collude in order to generate and deliver voting credentials. The current implementation is dependent on all the domains operating in order for initiation to be successful.

Vote casting The Vendor domain may choose to ignore $vid : pcin$ values received via the

gateway, although unless collusion occurs with the Returning Officer domain, the attacker is not able to determine whether it is refusing useful votes or not.

Tallying The Vendor domain or the Returning Officer domain may refuse to collaborate to produce the final tally of results.

Alternatively, DoS attacks may originate out with the election authority, either through interception of voting credentials, if the secure, authenticated assumptions of the delivery channel are violated; or during Vote Casting, through the prevention of vote transmission via advertised channels. An attacker may either flood voting channels with a large number of incorrect vote values, or alternatively damage the infrastructure on which voting channels may depend. Section 7.2 discusses the potential for adapting the basic mCESG scheme to improve resistance to DoS attacks.

6.5.3 Voting Channels

The implicit design assumption of the vote casting channels is that a voter's identity cannot be extrapolated from the channel on which they cast a vote. However, the reliability of the assumption depends on either:

- the gateway implementations functioning honestly and not colluding with the vendor domain by providing traffic information associated with a vote which may identify a voter such as email address, or mobile phone number. This risk is mitigated by the use of simple devices (enabled by the pollsterless scheme), since voters are not required to use devices associated with themselves in order to vote.
- the proportion of voters using channels with which they are not normally associated. Voters who choose to vote via SMS, may use another mobile phone; votes cast via email may be sent from temporary email accounts set up by the voter for that purpose only or use an anonymous remailer to send the email; votes cast using touch tone telephony is performed on a public kiosk telephone, rather than the voter's home

or office phone. This ability to use virtually any networked device to vote is associated with the pollsterless property of the mCESG scheme, rather than the underlying implementation.

Whilst educational efforts might be used to encourage voters to use a range of potential devices to cast a vote, a direct alternative may be to modify the operation of the Gateway Handler such that it operates outwith the Vendor domain and as an anonymous channel.

6.5.4 Credential Delivery

For the mCESG scheme, the secure, authenticated channel between the election authority delivery domains and the voter is necessary to ensure that the voter's vote remains private and that an external attacker is unable to cast a vote on the voter's behalf. If the properties of the delivery channel are violated, an attacker may choose to either allow the voter to vote, in order to surreptiously learn their choice, or alternatively cast a vote on the voter's behalf.

Although the division of credential delivery into two tasks is primarily intended to prevent vote stuffing and privacy violations by the election authority, an additional benefit is that an external attacker is required to violate the properties of two delivery channels in order to obtain access to the voter's credentials.

The use of tamper-evident stationary for credential delivery provides a reasonable implementation of a non-electronic secure, authenticated delivery channel, since the voter may detect that the privacy of their credentials has been violated and request fresh credentials or else, resort to a polling station voting system. The use of less secure delivery channels may be appropriate where the inconvenience or expense of employing secure payroll stationary is unjustified. We note the common use of email to deliver usernames and passwords to users for non-security critical accounts, for example.

6.5.5 Bulletin Board Implementation

The bulletin board implemented for the prototype mCESG system, is rather primitive, since it lacks mechanisms to prevent the Vendor from retracting rid values once published. Note that this is a vulnerability of the implementation, rather than the scheme, since the scheme assumes the presence of a secure bulletin board as a universal broadcast channel in common with a range of existing cryptographic voting schemes.

6.6 Summary

In order to evaluate the mCESG scheme it was necessary to construct a demonstrable prototype implementation, the features of which are discussed in Section 6.2. The evaluation of the mCESG scheme provides a formal consideration of the schemes suitability for use in the UK public election context; a threat analysis of collusions between domains within the election authority and a user acceptance study incorporating both live demonstrations and a focus group study using videotaped scenarios. The various evaluations raise further issues for study which are discussed in the following chapter.

Chapter 7

Future Research Directions

Overview

The preceding chapters formalised, adapted, implemented and evaluated the mCESG scheme as a prototype voting system. This chapter examines some future research possibilities that arise from the evaluation of the mCESG prototype system.

7.1 Introduction

As the framework and context survey described in Chapter 2 illustrate, the field of voting systems is necessarily diverse, with on-going work investigating the requirements, voting schemes and implemented systems for a multitude of contexts. The contribution of this work has been an exposition of a new, pollsterless class of remote voting schemes, together with a prototype electronic voting system implementation, within the discussed framework. Pollsterless remote voting schemes are a relatively new and publicly untested approach to achieving the requirements of the public election context. Pollsterless schemes which provide voter verifiability have not been employed for elections in the United Kingdom.

The sections of this chapter are structured as follows. In Section 7.2 the limitations of the mCESG scheme and implementation identified in Chapter 6 are reviewed and possible improvements to the scheme are proposed. Section 7.3 discusses the prospect of conducting pilots for various contexts using the mCESG REV scheme. The nature of the proposed future work is necessarily speculative, however, the proposed topic areas do provide a feasible outline for a substantial research agenda.

7.2 Further Adaptations to the mCESG Scheme and Implementation

Chapter 6 identified several limitations of the mCESG scheme and prototype implementation. To remedy such limitations, either the mCESG scheme must be extended through the incorporation of an adaptation further to those described in Section 5.5, or else the implementation decisions made for the prototype system must be re-evaluated for suitability and other potential candidates investigated.

When proposing further adaptations to the mCESG scheme, consideration must be made of the consequences of the adaptation for the fundamental pollsterless properties of the scheme (verifiability and mobility), together with an examination of the potential conflict between multiple adaptations being incorporated into the scheme simultaneously. Whilst several individual adaptations were investigated in Section 5.5, the prospect of combining, say, the receipt free and ordinal adaptation was not investigated. Whilst the ease of adaptation of the mCESG scheme demonstrates its considerable flexibility and thus potential suitability for a diversity of contexts the potential conflict between multiple adaptations is uninvestigated and represents by itself a considerable research topic of interest

This section examines three potential adaptations to the mCESG scheme which remedy limitations identified in the system evaluation in Chapter 6. In Section 7.2.1, a proposal for implementation of the secure bulletin board without employing extensive cryptography is

proposed. In Section 7.2.2 a consideration is made of the prospect of re-implementing the Vendor domain in a manner which mitigates the potential for collusion between domains as discussed in Section 6.5.1. Finally, Section 7.2.3 examines a strategy for mitigating the potential for external denial of service attacks affecting high risk voting contexts.

7.2.1 Distributed Bulletin Board

A limitation of the mCESG implementation identified in Chapter 6 is the primitive implementation of the bulletin board. The formalisation mCESG scheme assumes the availability of the bulletin board as a universally accessible, secure broadcast channel, such that messages written to the bulletin board are accessible by all participants in an election. The use of such a artifact prevents the Vendor domain attempting to later deny messages it wrote to the board, the rid values and candidate identities. However the precise form of the bulletin board is left unspecified in the formalisation.

An implementation of the bulletin board for the prototype mCESG system employs a web-page server for the role. The prototype is an unsatisfactory implementation of the scheme, since the Vendor domain is able to edit the web page published as desired. The web page publishing mechanism serves only as a suitable demonstration medium for the bulletin board, whilst a more secure approach is required for any pilots of the mCESG scheme.

To improve the mCESG scheme it is proposed that an implementation of the bulletin board be specified as a component of the scheme. The bulletin board could be implemented without cryptographic techniques employed to ensure the accuracy of the board, since the bulletin board is only required to commit to rid values which the Vendor domain publishes. As such, it is proposed that several autonomous domains out with the election authority monitor the values published by the election authority. The domains could represent media organisations which currently provide a similar informal role in the UK public election context by relaying results of elections as they are announced. Alternatively, the Vendor domain could be required to establish secure channels to several domains nominated by

candidates or other interested parties in the election. Each domain could maintain a list of rid values it has observed. Further, selected domains could conduct further communication between each other to check for discrepancies between sets of rid values provided to different domains. Voters may choose to check the presence of their rid value on a set of the domains which they trust such as sympathetic parties or trusted media outlets.

7.2.2 Distributed Domain Implementation

The collusion analysis described in Section 6.5.1 noted the potential for vulnerabilities to emerge in the mCESG scheme should the Vendor domain in particular become corrupted and co-opt one other domain in the election authority to participate in an attack. Further, the Vendor domain is particularly capable of performing an internal denial of service attack, either during initiation, vote casting or the tallying phase of the mCESG scheme. Under such circumstances the mCESG election authority reverts to the properties of the flawed, monolithic architecture proposed for the CESG scheme.

The design of the election authority in the mCESG scheme is a deliberate attempt to model the infrastructure of elections in the UK, the context for which the scheme is designed. The scheme deliberately does not attempt to incorporate a security parameter in terms of the number of corrupt election authorities required to violate secrecy or the accuracy of tally, as is the approach of a number of cryptographic schemes [9, 71, 94]. Such an approach requires the availability of sufficient independent organisations to host the domains, whilst the mCESG scheme is designed to operate in parallel with the UK's existing public election voting system. Each domain in the mCESG scheme has a corresponding organisation able to host it and each domain is labelled to indicate the appropriate host.

However, the Vendor domain of the election authority is the anomaly to the motivation described above, since the UK infrastructure does not prevent the possibility of multiple Vendor domains being implemented within the election authority. Such an approach might have two potential advantages if only a subset of functioning Vendor domains are required

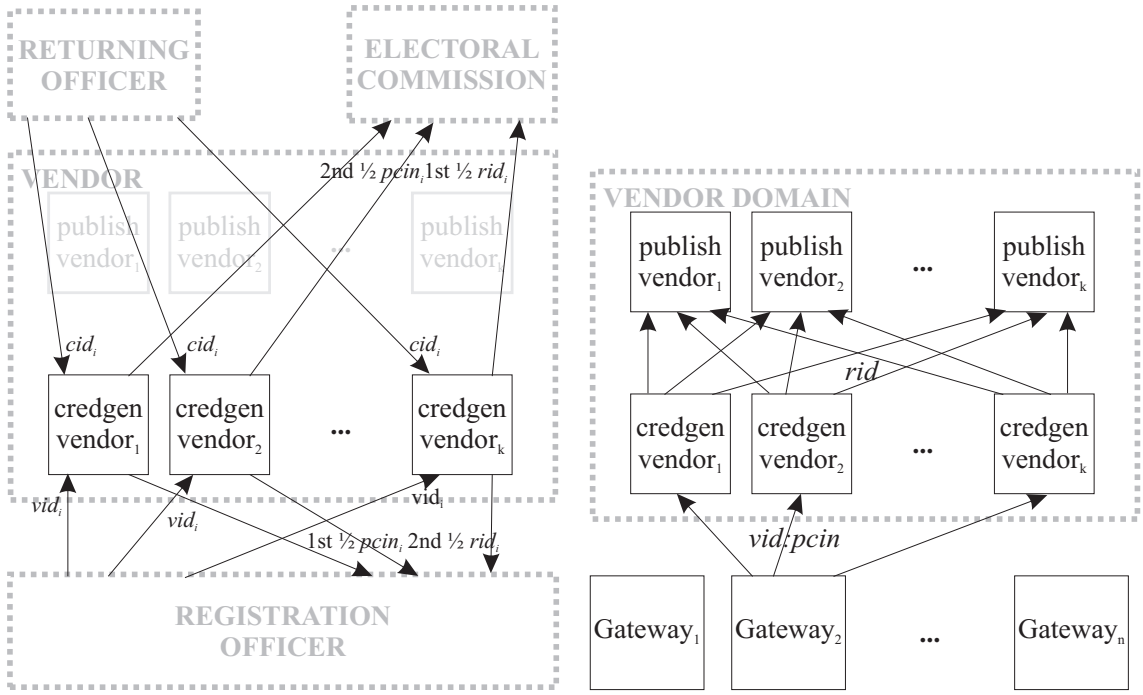
to operate, as:

- multiple Vendor domains provides a parameter for the difficulty of performing a successful internal DoS attack from the Vendor domain in terms of the proportion of Vendors that must be corrupted in order to prevent correct voting credentials reaching a voter. An election organiser is able to utilise the services of sufficient k Vendor domains to prevent the DoS attack from successfully operating.
- an attacker would need to corrupt some sub-set of the Vendor domains in order to conduct vote stuffing attacks.

The first advantage of employing multiple Vendor domains may be obtained through the use of multiple identical Vendors. The set of Vendor domains must agree on a common key set for the generation of credentials, for example using a key agreement protocol [90]. The initiating domains of the election authority, Registration and Returning Officer, pass initiation values to all k Vendor domains. Each Vendor computes the values required of them and returns these to the delivery domains, the Registration Officer and Electoral Commission. The problem of identifying correct output values if some domains differ is then equivalent to the Byzantine Generals problem [79].

To obtain the second advantage of employing multiple Vendors to prevent vote stuffing attacks, it is necessary to divide up the responsibility of Vendors between *credgen-Vendors* which compute credential values and *publishers-Vendors* which interact with the bulletin board to publish credentials. In this scenario, gateways forward voting credentials to all k credential generators. Each credential generator produces an rid value for the received vote and forwards the value to the publisher-Vendors. The publisher Vendors agree, again using Byzantine general techniques, when a credential has been received from sufficient credgen-Vendors to be published. Figure 7.1 illustrates the combination of two approaches described here for distributing the role of the Vendor domain.

Potentially, employing multiple domains might also be useful to prevent violations of vote secrecy, as distribution of Vendor domains reduce the potential for intelligent vote stuffing



(a) Credential Generation (b) Vote Collection

Figure 7.1: Distributed Vendor domain architecture. The diagrams illustrate credential generation and the collection of votes in the revised mCESG scheme. The single Vendor domain of the mCESG scheme is distributed into k credgen-vendors and k publisher-vendors domains. During credential generation, the initiating domains pass input values to all vendor domains, which in turn send outputs to the delivery domains. In the event of a discrepency, the delivery domains then adopt a policy to decide which received credentials to employ. During vote casting the gateways which collect votes, forward voting values to each of the k credgen-vendor domains, which in turn pass rid values to all of the k publisher-vendor domains. The publisher domains then employ Byzantine General strategies to decide when sufficient credgen-vendors have announced receipt of a particular vote before publishing that receipt.

attacks, from within the Vendor domain. However, such an adaptation would require the use of more complex cryptographic techniques such that no single Vendor domain obtains the complete set of voter credentials for any one voter. This might be achieved using secure multi-party computation techniques similar to that adopted in [85], for example, although an implication of this approach is that a voter may be required to assemble a voting credential from $n > 2$ rather than at present 2 components and as such may be impractical.

7.2.3 Distributed Election Scheme

The threat analysis conducted in Section 6.5.2 noted that the mCESG scheme is vulnerable to DoS attacks, both internal attacks originating from malfunctioning or malicious domains of the election authority, or from external attacks which disable available voting channels, through excessive network load, for example. The previous section discusses adaptations to the mCESG scheme which reduce the opportunity for internal DoS attack to originate from the Vendor domain. The threat analysis notes how the deployment of multiple voting channels reduces the potential for conducting external DoS attacks, since an attacker needs to disable multiple channels deployed across multiple platforms in order for the attack to prevent all attacks from successfully operating.

An alternative strategy for mitigating the consequences of DoS attacks is outlined in this section. So far, the mCESG scheme has envisaged a single election authority for the conduct of a given election. That is, the responsibility for registration of voters, nomination of candidates, processing of votes and generation of the final tally of votes is all conducted by a single set of domains, albeit domains distributed amongst autonomous organisations. This approach to deployment provides a single target for an attacker to focus on.

A common strategy to mitigate the consequence of external DoS attacks is to distribute replicas of a service's functionality such that even if a sub-set of services are attacked, the overall service remains largely unaffected. For public elections employing paper ballots

and polling stations, the replication occurs on a hierarchical geographic basis, where an attacker must close a large number of polling stations in order for the attack to have a serious consequence for the result of an election. In such circumstances, some contexts, for example in some areas of the United States, a voter may cast a vote at a polling station to which they have not been formally assigned. This replication strategy is modelled in several cryptographic schemes, either hierarchically, or through multiple replicated voting services, most notably [9, 71, 117].

A useful adaption for the mCESG scheme, then, would enable multiple election authorities to be deployed for an election, with a discrete partition of the electorate formally assigned to each election authority. Such a setup would require policies and mechanisms to govern:

- the release of partial tallies from election authorities. It may be either desirable or undesirable for a single election authority to reveal the partial tally on the total tally for which it is responsible. Publishing a partial tally may be undesirable because it provides evidence to an external observers of the preferences of a particular set of voters (potentially violating secrecy). Conversely, publishing partial tallies may be considered desirable in other contexts in order to provide re-assurance as to the accuracy of a complete tally.

- the transfer of $vid : pcin$ between domains, where a voter accidentally or intentionally uses a voting channel assigned to another election authority. Mechanisms for transferring or buffering votes of election authorities whose service is temporarily reduced would further improve the robustness of the mCESG scheme to withstand DoS attacks.

7.3 Pilot Elections

One of the most curious phenomenon of published voting schemes is the lack of live trials of the schemes in pilots. Although schemes have been trialed in some limited contexts,

including the CESG scheme employed for public election pilots in the UK [45]; pilots conducted in Europe via the True-Vote project [107, 109]; and the Sensus scheme (based on blind signatures) implemented and piloted for use in student organisation office bearer elections [28, 29, 30], the use of formally specified voting schemes for public elections is relatively uninvestigated, despite the plethora of schemes proposed. Conversely, voting systems which employ technology not based on explicit voting schemes with demonstrable properties enjoy widespread use for voting in a variety of contexts, sometimes controversially [64, 77, 131].

This section outlines a proposal for studying the mCESG scheme during live pilots to provide both guidance for future adaptations and also to provide experience of conducting research into pilots employing cryptographic schemes where permissible.

7.3.1 Research Questions

The conduct of new voting scheme pilots within a research context requires sound research questions. The following questions for investigation are proposed here, either with respect to the mCESG scheme, but with wider applicability to cryptographic voting schemes and their implementations.

Usability

1. What considerations for voter access and input error rate should be made when implementing remote voting schemes?
2. Would a two step voting scheme prove more acceptable to voters, that is authentication followed by vote casting rather than a one step process?
3. What character sets and lengths of text strings are acceptable and less error prone than others?

4. Do specific vote casting technologies, such as SMS/Internet, have an impact on the usability of a voting scheme?

Acceptability

1. Is the provision of a vote checking mechanism sufficient to ensure that voters trust the system to count their votes and that their own personal vote remains secret?
2. What proportion of a target electorate will wish to validate their vote by means of an electronic bulletin board? What are the influences on a voter's willingness to validate their vote?

The first usability research question provides a more extensive assessment of the mCESG scheme than has been conducted here, with implications for future proposals for voting schemes. The mCESG scheme itself specifies a simple user interface which accepts strings of input characters from the user, without any further processing. However, the scheme does not preclude the use of more complex interfaces to support input for voters with particular disabilities where necessary, or to reduce potential for incorrect vote entry. Factors addressing data entry error-rates have been investigated [136, 137], however voting, particularly in public elections provides a new context which may have an impact on usability. The second question is designed to investigate the usefulness of the two-step voting adaptation proposed in Section 5.5.3, which was intended to accommodate the "mistake" made by voters during live demonstrations described in Section 6.4.2. The third usability question considers the possibility of increasing the character set for voting credential values. Whilst the use of an increased character set may partially limit the available voting channels (touch tone telephony channels may be unusable for alpha-numeric character sets, for example), a larger range provides greater security of voting credentials, by increasing the difficulty of guessing a credential value, without the need to increase the length of the credential values.

The proposed investigation of acceptability extends that conducted for the mCESG scheme described in Section 6.4. Whilst the scenario directed focus group methodology provides

some results as to the usefulness of providing voters with re-assurance as to the accuracy of a tally of votes, the conduct of a pilot would provide evidence for the basis of a live election. Further, a pilot would enable the examination not only of whether voters understand the checking mechanism, but also the proportion of voters likely to participate in checking the vote. This would provide an estimate of an election authoritie's likelihood of detection in the event of malfunction or deliberate corruption.

7.3.2 Target Context

A difficulty of conducting research into the suitability of voting schemes whilst simultaneously operating a pilot is that the researcher has an ethical responsibility to ensure that the results of the pilot election are obtainable, regardless of whether the implementation of a particular scheme was deemed to have failed in the context of the research. Voters cannot be used as "guinea pigs" for poorly designed or implemented voting schemes. The conflict between conducting a "pilot" using a live election and the demand for "nothing to go wrong" by election administrators is particularly acute in the conduct of public elections, particularly in circumstances where the control of government may change as a result of mistakes attributable to a voting system.

In addition to the high "conversion" risks, mistakes or perceived failures of new voting systems may encourage election administrators to refuse to host pilots in future, making examination of the impact of new voting systems over successive elections difficult to measure. In the UK, for example, pilots equivalent to those conducted using new voting systems in 2002 and 2003 were cancelled for 2006 because of a perceived lack of impact on turnout, despite only limited testing of the pilots and a lack of experience of the new systems by the electorate [42]. Similarly in the US, critics of DRE machine based systems argue that such devices increase residual rate votes, that is the proportion of votes cast for a particular race compared to the total votes cast at one time, compared with optical scan or paper ballot based system, citing evidence in presidential elections between 1988 and 2000 [2]. Conversely, opponents cite evidence that DRE machines had lower residual rates than

other systems in the 2000 election, suggesting that the US electorate were becoming more experienced with DRE machines [11]. [1]

To avoid the difficulties described above, it is proposed that a voting context is selected for conducting pilots that has similar, if not identical, requirements to the UK public election context, for which it will be possible to conduct pilots using the same electorate more frequently. An ideal candidate for such a pilot study would be the election of student representatives, since such a context provides:

- A similar requirements context to UK public elections in terms of secrecy and accuracy requirements.
- Reduced costs of deployment, both in terms of time and finance.
- Frequent election cycles for the same electorate - often once or twice a year, permitting an identification of trends in voting system usage.
- A lower "conversion" risk threshold.

It is not argued here that the results of elections conducted to choose student representatives are not important, however it is argued that the consequences of a failure of the voting system are less severe than for an election conducted to choose a public representative such as a Member of Parliament. Further the contrast between the attributes of a student population and the electorate in the public election context must be considered when evaluating results from a study.

7.4 Summary of Future Work

This chapter has discussed future possible extensions to the research work described in this thesis. The flexibility of the mCESG scheme gives rise to the potential for a number of

[1] The author of the study noted that it was partially funded by a voting systems vendor that produces both DRE and optical scan based systems.

adaptations to compensate for the limitations identified in Chapter 6. This chapter also provides an outline motivation for the conduct of pilots using the implementations of proposed voting schemes and justifies the use of student organisation elections to conduct these pilots, at least when employing early implementations of new voting schemes. The final chapter of this thesis reviews the work described in the previous chapters and discusses the potential for new voting schemes in the future.

Chapter 8

Conclusions

Overview

The preceding chapters have described a framework for understanding the relationship between the various diverse research efforts in the field of electronic voting and demonstrated the framework through the description of a novel remote electronic voting scheme, mCESG. This chapter reviews the work so far described and re-examines the thesis hypothesis explained in Chapter 1. The chapter concludes by re-iterating the significance of context when designing or selecting voting systems for deployment.

8.1 Review of Chapters

This section reviews the individual contributions of the preceding chapters of this thesis:

Chapter 1: Introduction The topic of interaction between voting and voting technology was introduced, particularly with respect to the role of computer science in voting technology. The motivation and contributions of this thesis were explained together with the core

hypothesis describing the significance of context when evaluating voting systems and the suitability of pollsterless schemes for implementation in the UK context.

Chapter 2: Voting and Technology The interaction between voting and technology was elaborated, providing an illustrative history of technological use in public elections. The chapter introduced a layered framework for integrating the various research efforts into voting systems, distinguishing between contexts, requirements, schemes and systems. The chapter provides a survey of the various research efforts, again in terms of contexts, requirements, schemes and systems to illustrate the suitability of the voting framework for integrating research efforts.

Chapter 3: Requirements for UK Public Elections The UK public election context specific requirements for voting systems was described in terms of motivational requirements; the electoral systems to be accommodated and the secrecy and accuracy requirements specified by electoral law. The chapter notes that a new voting system is required to both improve the convenience of voting and fulfill the existing requirements of voting systems in order to motivate change.

Chapter 4: Pollsterless Remote Electronic Voting Schemes The notion of pollsterless remote voting schemes was introduced. The origins of the term and the advantageous properties of pollsterless schemes with respect to the requirements of UK public elections were described. The chapter described two pollsterless schemes (Malkhi et al and CESG) noting the advantages and flaws of both approaches.

Chapter 5: The mCESG Pollsterless Remote Electronic Voting Scheme The notion of pollsterless voting schemes was developed by demonstrating that the flaws of the CESG scheme (monolithicity, lack of voter verifiability) could be corrected without loss of the advantageous properties of the scheme (mobility, simplicity). The chapter demonstrated the flexibility of the mCESG scheme by detailing several adaptations to fulfill alternative re-

quirements of the UK context. The range of adaptations available for the scheme illustrated that mCESG represents a class of pollsterless remote voting schemes.

Chapter 6: Evaluation of mCESG Scheme This chapter reviewed the novel pollsterless remote voting scheme mCESG through several methodologies: an analysis of the mCESG scheme with respect to the requirements for UK public elections described in Chapter 3; threat analysis, including a collusion analysis; and a user acceptance study employing scenario directed focus groups.

Chapter 7: Future Research Directions The potential for further research employing the mCESG scheme was demonstrated, both through outlines of further adaptations to correct the limitations discussed in Chapter 7 and also the motivation and target context for conducting pilot elections with the scheme.

8.2 Assessment of Contribution

The contribution of this thesis to the field of voting systems in general and voting schemes in particular are as follows:

- A novel class of pollsterless remote voting schemes, mCESG which permits votes to be cast via any simple networked device. The specification of the scheme demonstrates that it is voter verifiable and mobile. Additionally, the scheme specification includes a number of adaptations which demonstrates its flexibility with respect to different voting contexts requirements.
- A layered framework into which the various diverse research efforts into voting systems may be understood. In particular, the approach separates voting schemes from the systems which implement them, permitting requirements to be established against

voting contexts, but evaluated against voting schemes, rather than the far more complex voting systems which implement them. The task of implementation then becomes one of ensuring correctness with respect to an abstract voting scheme.

- A discussion of the requirements for the UK public election context, with respect to the requirements expressed by CESG and the UK's electoral law as a model against which a suitable voting scheme can be evaluated.

- A comprehensive evaluation of the mCESG scheme, both with respect to the requirements identified for the UK public election context, but also via a user acceptance study employing scenario-directed focus groups.

8.3 Review of Hypothesis

The original hypothesis of this work stated that voting schemes and systems must be understood within the wider voting context into which they are deployed; and that a novel class of pollsterless voting schemes are particularly suitable for the UK voting context. To support this argument, a novel class of pollsterless voting schemes were established with respect to requirements identified for the UK public election context. A prototype remote voting system was developed from the scheme designs and evaluated with respect to identified requirements. The novel scheme proposed for the UK was demonstrated to be adaptable and flexible with respect to the variation in requirements that may occur even within the UK public election context. In addition, a user acceptance study was undertaken, which illustrated both the potential benefit of the pollsterless voting system for enchancing convenience and mobility of voting as well as the concerns of voters.

The work described in this work then supports the hypothesis that voting systems must be considered in context, and that the UK voting context is suitable for a remote, pollsterless voting system.

8.4 Concluding Remark: The Importance of Context

The extract at the start of this thesis is taken from a chapter in which Mill argues against the introduction of ballot papers and boxes because of the perception that the electorate, who at the time formed only a small, wealthy subset of the population, had a responsibility to the wider public, beyond individual interest. By requiring a voter to announce their choice they were also required to explain and justify it. His abhorence of the notion of postal voting is not that a voter should not be influenced, but rather that they should be influenced in their choice by the needs of the wider public. Whilst historically Mill was on the losing side of the debate, he was arguing for a voting system which fitted the requirements of the context in which Members of Parliament at the time were elected.

As computer scientists, our responsibility is to ensure that the voting schemes and systems we design, implement and analyse must be viewed in the context in which they are employed.

Bibliography

This bibliography contains some citations to Hansard (UK Parliamentary debates). An example format for such citations is HL, Vol 678, cols 51–53, February 13, 2006. The citation begins with HL (referring to the House of Lords, HC for House of Commons), followed by the volume and column of Hansard for the extract and finally the date on which the debate took place. The addition of 'W' or 'WS' indicates the citation is written statement.

[1] Rushmoor to trial early voting. Rushmoor Borough Council, February 2006.

[2] R. Michael Alvarez, Stephen Ansolabehere, Erik Antonsson, and Jehoshua Bruck. Voting what is, what could be:. Research findings, Caltech-MIT Voting Technology Project, July 2001.

[3] R. Michael Alvarez and Thad E. Hall. *Point Click and Vote: The Future of Internet Voting*. The Brookings Institution Press, March 2004.

[4] Chris Armen and Ralph Morelli. Teaching about the risks of electronic voting technology. In *ITiCSE '05: Proceedings of the 10th annual SIGCSE conference on Innovation and technology in computer science education*, pages 227–231, Caparica, Portugal, 2005. ACM Press.

[5] Gearing up for India's electronic election. BBC News, February 2004.

[6] Benjamin B. Bederson, Bongshin Lee, Robert M. Sherman, Paul S. Herrnson, and Richard G. Niemi. Electronic voting system usability issues. In Gilbert Cockton

and Panu Korhonen, editors, *Proceedings of the 2003 Conference on Human Factors in Computing Systems, CHI 2003*, volume 5 of *chi letters*, pages 145–152, Ft. Lauderdale, Florida, USA, April 2003. ACM.

[7] Josh Benaloh. *Verifiable Secret Ballot Elections*. PhD thesis, Yale University, December 1996.

[8] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 544–553. ACM Press, 1994.

[9] Josh Benaloh and Moti Yung. Distributing the power of a government to enhance the privacy of voters. In *Proceedings of the Fifth Annual ACM Symposium on Principles of Distributed Computing*, pages 52–62, Calgary, Alberta, Canada, August 1986. ACM.

[10] Sarah Birch and Bob Watt. Remote electronic voting: Free, fair and secret? *Political Quarterly*, 75(1):60–60, 2004.

[11] Henry E. Brady, Justin Buchler, Matt Jarvis, and John McNulty. Counting all the votes: The performance of voting technology in the United States. Department of Political Science, Survey Research Center, and Institute of Governmental Studies, University of California, Berkeley, September 2001.

[12] Henry E. Brady, Michael C. Herron, Walter R. Mebrane Jr., Jaskeet Singh Sekhon, Kenneth W. Shotts, and Jonathan Wand. "law and data": The butterfly ballot episode. *Political Science and Politics*, 34(1):59–69, March 2001.

[13] Robert Sherrick Brumbaugh. *Ancient Greek Gadgets and Machines*. Greenwood Press, Westport, Connecticut, US, 1975.

[14] Jeremy Bryans and Peter Ryan. A dependability analysis of the Chaum digital voting scheme. Technical Report CS-TR-809, School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK, July 2003.

[15] Jeremy W Bryans and Peter Y A Ryan. A simplified version of the Chaum voting scheme. Technical Report CS-TR-843, School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK, May 2004.

[16] Prashanth P. Bungale and Swaroop Sridhar. Electronic voting - a survey. John Hopkins University, 2003.

[17] The European Convention on Human Rights. Council of Europe, 1950.

[18] e-voting security study. Communications and Electronic Security Group (CESG), July 2002.

[19] e-voting technical and security requirements. Communications and Electronic Security Group (CESG), November 2002.

[20] Doug Chapin. Whats changed, what hasn't, and why: Election reform since november 2001. Research report, electionline.org, October 2002.

[21] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, February 1981.

[22] David Chaum. Secret-ballot receipts: True voter verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, January 2004.

[23] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, January 2004.

[24] David Chaum, Peter Y. A. Ryan, and Steve A. Schneider. A practical, voter-verifiable election scheme. Technical Report CS-TR-880, School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK., December 2004.

[25] David Chaum, Peter Y.A. Ryan, and Steve Schneider. A practical, voter-verifiable election scheme. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, *Computer Security - ESORICS 2005, 10th European Symposium*

on Research in Computer Security, volume 3679 of *Lecture Notes in Computer Science*, pages 118–139, Milan, Italy, September 2005. Springer Verlag.

[26] Michael R. Clarkson and Andrew C. Myers. Coercion-resistant remote voting using decryption mixes. In *Frontiers in Electronic Elections (FEE 2005)*, Milan, Italy, September 2005.

[27] e-democracy report of research findings. COI Communications/Office of the e-Envoy, December 2002.

[28] Lorrie Cranor and Ron Cytron. Design and implementation of a practical security-conscious electronic polling system, January 1996.

[29] Lorrie Cranor and Ron Cytron. Towards an information-neutral voting scheme that does not leave too much to chance. In *Midwest Political Science Association 54th Annual Meeting*, April 1996.

[30] Lorrie Cranor and Ron Cytron. Sensus: A security-conscious electronic polling system for the internet. In *Proceedings of the Hawai'i International Conference on System Sciences*, Wailea, Hawaii, January 1997. IEEE Computer Society Press.

[31] Electronic proxy voting. CRESTCo Limited Consultation Document, July 2001.

[32] Alan Dearle, Graham N.C. Kirby, Andrew McCarthy, and Juan Carlos Dias y Carballo. An information flow architecture for global smart spaces. Technical Report D15, Global Smart Spaces Project IST-2000-26070, 2003.

[33] AccuVote-TS. Diebold Election Systems, Corporate Advertising Available at `http://www.diebold.com/dieboldes/accuvote_ts.htm`.

[34] David Dill. Resolution on electronic voting, 2003.

[35] Brandon William DuRette. Multiple administrators for electronic voting. Bachelor's thesis, Massachusetts Institute of Technology, May 1999.

[36] Frank Lewis Dyer and Thomas Commerford Martin. *Edison, His Life and Inventions*. University Press of the Pacific, December 2001.

[37] Electoral Administration Bill, 2005. No. 50.

[38] Election Assistance Commission, 1225 New York Ave., NW, Suite 1100, Washington, D.C. 20005. *Voluntary Voting System Guidelines*, draft edition, July 2005.

[39] Recounts: From punch cards to paper trails. Election Reform Briefing 12th, electionline.org, 1101 30th Street, NW, Suite 210, Washington, DC 20007, October 2005.

[40] Election 2001: the official results. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, July 2001.

[41] Modernising elections, a strategic evaluation of the 2002 electoral pilot schemes. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, August 2002.

[42] The shape of elections to come: A strategic evaluation of the 2003 electoral pilot schemes. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, July 2003.

[43] Delivering democracy? the future of postal voting. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, August 2004.

[44] European Parliamentary And Local Elections (Pilots) Act, 2004. Ch. 2.

[45] Piloting alternative voting methods in the 2003 local elections in England. Electoral Reform Society, 2003.

[46] Nicholas Ben Fairweather. CESG report on evoting security - response of the centre for computing and social responsibility. De Montfort University, 2002.

[47] Robin Farquharson. *Theory of Voting*. Yale University Press, New Haven, 1969.

[48] Federal Election Commission, 999 E Street, NW, Washington, DC 20463. *Voting Systems Standards*, January 1990.

[49] Federal Election Commission, 999 E Street, NW, Washington, DC 20463. *Voting System Standards*, April 2002.

[50] Response to e-democracy consulation. Foundation for Information Policy Research(FIPR), 2002.

[51] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - ASIACRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques*, volume 718 of *Lecture Notes in Computer Science*, pages 244–251, Gold Coast, Queensland, Australia, December 1992. Springer Verlag.

[52] John Fund. *Stealing Elections: How Voter Fraud Threatens Our Democracy*. Encounter Books, USA, September 2004.

[53] Dimitris A. Gritzalis, editor. *Secure Electronic Voting*. Kluwer Academic Publishers, 101 Philip Drive, Assinippi Park, Norwell, Massachusetts, 020601 USA., 2003.

[54] Andrew Gumbel. *Steal this vote*. Nation Books, 245 West 17th Street, 11th Floor, New York, NY 10011, 2005.

[55] HC Deb, 12 Sept 2005, vol 436, c2251W.

[56] Stuart Harrington. Electoral modernisation pilots. Statement of Requirement 2002/S 191-150905, Office of the Deputy Prime Minister, Eland House, Bressenden Place, London, SW1E 5DU, November 2002.

[57] Bev Harris. *Black Box Voting Ballot Tampering in the 21st Century*. Plan Nine Publishing, 1237 Elon Place, High Point, NC 27263, 2003.

[58] Help America Vote Act, 2002. (P.L. 107-252).

[59] Guilherme Campos Hazan. *SuperWaba Software Development Kit*. SuperWaba, April 2004.

[60] Susan Henry. Can remote internet voting increase turnout? *Aslib Proceedings*, 55(4):193–202, 2003.

[61] Alejandro Hevia and Marcos A. Kiwi. Electronic jury voting protocols. In *Latin American Theoretical INformatics*, pages 415–429, 2002.

[62] HL, Vol 678, cols 51–53, February 13, 2006.

[63] Englebert Hubbers, Bart Jacobs, and Wolter Pieters. RIES: Internet voting in action. In Randal Bilof, editor, *Proceedings of the 29th Annual International Computer Software and Applications Conference, COMPSAC'05*, pages 417–424, Edinburgh, Scotland, July 2005. IEEE Computer Society.

[64] Harri Hursti. *Critical Issues with Diebold Optical Scan Design*. Black Box Voting Inc, 330 SW 43rd St Suite K PMB-547 Renton WA, July 2005.

[65] Spyros Ikonomopoulos, Costas Lambrinoudakis, Dimitris Gritzalis, Spyros Kokolakis, and Kostas Vassiliou. Functional requirements for a secure electronic voting system. In Adeeb Ghonaimy, Mahmoud T. El-Hadidi, and Heba K. Aslan, editors, *Security in the Information Society: Visions and Perspectives, IFIP TC11 17th International Conference on Information Security (SEC2002)*, volume 214 of *IFIP Conference Proceedings*, pages 507–520, Cairo,Egypt, May 2002. IFIP, Kluwer.

[66] Description of EVM (slides). Indian Electoral Commission Available at `http://www.eci.gov.in/EVM/EVM_3.htm`.

[67] Natsuki Ishida, Shin'ichiro Matsuo, and Wakaha Ogata. Divisible voting scheme. Cryptology ePrint Archive Report 2003/074, IACR, 2003.

[68] Peter Jackson, Colin Rosenstiel, and Seamus O'Connell. Ballot secrecy. Electoral Reform Society, 1997.

[69] Dr. David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A security analysis of the secure electronic registration and voting experiment (SERVE). Security analysis, Security Peer Review Group), January 2004.

[70] Dylan Jeffrey and Xavia Morbey. Co-ordinated on-line register of electors (CORE) standardising electoral registration. Consultation paper, Office of the Deputy Prime Minister, Eland House, Bressenden Place, London, SW1E 5DU., May 2004.

[71] Rui Joaquim, André Zuúquet, and Paulo Ferreira. Revs – a robust electronic voting system. *IADIS International Journal WWW/Internet*, 1(2):47–63, December 2003.

[72] Alastair Jones. The classification of electoral systems: Towards a multi-dimensional approach. In Jeffrey Stanyer and Gerry Stoker, editors, *Political Studies Association Annual Conference Papers*, pages 510–525, University of Ulster, Jordanstown, UK, 1997. Contemporary Political Studies.

[73] Douglas W. Jones. A brief illustrated history of voting, 2001. online.

[74] Ari Juels and Markus Jakobsson. Coercion resistant electronic elections. `eprint.iacr.org/2002/165.pdf`, 2002.

[75] Chris Karlof, Naveen Sastry, and David Wagner. Cryptographic voting protocols a system perspective. In *Proceedings of the 14th USENIX Security Symposium*, pages 33–50, Baltimore, MD, 2005. USENIX.

[76] Jason Kitcat. GNU.FREE a free software odyssey. j-dom.org, March 2003.

[77] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. Analysis of an electronic voting system. Technical report, John Hopkins University, July 2003.

[78] Steve Kremer and Mark Ryan. Analysis of an electronic voting protocol in the applied pi calculus. In Shmuel Sagiv, editor, *Programming Languages and Systems, 14th European Symposium on Programming,ESOP 2005, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005, Proceedings*, number 3444 in Lecture Notes in Computer Science, pages 186–200, Edinburgh, U.K., April 2005. Springer.

[79] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.

[80] Recommendations for improving reliability of direct recording electronic voting systems. Brennan Centre for Justice and Leadership Conference on Civil Rights, July 2004.

[81] Jong-Hyeon Lee. The big brother ballot. *Operating Systems Review*, 33(3):19–25, 1999.

[82] Linda Little, Pam Briggs, and Lynne Coventry. Activity theory and videotaped activity scenarios: Verification of factors that influence technology use in public areas. Prepared for HCI 2004, 2004.

[83] Linda Little, Stephen Marsh, and Pam Briggs. Trust and privacy permissions for an ambient world. To Appear Trust in E-Services: Technologies, Practices and Challenges, January 2006.

[84] Guidance for Acting Returning Officers in England and Wales. The Lord Chancellor's Department, 2001.

[85] Dahlia Malkhi, Ofer Margo, and Elan Pavlov. E-voting without 'cryptography'. In Matt Blaze, editor, *Financial Cryptography, 6th International Conference, FC 2002, Revised Papers*, volume 2357 of *Lecture Notes in Computer Science*, pages 1–15, Southampton, Bermuda, 2003. International Financial Cryptography Association, Springer.

[86] Donna Maurer. What is usability? Step Two Designs Pty Ltd, November 2004.

[87] Richard Mawrey QC. Judgement in the matter of a local government election for the Bordesley Green ward of the Birmingham City Council held on the 10th June 2004 and in the matter of a local government election for the Aston ward of the Birmingham City Council held on the 10th June 2004. HM Courts Service, April 2005.

[88] Margaret McGaley. Report on DIMACS workshop on electronic voting theory and practice, May 26 - 27, 2004, December 2004.

[89] McMahon vs Attorney General, 1972. IR69 at p106.

[90] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*, volume 6 of *Discrete Mathematics and Its Applications*. CRC Press, 23-25 Blades Court, Deodar Road, London, SW15 2NU, UK, fifth edition, August 2001.

[91] Rebecca Mercuri. *Electronic Vote Tabulation: Checks and Balances*. PhD thesis, University of Pennsylvannia, 2001.

[92] Rebecca Mercuri. A better ballot box? *IEEE Spectrum*, 39(10):46–50, October 2002.

[93] Rebecca Mercuri. Response to formal request for comment by the CESG (UK) on internet voting, October 2002.

[94] Michael Merritt. Elections in the presence of faults. In *Proceedings of the third annual ACM symposium on Principles of distributed computing*, pages 134–142, 1984.

[95] Markus Michels and Patrick Horster. Cryptanalysis of a voting scheme. Tr-96-1, University of Technology Chemnitz-Zwickau, Straße der Nationen 62 D-09111 Chemnitz Germany, February 1996.

[96] Harriet Nathan. Joseph P. Harris professor and practitioner: Government, election, reform and the votomatic. Unversity of California, 1983. An interview conducted by Harriet Nathan in 1980.

[97] Andrew C. Neff. A verifiable secret shuffe and its application to e-voting, August 2001.

[98] C. Andrew Neff and Jim Adler. Verifiable e-voting. VoteHere Inc. White Paper, August 2003.

[99] Peter G. Neumann. Illustrative risks to the public in the use of computer systems and related technology. NAS Framework for Understanding Electronic Voting, white paper, November 2004.

[100] Terry Newman. Tasmania and the secret ballot. *Australian Journal of Politics and History*, 49(1):93–101, 2003.

[101] NIST. *Common Criteria for Information Technology Security Evaluation*, 2.1 edition, August 1999.

[102] Pippa Norris. Will new technology boost turnout? Working Paper Series RWP03-034, Social Science Research Network, August 2003.

[103] Pippa Norris. *Electoral Engineering: Voting rules and behaviour*. Cambridge University Press, The Edinburgh Building, Cambridge, CB2 2RU, UK, 2004.

[104] Eric J. Novotny. Democracy by computer: Design, operation, and implementation of a civic communications system. In *The Systems Approach: Key to Successful Computer Applications, Thirteenth Annual Technical Symposium*. Washington D.C. Chapter ACM and Institute for Computer Science and Technology, National Bureau of Standards, June 1974.

[105] UK-St Leonards-on-Sea: electronic electoral services and systems. contract notice 2005/s 67-064977. Office of the Deputy Prime Minister, April 2005.

[106] Cornelius O'Leary. *The Elimination of Corrupt and Illegal Practices in British Elections 1868–1911*. Oxford University Press, Amen House, London E.C.4, 1962.

[107] Anne-Marie Oostveen and Peter van den Besselaar. E-voting and media effects, an exploratory study. In *EMTEL 2003: New Media and Everyday Life in Europe*, London, UK, April 2003.

[108] Anne-Marie Oostveen and Peter van den Besselaar. Ask no questions and be told no lies security of computer based voting systems; user's trust and perceptions. In

Urs E. Gattiker, editor, *EICAR 2004 Annual Conference CD-ROM*, Grand-Duché de Luxembourg, May 2004. European Institute for Computer Anti-Virus Research.

[109] Anne-Marie Oostveen and Peter van den Besselaar. Security as belief user's perceptions on the security of e-voting systems. In Alexander Prosser and Robert Krimmer, editors, *Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG*, volume 47 of *Lecture Notes in Informatics*, pages 73–82, Schloß Hofen / Bregenz, Lake of Constance, Austria, July 2004. Gesellschaft fr Informatik.

[110] Wolter Pieters. What proof do we prefer? Variants of verifiability in voting. In Ryan et al. [123], pages 33–39.

[111] Jessie Pilgrim. United Kingdom of Great britain and Northern Ireland general election 5 May 2005. Assessment Mission Report 15921, Organisation Security and Co-operation in Europe/Office for Democratic Institutions and Human Rights, Warsaw, August 2005.

[112] Parliamentary and Municipal Elections (Ballot) Act, 1872. Ch. 33.

[113] Lawrence Pratchett. *The Implementation of Electronic Voting in the UK*. LGA Publications, 2002.

[114] Brian Randell and Peter Y.A. Ryan. Voting technologies and trust. Technical Report 911, University of Newcastle upon Tyne, School of Computing Science, June 2005.

[115] Andrew Reynolds and Ben Reilly. *International IDEA Handbook of Electoral System Design*. SRM Production Services, Sdn. Bhd. Malaysia., 2nd edition, 2002.

[116] David J. Reynolds. A method for electronic voting with coercion-free receipt. In *Frontiers in Electronic Elections (FEE 2005)*, Milan, Italy, September 2005.

[117] Andreu Riera. *Design of Implementable Solutions for Large Scale Electronic Voting Schemes*. PhD thesis, Autonomous University of Barcelona, Bellaterra, Spain, December 1999.

[118] Andreu Riera. Comments by Scytl on the SERVE security report. Response, Scytl Online World Security, Barcelona, Spain, April 2004.

[119] Susan King Roth. Disenfranchised by design: voting systems and the election process. *Information Design Journal*, 9(1), 1998.

[120] Representation of the People Act, 1918. Ch. 64.

[121] Representation of the People Act, 1983. Ch. 2.

[122] Representation of the People Act, 2000. Ch. 2.

[123] Peter Ryan, Stuart Anderson, Tim Storer, Jeremy Bryans, and Ishbel Duncan, editors. *Workshop on e-Voting and e-Government in the UK*, Edinburgh, UK, February 2006. National e-Science Centre, University of St Andrews.

[124] Peter Y.A. Ryan and Thea Peacock. Prêt á voter: a system perspective. Technical Report CS-TR-929, School of Computing Science, University of Newcastle, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, September 2005.

[125] Scotland Act, 1998. Ch. 46.

[126] Larry Sabato and Glenn Simpson. *Dirty Little Secrets: The Persistence of Corruption in American Politics*. Random House/Times Books, New York, N.Y., 1996.

[127] Roy G. Saltman. Effective use of computing technology in vote tallying. Final Project Report NBS SP 500-30, National Bureau of Standards, Washington D.C. 20234, March 1975.

[128] Roy G. Saltman. Accuracy, integrity and security in computerized vote-tallying. Research Report 500-158, National Bureau of Standards, August 1988.

[129] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, 605 Third Avenue, New York, N.Y. 10158-0012, third edition, 1996.

[130] Bruce Schneier. Voting security and technology. *IEEE Security and Privacy*, 2(1):38–47, January 2004.

[131] Diebold accuvote-ts voting system and processes. Risk assessment report, Science Applications International Corporation on behalf of the State of Maryland Department of Budget and Management, Office of Information Technology, 45 Calvert Street Annapolis, MD 21401, September 2003.

[132] Chris Sear and Oonagh Gay. Measures to address low turnout. Standard Note SNPC 2051, House of Commons Library, August 2003.

[133] Disability access standards for the electoral modernisation pilot projects access standards for e-voting and e-counting technology version 1. Sense/SCOPE, November 2002.

[134] Matthew P. Smith, Kieran Coughlan, Deirdre Lane, Danny O' Hare, and Brian Sweeney. First report on the secrecy, accuracy and testing of the chosen electronic voting system. Commission on Electronic Voting, Kildare House, Kildare Street, Dublin, December 2004.

[135] Warren Smith. Cryptography meets voting. Temple University, September 2005.

[136] R. William Soukoreff and I. Scott MacKenzie. Metrics for text entry research: an evaluation of MSD and KSPC, and a new unified error metric. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 113–120, Ft. Lauderdale, Florida, USA, 2003. ACM Press.

[137] R. William Soukoreff and I. Scott MacKenzie. Recent developments in text-entry error rate measurement. In *CHI '04: CHI '04 extended abstracts on Human factors in computing systems*, pages 1425–1428, Vienna, Austria, 2004. ACM Press.

[138] Tim Storer and Ishbel Duncan. Polsterless remote electronic voting. *Journal of E–Government*, 1(1):75–103, October 2004.

[139] Electronic counting at the london elections june 2004. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, December 2004.

[140] Ken Thomson. reflections on trust. *Communications of the ACM*, 27(8):761–763, August 1984.

[141] Alan M. Turing. On computable numbers with an application to the entscheidungsproblem. In *London Math. Soc*, volume 42, pages 230–265, 1936.

[142] Bush vs Gore 531 U.S. 98 (2000).

[143] Maarten W. van Someren, Yvonne F. Barnard, and Jacobijn A.C. Sandberg. *The Think Aloud Method A practical guide to modelling cognitive processes*. Knowledge Based Systems Series. Academic Press, London, 1994.

[144] David A. Wheeler. Countering trusting trust through diverse double-compiling. In *21st Annual Computer Security Applications Conference*, pages 33–48, Tucson, Arizona, December 2005. IEEE Computer Society.

[145] Eugene Windsor. Local government and transport committee 2nd meeting. Scottish Parliament, January 2004.

[146] Jessica Yonwin. Election statistics 1918–2004. Research Paper 04/61, House of Commons Library, July 2004.

Glossary

A

Anonymity With respect to voting schemes, anonymity refers to the inability of an observer to determine the identities of voters participating in an election.

B

Ballot Voting system implementation and record of a voter's choice (vote).

Balloted Voting System A voting system which does store a collection of votes individually prior to tallying.

Ballotless Voting System A voting system which does not store a collection of votes individually prior to tallying.

Blind Signature Scheme A voting scheme in which a *blinding* layer of encryption is applied to a vote, prior to a *Validator* applying a signature. When the blinding layer is removed from the vote, a signature for the vote may be obtained from the signature applied to the blinded vote.

Bulletin Board A cryptographic primitive which models a secure public broadcast channel.

C

CESG Formally Communications and Electronic Security Group, the commerical arm of GCHQ, the United Kingdoms telecommunications interception agency. CESG conducted a study into electronic voting requirements for the UK and proposed a potential security mechanism.

Coercion Resistance A property of some remote voting schemes, in which an external observer is unable to determine (after the fact) whether a voter participated in a particular election.

D

DRE Direct Recording Electronic. A type of voting system technology typically employed in a polling station, which presents voters with choices on an touch screen interface and records choices on electronic media.

E

EAC Election Assistance Commission. US federal body responsible for distributing HAVA 2002 funds and specifying new federal voting system standards.

El Gamal A public key crypto scheme with homomorphic properties.

Election The execution of the rules specified by an electoral system according to some initiation parameters (candidates, voters etc).

Electoral Commission An organisation common in many states responsible for some administration of elections. In the United Kingdom, the Electoral Commission monitors campaign spending, specifies constituency boundaries and conducts research into alternative voting systems.

Electoral System Set of rules under which define how votes are cast and counted for an election. Examples include:

- Single Member Simple Pluarality(SMSP)
- Multi Member Simple Plurality(MMSM)
- Single Non Transferable Vote(SNTV)
- Single Transferable Vote (STV)
- Closed List (CL)
- Open List (OL)

.

Electorate The collective term for the eligible voters in an election.

F

FEC Federal Election Commission. US federal body responsible for establishing Voluntary Voting System Standards in 1990 and 2002. The body also administer campaign finance reporting for US public elections.

Franchise The criteria by which a voter's eligibility to participate in an election is defined.

H

HCI Human Computer Interaction - a field in computer science.

Homomorphic encryption scheme An encryption scheme for which for plain text operator $\oplus$ and cipher text operator $\otimes$ the property $E(a) \times E(b) = E(a \oplus b)$ holds.

I

ICHR International Convention on Human Rights.

ISO International Standards Organisation.

M

MAC Message Authentication Code.

Mix Net Cryptographic primitive which may be employed as an anonymous channel.

O

Optical Scan A class of voting technologies in which paper ballots are scanned for marks made by voters to indicate choices. Marking devices vary from infra-red reflective inks to ordinary ink marks which a scanner is able to distinguish from background colours.

P

Paper Ballot Class of voting technologies on which choices are marked on sheets of paper and counted by hand. Paper ballots may be pre-prepared by election organisers to list nominated choices, or else prepared individually by a voter. Paper ballots have recently been proposed for combination with DRE machines.

Personation Attack on the accuracy on an election in which a voter's identity is used by another to cast an illegal vote.

Public Key Infrastructure A cryptographic technology to support the secure distribution of public keys.

Punch Card A class of voting technologies in which a vote is marked on a card ballot by punching through pre-scored holes. Votes are counted by a device which checks for holes (using a light sensor) in pre-programmed positions.

R

Receipt Free A voting scheme which does not provide a voter with a transferable proof of how they voted.

Requirements Model A methodology for the capture of requirements from a voting context.

REV Remote Electronic Voting. A type of voting system which permits vote casting from an unsupervised location using electronic communication channels.

RSA Rivest Shamir Adleman. A public key crypto scheme.

S

SMS Simple Message Service. A common messsaging application for mobile phones.

SSL Secure Socket Layer. Secure protocol in common use, for example to secure HTTP comunication.

System Indistinguishability In terms of secrecy requirements, system indistinguishability refers to a property of a voting scheme in which an observer cannot distinguish between two voting schemes in which two voters swap the votes they cast. The definition avoids the difficulties associated with ensuring secrecy in the presence of unanimity of votes.

T

TGDC Technical Guidelines Development Committee. A committee of the US EAC responsible for developing the VVSG standards for voting systems.

U

Universially Verifiable A voting scheme which provides the external observers of an election to determine whether a published tally is accurate.

V

Vote Electoral system level description of a voter's choice, constrained by the properties of the electoral system and the constraints on vote casting made by usability requirements.

Voter Agent permitted to participate in one or more rounds of voting in an election.

Voter Verifiable A voting scheme which permits a voter to confirm that their vote has been incorporated in a tally. The verification may or may not be receipt free.

Voting Context The circumstances in which a vote takes place. The voting context provides a set of requirements to be fulfilled by a voting system used to conduct the vote.

Voting Privacy With respect to voting schemes, privacy refers to the inability to associate a vote with a voter participating in an election.

Voting Scheme An abstract description of a voting system which implements a set of requirements for a particular voting contexts.

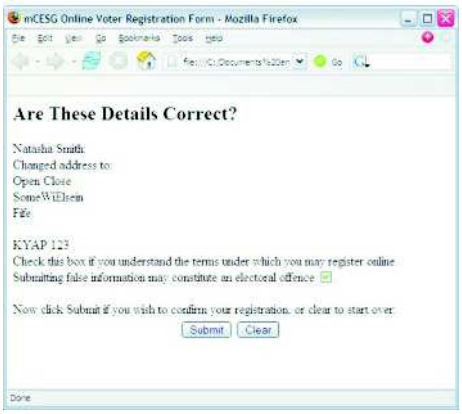
Voting System Collection of technologies, media and processes that implement a voting scheme.

Appendix A

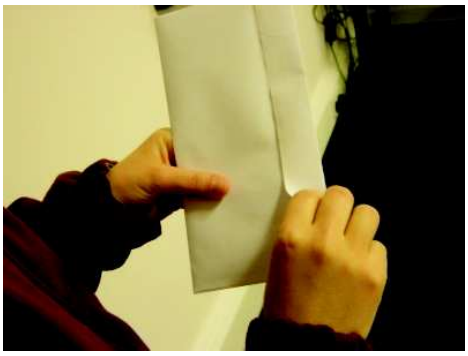
User Acceptance Study Storyboard

The storyboard below illustrates the storyboard used to develop the videotaped scenario for the user-acceptance study of the mCESG scheme discussed in Section 6.4.

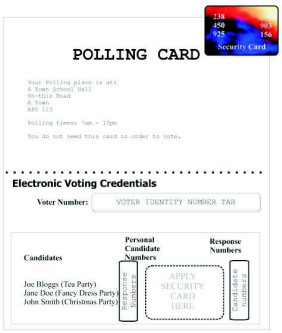
	
1.Having moved house, Natasha decides to register to vote at her new local authority online, rather than by post.	2.Natasha fills in a form online, using the registration document sent to her house. She decides to request electronic voting credentials because she may be busy on polling day.



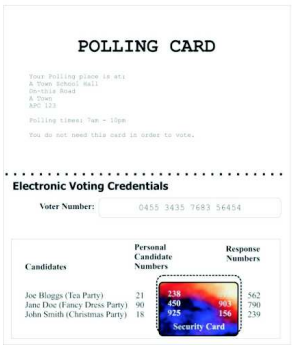
3.Natasha checks the box to indicate that she has understood her legal obligations before clicking submit.



4.Two separate voting credential documents arrive in the post. This helps prevent the credentials being intercepted by a fraudster.



5.The voting credentials are sent as two separate documents polling card and a security card (top right).

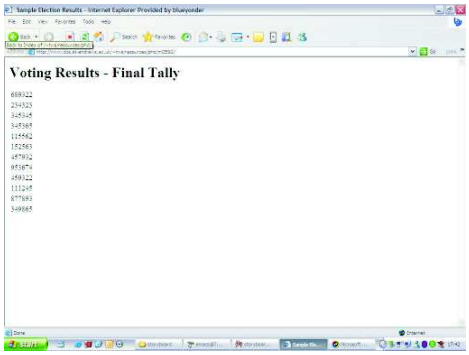


6.Natasha removes the protective tabs on the polling card and sticks the security card where indicated, to reveal the complete Voter Number and Candidate Numbers.

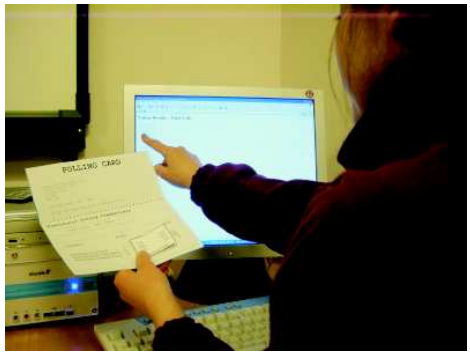
	
7.On her way to work, Natasha opens her polling card to cast a vote, using her mobile phone. She types her Voter Number and the Candidate Number of her choice into an SMS message.	8.In a few mintues, a confirmation message arrives at Natasha's mobile.

9.Natasha sits down at her desk at work. She works in an open plan office, where one colleague sits near enough to see her screen.

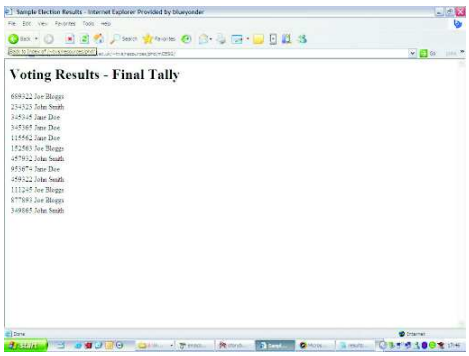
10.Natasha checks that the Response Number next to her chosen candidate on her voting credential has been published on the election's webpage along with those for all votes cast.



11.Natasha uses the search function of her web–browser to find the number.



12.After the close of poll, Natasha can confirm that the correct candidate was published next to her Response Number on the election's webpage.



13.Natasha uses the browser search function to find her number again. Assuming everybody else checks their vote, the results of the election will be accurate.