

Two Variations to the mCESG Pollsterless e-Voting Scheme

Tim Storer and Ishbel Duncan
University of St. Andrews
{tws,ishbel}@dcs.st-and.ac.uk

Abstract—Over the past several years, the UK Government has piloted several new voting technologies during local authority elections. The mCESG pollsterless Remote Electronic Voting (REV) system, which was designed with the UK electoral context in mind, is described in detail in [1]. Here, we describe two variations to the mCESG scheme which (a) improve its suitability for the variety of electoral systems in use in the UK and (b) provide a means for resisting coercion attacks to which the original scheme was vulnerable.

I. THE UK ELECTORAL CONTEXT

Elections in the United Kingdom are governed by a variety of Acts of Parliament, most notably the Representation of the People Act 1983 [2], although this has been amended several times [3], [4]. Prior to 1999, elections on the mainland were conducted via a simple plurality electoral system, generally to single member wards and constituencies.¹ However, following the passage of devolution legislation [5] and changes to the way in which members of the European Parliament are elected [6], the UK has begun to experiment with a variety of electoral systems.

Most significantly, the instant run-off electoral system is used to elect the Mayor of London, whilst a Single Transferable Vote (STV) system will be employed for local authority elections in Scotland in 2007, previously only used for provincial elections in Northern Ireland [7]. The manner in which successful candidates are elected under such systems is described in detail elsewhere [8] and will not be repeated here. Suffice that voting systems employed where STV has been chosen as the appropriate electoral system must permit voters to rank their choices of candidates, 1...n as desired, rather than selecting a single option.

A second feature of UK elections is that (despite the requirement for vote secrecy) due to the weak procedure employed for authenticating voter identities, a tracing mechanism is incorporated with the existing paper ballot voting system [9]. For the current voting system, voters are required to assert their name and address in order that a polling official may identify their entry in an electoral roll published for the election. In the first instance, a voter may only be asked to confirm their name and address and that they have not yet voted by a polling official [10]. The ballot tracing mechanism thus permits identifiable ballots to be removed from a tally after

the act of voting, although such a practice is extremely rare [11].

Given the context, a single electronic voting system employed in the UK must fulfill a number of high-level requirements.

- The range of electoral systems now employed in the UK would need to be accommodated by the chosen system, including single option and ranked voting systems.
- Improve the convenience of casting a vote and accessibility of the electoral process for voters with a range of capabilities and resources.
- Assuming that the method of authenticating voters prior to permitting them to cast a vote is unchanged, a UK electronic voting system would likely need to provide a continuing means of tracing and removing votes from a tally where they have been found to have been cast fraudulently. Such a mechanism must not provide a general means for violating voter secrecy without collusion between the various actors in the electoral infrastructure.
- The voting system technology would need to be acceptable within the Electoral Commission's proposed foundation model requirements for multi-channel voting in the UK [12].

Section II summarises the mCESG remote electronic voting scheme which has been proposed as partially satisfactory for the requirements of the UK electoral context [1]. Section III presents a generalisation of the mCESG scheme in order to provide a feasible means of conducting an election using an ordinal electoral system. Section IV presents a means of converting the publication mechanism such that the verification becomes receipt free. Section VI considers the consequences of introducing the two modifications to the scheme and the prospects for future improvements.

II. OVERVIEW OF THE MCESG REV SCHEME

The mCESG scheme is a modification of a scheme proposed by UK Government's Communication and Electronics Security Group as suitable for UK elections [13]. The CESG scheme was attractive because the voter was not required to perform any cryptographic computations, a requirement of most other proposed REV schemes. Schemes that dispense with this requirement have been termed *pollsterless* since there is no software artifact required to interpret a voter's choices and communicate these to other participants in the vote [14]. These schemes are attractive, as:

¹Prior to 1945, two-member parliamentary constituencies were relatively common; multi-member wards are still employed for local-authority elections in England.

- Votes could be cast using virtually any device capable of remote communication. This includes, for example, mobile phone SMS messaging, ATM bank machines, touch tone telephones.
- *Voter verifiability* permits a voter to confirm that their vote was accurately incorporated in a tally. Many remote electronic voting schemes employ verification mechanisms as a substitute for the perceived transparency of using paper ballots, for example [15], [16]. If a pollster-less scheme is voter verifiable, this may be accomplished without requiring the voter to trust the software artifact (hence *pollster*) to interact correctly with other participants and report back results honestly.

Unfortunately, the original CESG scheme was severely criticised during a consultation period [17], [18], and was dropped from a final document which outlined requirements for REV systems in UK elections [19]. Although the response documents were rather general with regard to the scheme, two specific flaws may be identified:

- The confidentiality of the voting credentials is crucial to the integrity of the election. The monolithic design of the election authority in the original document suggests that there is potential for the election authority to access the voting credentials it generates and then perform a number of un-desirable operations such as electronic ‘ballot box stuffing’.²
- Although the CESG scheme permits voters to confirm that the election authority has correctly received their vote, it is not verifiable, since voters are unable to confirm that their vote is handled properly after receipt.

The mCESG scheme remedied these two deficiencies by distributing the functions of the election authority into several autonomous domains, under the control of organisations that already exist in the UK electoral infrastructure; and by publicly committing the election authority to votes as they are received.

A. Distributed Voting Credential Generation

The mCESG remote electronic voting system depends upon the secure distribution of electronic voting credentials to the voters. The system assumes that the use of the UK postal system in combination with secure payroll stationary constitutes a secure channel between the election authority and the voter for this communication. These consist of a polling card and a security card delivered to the voter separately. Figure 1 illustrates the independent domains of the election authority which are collectively responsible for this task. The election authority consists of:

- A Registration Officer responsible for managing the identities of voters and for the delivery of a polling card containing partial voting credential information.
- A Returning Officer responsible for managing the identities of nominated candidates.

²The practice of adding extra illegitimate votes to a ballot box prior to tallying [11].

- A Vendor responsible for generation of most voting credential values and for the collection of votes during the election.
- An Electoral Commission responsible for delivery of a security card to each voter containing remaining voter credential information.

Figure 1 illustrates the construction of voting credentials for a single voter. The construction involves the generation of various cryptographic Message Authentication Codes (MAC) values by the Returning Officer, Registration Officer and Vendor. The specific algorithm used for this task is not considered here, although MD5 was used in a prototype implementation. Each domain is responsible for the storage of a secret key used in the generation of its own cryptographic MAC values.

On receipt of request for a set of voting credentials for an identified voter, the Registration Officer generates a Voter Number (VN) using the voter’s identity as a seed and requests a permutation of candidate identities from the Returning Officer. On completing this request, the Returning Officer passes a corresponding permutation of Candidate Numbers (CNs) seeded from the candidate’s identities to the Vendor, who also receives the VN from the Registration Officer. The Vendor then generates a set of Personal Candidate Numbers (PCNs) and Response Numbers (RNs) using the VN and CNs as seeds.

The Vendor then passes the generated values back to the Returning Officer and to the Electoral Commission as follows. The Returning Officer receives the first half of each PCN and the second half of each RN; whilst the Electoral Commission receives the second half of each PCN and the first half of each RN. The Returning Officer then compiles these values and the VN into a polling card and delivers this to the Voter. The Returning Officer also passes the voter’s identity to the Electoral Commission which compiles the values it received from the Vendor into a security card and delivers this to the voter.

Note that the VN is unique to each voter, whilst the response numbers are unique between a voter and a candidate. PCN values are non-unique. The complete voting credential is assumed to be a secret owned by the voter, sub-elements of which are known by different domains of the election authority.

B. Casting a Vote

Having received the polling card and security card, the voter is now able to assemble their voting credential (see Figure 2) and cast a vote. To do so, the voter sends a message (for example, in an SMS message) consisting of their VN and the PCN of their chosen candidate to the Vendor domain:

$$\underbrace{4547129037384571}_{VN} \underbrace{1642}_{PCN}$$

The voter then waits for a generic response/failure message for their vote. If the response indicates the vote was incorrect the voter is permitted to try again. Alternatively, if the response

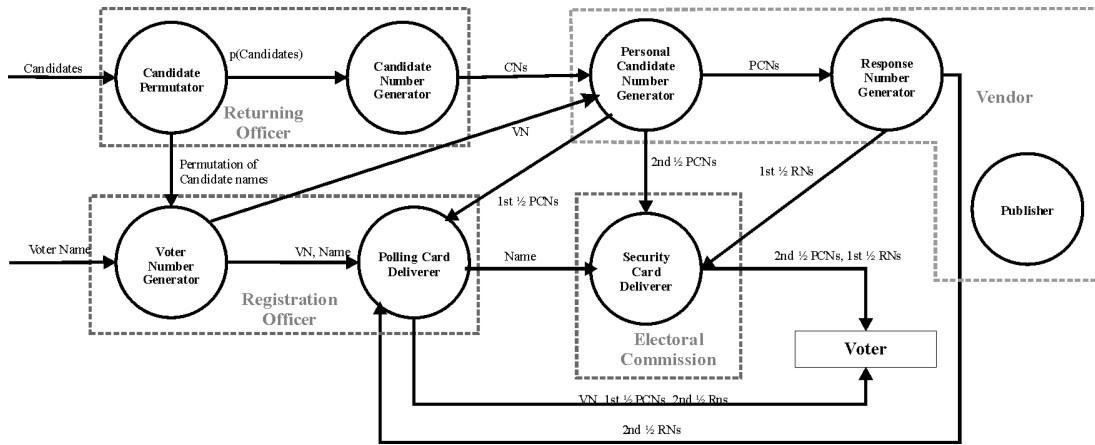


Fig. 1. Communication between the separate domains mCESG election authority architecture during the generation of voting credential documents for a single voter. Note that no single domain has access to all voting credential information for a voter.

Voter Name: Alice JONES				
Voter Number: 4547 1290 3738 4571				
Candidates	Personal Candidate Numbers	Response Numbers		
M. Thatcher	16 42	712 583		
N. Chamberlain	67 24	835 572		
C. Atlee	60 12	932 701		

SECURITY CARD

POLLING CARD

Fig. 2. 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.

indicates that the vote was correctly received, the voter may now proceed to verify this.

C. Verification of Vote

Verification occurs in two stages – pre and post declaration of results, as illustrated in Figure 3. In the initial verification step the election authority publicly commits to the voter’s choice, without having to reveal its value. To achieve this, the Vendor converts received votes to the corresponding RNs, as illustrated on the voting credential (Figure 2). Note that the Vendor is the domain responsible for generating response numbers from Voter VN/PCN combinations during the initiation phase. The calculated RN is then published by the Vendor, for example on an electronic bulletin board.

Since each RN is a unique value describing a relationship between a voter and a chosen candidate, publishing the response number commits the election authority to the voter’s choice without directly revealing the value of that choice. Publishing the RN does not violate the secrecy of the voter’s choice. The voter accesses the bulletin board of RNs after

casting a vote and confirms that the correct value is present in the list. In the event that the RN does not appear after some period of time (before the results are declared), the voter may contact the election authority to resolve the dispute or obtain another vote.

The second stage of the verification process occurs after the publication of results. The Returning Officer supplies the Vendor with the identity of the candidate associated with each RN published on the bulletin board which are then also published. Each voter may then confirm that the candidate published next to their RN corresponds to that on their voting credential. Note that following the publication of candidate names, a voter can only challenge a discrepancy between a published RN and a candidate - they cannot challenge which RN appears in the published list.

The voting and verification procedure requires only communication on the part of the voter – cryptographic operations are only performed across the domains of the election authority during initiation. This approach preserves the pollsterless property of the original CESG scheme (and its benefits) whilst also permitting direct voter verifiability. Cryptographic computations are only employed in the generation of voting credentials by the election authority during the initiation phase.

III. VARIATION FOR 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 exacerbates this complexity, since a voter would need to be presented with a PCN 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 increase the size of the voting credential provided to the voter.

To permit ranked votes, the voting credentials are modified as illustrated in Figure 4. *Preference numbers* are incorporated

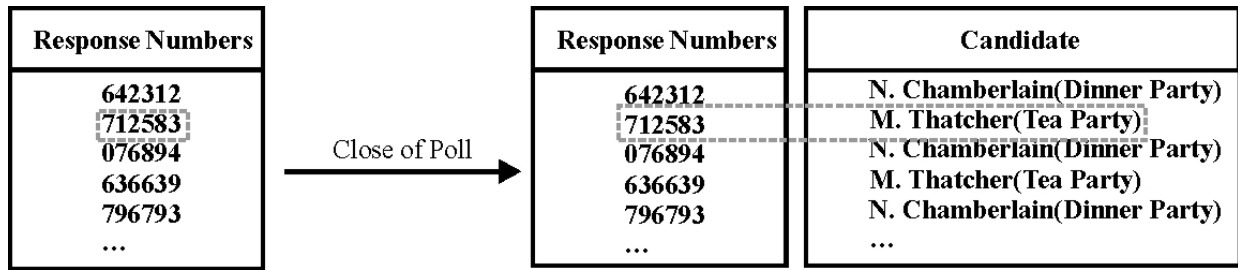


Fig. 3. The lists of response numbers and votes committed to by the Vendor’s Publisher module during the two phases of verification. The gray dotted boxes indicate the location of Alice’s vote in the list.

Voter Name: Alice JONES Voter Number: 4547 1290 3738 4571		Check Sum Numbers 1: 5423 2: 8965 3: 1209
Candidates	Personal Candidate Numbers	Response Numbers
	{1, 2, 3}	{1, 2, 3}
M. Thatcher	1{6, 4, 8}42	712{5, 9, 3}83
N. Chamberlain	6{7, 1, 0}24	835{5, 0, 2}72
C. Atlee	6{0, 8, 1}12	932{7, 7, 9}01

SECURITY CARD

POLLING CARD

Fig. 4. Voting credentials modified to permit ordinal (ranked) voting for electoral systems such as Single Transferable Vote (STV). The credentials are modified from figure 2 to include *preference codes* which indicate the preference to be associated with a particular candidate.

into the PCNs and the RNs 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 4 the preference codes for PCNs are inserted at index one, whilst the preference codes for the RNs are inserted at index three. In addition, a set of Check Sum Numbers (CSNs) are added to the voting credential. The CSNs are used to indicate to the election authority the number of preferences that are to be in the voting message, preventing an attacker from intercepting a message and removing lower order ranked candidates.

To cast a vote, the voter sends a message similar to that described in section II-B. However, the voter must choose a rank for each candidate voted for, by choosing exactly one preference code. For example, should the voter wish to vote Neville Chamberlain as first preference and Clement Atlee for second preference, they would send the following message:

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

N. Chamberlain C. Atlee

During the first phase of the verification process, the voter

would expect to see the RNs for each candidate they voted for as before, but also containing the correct RNs. 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 RN, for example:

835{5}72 932{7}01 1st: N. Chamberlain 2nd: C. Atlee

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.

IV. PROVIDING RECEIPT-FREENESS

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 voting schemes are designed to be *receipt-free* (for example [20]) where a voter is unable to prove they voted a certain way to another participant after the fact. Further, the voter cannot prove to an attacker that their vote was incorporated in the tally of votes.

The goal of the adaption 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 Number (PRN) on their voting credential. Each candidate on the voting credential is assigned a smaller, non-unique Candidate Response Number (CRN). Figure 6 illustrates the modified voting credential. Note that the responsibility for generation and delivery of both new types

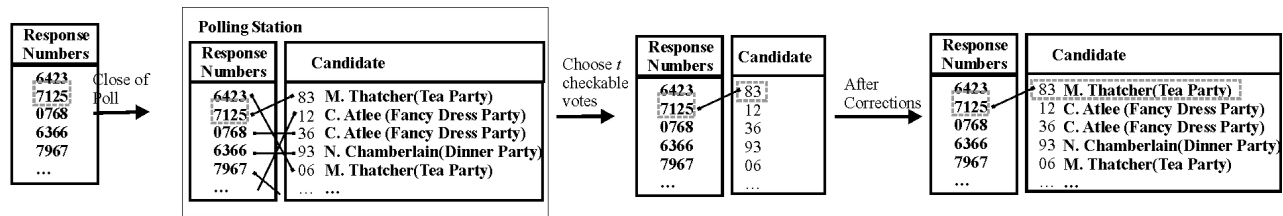


Fig. 5. The transitions that occur in the published list of response numbers during the phases of verification in the receipt-free adaption of the mCESG scheme.

Voter Name: Alice JONES			
Voter Number: 4547 1290 3738 4571			
Personal Response Number: 7125			
Candidates	Personal Candidate Numbers	Response Numbers	
M. Thatcher	16	42	8 3
N. Chamberlain	67	24	7 2
C. Atlee	60	12	0 1
SECURITY CARD			
POLLING CARD			

Fig. 6. Receipt free voting credentials. Note the Response Number is now explicitly divided into Vote Response Number and Candidate Response Numbers.

of RN 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 containing their Personal Voter Number and the Personal Candidate Number of their choice. Figure 5 illustrates the receipt-free verification procedure, which is now split into three phases. Prior to the close of poll, the voter is only able to observe their PRN 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 [21].

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 PRNs, CRNs 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 can-

didates are now permitted to select a small number to be published on the bulletin board. Initially, only the association between the chosen personal RNs and candidate RNs 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 PRNs and CRNs 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 [22], [23].

A. 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:

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

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 t variable could be chosen at the start of the verification process, in agreement between the candidates and election officials.

V. FUTURE WORK: USABILITY TESTING

The preceding discussion has omitted a discussion on the consequences of the adaptations for usability of the mCESG scheme. Previously we posed several questions regarding the usability of the original mCESG scheme [24]. It may be noted that the work-load required of a voter for the ordinal electoral system adaption is linear, as opposed to constant for the original scheme for casting a vote. Although the receipt-free adaption does not require extra work on behalf of the voter, it is perhaps intuitively hard to understand, since the voter may only verify that their vote was counted correctly if their vote is selected.

The variations of the mCESG scheme thus raises several further questions;

- 1) *What additional error rate can be expected from voters using the ordinal electoral system variation.* If a sizable proportion of voters are unable to follow the voting procedure the accessibility of the mCESG consequently will reduce.
- 2) *What proportion of voters will take the necessary measures to verify that their vote has been correctly tallied?* Although the election authority cannot determine which voters have not verified their vote, if the proportion of voters who do so is sufficiently low, then the probability of the election authority cheating undetectably will increase (effectively due to reduced t).

It is anticipated that only substantial usability testing will resolve the two questions posed above. A prototype of the modified CESG system has already been implemented - it is anticipated that trials will take place within the next year.

VI. CONCLUSIONS

Two variations have been presented to the mCESG pollsterless remote electronic voting scheme. The scheme has been demonstrated to be capable of supporting ordinal electoral systems that are currently being introduced for UK elections. A means of providing a threshold receipt-free mechanism for the scheme is also described, in which the candidates for election and a small sub-set of voters (the vote checkers) co-operate to verify that the election authority has not cheated, with high probability.

The variations retain the advantageous features of the original scheme, permitting voters to cast and (partially) verify their vote without recourse to a pollster artifact. The design of the scheme is intended to fulfill the requirements of the UK electoral context and thus must be adapted as those requirements change. In particular the scheme has been designed

with the UK government's requirement for multi-channel elections, by providing a scheme that may be employed on a variety of platforms. It is anticipated that testing in elections using a prototype implementation of the scheme will examine questions raised here and elsewhere regarding the usability of the mCESG scheme.

ACKNOWLEDGEMENTS

The work described in this paper is supported by Microsoft Research, Cambridge.

REFERENCES

- [1] T. Storer and I. Duncan, "Polsterless remote electronic voting," *Journal of E-Government*, vol. 1, no. 1, pp. 75–103, October 2004.
- [2] "Representation of the People Act," 1983, ch. 2.
- [3] "Representation of the People Act," 2000, ch. 2.
- [4] "Political Parties, Elections and Referendums Act," 2000, ch. 41.
- [5] "Scotland Act," 1998, ch. 46.
- [6] "European Parliamentary Elections Act," 1999, ch. 1.
- [7] "Local Governance (Scotland) Act," 2004, asp. 9.
- [8] A. Reynolds and B. Reilly, *International IDEA Handbook of Electoral System Design*, 2nd ed. Sdn. Bhd. Malaysia.: SRM Production Services, 2002.
- [9] P. Jackson, C. Rosenstiel, and S. O'Connell, "Ballot secrecy," Electoral Reform Society, 1997.
- [10] "Representation of the People Act," 1983, ch. 2. Sch. 1, R. 35.
- [11] R. Blackburn, *The Electoral System in Britain*. 175 Fifth Avenue, New York N.Y. 10010: St. Martin's Press, 1995.
- [12] "The 2004 European parliamentary elections in the United Kingdom," The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, December 2004. [Online]. Available: http://www.electoralcommission.org.uk/files/dms/ECPartElections2004_154%38-11422_E_N_S_W...pdf
- [13] "e-voting security study," Communications and Electronic Security Group (CESG), July 2002. [Online]. Available: <http://www.edemocracy.gov.uk/library/papers/study.pdf>
- [14] D. Malkhi, O. Margo, and E. Pavlov, "E-voting without 'cryptography'," February 2003. [Online]. Available: citeseer.nj.nec.com/malkhi02evoting.html
- [15] D. Chaum, "Secret-ballot receipts: True voter verifiable elections," *IEEE Security and Privacy*, vol. 2, no. 1, pp. 38–47, January 2004.
- [16] J. Benaloh, "Verifiable secret ballot elections," Ph.D. dissertation, Yale University, December 1996.
- [17] R. Mercuri, "Response to formal request for comment by the CESG (UK) on internet voting," October 2002.
- [18] J. Kitcat, "e-voting security study response: FREE e-democracy project." [Online]. Available: <http://www.free-project.org>
- [19] "e-voting technical and security requirements," Communications and Electronic Security Group (CESG), November 2002. [Online]. Available: <http://www.edemocracy.gov.uk/library/papers/evoting.pdf>
- [20] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections (extended abstract)," in *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*. ACM Press, 1994, pp. 544–553.
- [21] "Representation of the People Act," 1983, ch. 2. Sch. 1, R. 57.
- [22] M. P. Smith, K. Coughlan, D. Lane, D. O'Hare, and B. Sweeney, "First report on the secrecy, accuracy and testing of the chosen electronic voting system," Commission on Electronic Voting, Kildare House, Kildare Street, Dublin 2., December 2004. [Online]. Available: http://www.cev.ie/htm/report/first_report.htm
- [23] "Recommendations for improving reliability of direct recording electronic voting systems," Brennan Centre for Justice and Leadership Conference on Civil Rights. Available at www.civilrights.org/issues/voting/lccr_brennan_report.pdf, July 2004.
- [24] T. Storer and I. Duncan, "Practical remote electronic elections for the UK," in *Privacy, Security and Trust 2004 Proceedings of the Second Annual Conference on Privacy, Security and Trust*, S. Marsh, Ed., National Research Council Canada. Fredericton, New Brunswick, Canada: University of New Brunswick, October 2004, pp. 41–45.