

Practical Remote Electronic Elections for the UK

Tim Storer and Ishbel Duncan
School of Computer Science
University of St Andrews
St Andrews, Fife, KY16 9SS, Scotland.
Email: {tws, ishbel}@dcs.st-and.ac.uk

Abstract—The United Kingdom (UK) government has repeatedly expressed a desire to employ a Remote Electronic Voting (REV) system in a general election after 2006. Most existing REV schemes employ some form of cryptography, either to secure transmission of votes, or to model some desirable feature of public elections. This paper outlines the limitations of employing cryptographic REV schemes and proposes an alternative, *polsterless* scheme, that provides a practical possibility for implementing remote electronic voting in the UK.

I. INTRODUCTION

The United Kingdom (UK) government has repeatedly expressed a desire to conduct an “e-enabled” General Election, sometime after June 2006 (the latest date for the next election). In this context, e-enabled refers to the possibility of casting a vote using a Remote Electronic Voting (REV) system. The interest in such technology has been associated with the desire to increase the convenience of participating in elections, in the face of a declining voter turnout [1].

Evident in the literature, a general assumption regarding REV schemes is that some cryptographic mechanism will be necessary in order to secure communications between a voter and some authority organising the vote, for example [2]–[4]. Alternatively, cryptographic mechanisms have been employed in order to replicate particular properties identified as desirable for REV schemes. A brief summary of the most commonly cited REV schemes demonstrates the significance placed upon cryptography.

A. Existing Cryptographic REV Mechanisms

Chaum proposed a cryptographic mix-network that replicates the mixing and anonymising properties of a ballot box for paper based voting [5]. The mix-network consists of a sequence of mixing servers, each of which obtains from the previous server a collection of votes, which are permuted before being transferred to the next mixing server. Layers of encryption on the votes (which are successively removed by each server) ensure that a vote cannot be traced through the network.

Later, Benaloh proposed the use of homomorphic public key encryption in order to provide a universally verifiable REV scheme [6], such that for votes $a, b \in \{0, 1\}$ and a homomorphic public key encryption mechanism E :

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

Therefore, if the votes consist of only 0s and 1s, the decryption of the sum of votes (using the secret key) produces a tally of the votes.

Alternatively, a two-step blind signature REV scheme was proposed in [7] as a means of authenticating and then anonymising a vote. Blind signature schemes have been implemented in several REV systems [8], [9]. A voter completes and encrypts a vote employing a public key provided by the voting authority. Then the voter signs the encrypted vote using their personal secret key. Next, the vote is transmitted to a validator that verifies the voter’s signature before adding their own signature to the vote. The validator returns the vote to the voter, who removes their original signature and sends the now anonymous vote to an electronic ballot box for later tallying.

The three schemes outlined above form the basis for a larger number of variants and/or later improvements. Various other cryptographic REV schemes have also been proposed for non-election circumstances, for example jury voting [10] or parliamentary voting where it may be desirable to reveal the association between a voter and a vote [11]. Such schemes demonstrate that the context in which a vote takes place (and therefore the requirements of a suitable REV system) vary considerably.

B. Limitations of Cryptographic REV Schemes

A prior requirement of all cryptographic REV schemes is that the voter is capable of performing cryptographic computations, typically involving non-trivial mathematics such as logarithms. Malkhi noted that in practice, this requires that the authority conducting a vote provides the voter with a software artifact, or *polster* [12]. The polster accepts the voter’s choices through some user interface and then conducts the particular REV scheme’s protocol with the components of the election authority, performing all the necessary cryptographic computations on behalf of the voter. The polster may also report back to the voter whether the vote has been correctly incorporated in the tally of results, if this is a feature of the REV scheme. This necessary deployment of a software polster for cryptographic REV schemes imposes two significant limitations:

- 1) *The mobility of voting is limited to cryptographically capable devices.* The voter must use a device that is powerful enough to undertake cryptographic operations secure enough to minimise the threat of secrecy being violated. Presently, this requirement limits the range of devices able to support the activities of a polster

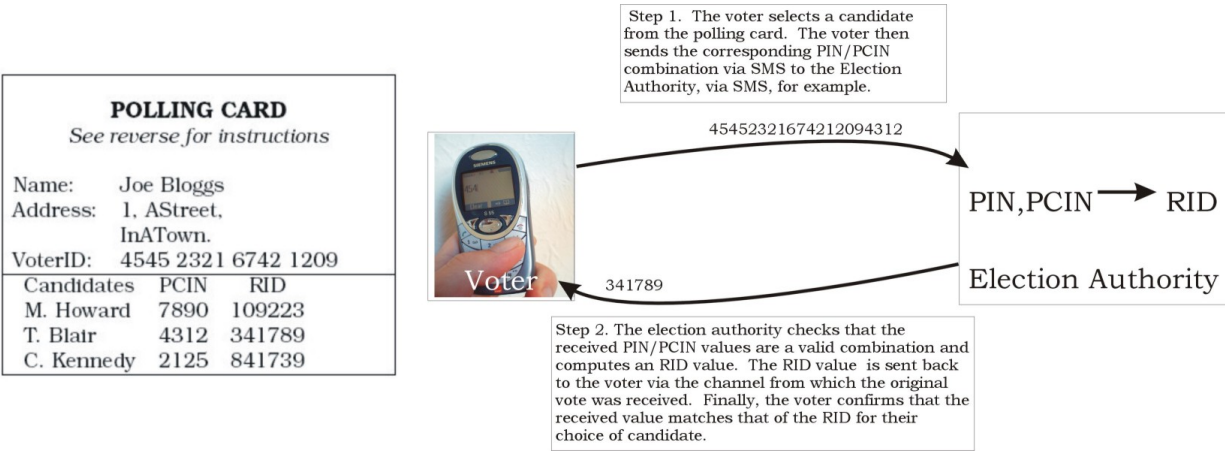


Fig. 1. The CESG Polsterless Remote Electronic Voting Scheme.

[2], although future advances in mobile technology may mitigate this problem. In the mean time, the dependence on computing technology such as desktop or laptop PCs exasperates the so-called *digital divide* as a significant obstacle to the implementation of an REV system. Whilst less powerful networked devices such as mobile phones are relatively pervasive in the UK, only just over half of the same population have home Internet access [1]. For REV to be successful, it would seem likely that implementation would be via a technology that a near total proportion of the population had access to and were familiar with operating.

- 2) *The voter is required to trust the polster to operate correctly.* A range of proposed REV schemes are stated to support *voter verifiability*, such that a voter may determine (through some cryptographic mechanism) that their vote has been correctly incorporated in the tally of results and that the REV scheme in general has functioned as expected. However, since the voter is likely to be unable to perform the necessary computation for themselves (particularly in public elections, where the skills and education of voters varies considerably), the schemes are perhaps better described as *polster verifiable*, since it is the polster that determines whether the cast vote has been correctly incorporated in the tally of results. The voter is instead reliant on the polster to report back honestly; since the polster was provided by the election authority, it is questionable whether the reporting of the polster could be considered independent of the election authority.

Alternatively, if the specifications of the REV scheme's implementation are publicly available, the voter may choose to rely on a polster provided by a third party source. In these circumstances the voter is asked to trust both that the third party does not act in collusion with the election authority and also that the polster does not leak the voter's choices to the third party. Whilst the risks associated with this option depend to some degree on the choice of third party, the voter is

provided with no absolute guarantee that the polster has acted only on their behalf for the vote. Nor does this approach limit the need for sufficiently powerful technology to execute the polster software.

II. POLSTERLESS REMOTE ELECTRONIC VOTING

In response to the limitations imposed by the need for the voter to conduct cryptographic operations, two schemes have been proposed that attempt to eliminate the intermediary activity of a polster. It is anticipated that *polsterless* REV schemes will provide more practical solutions to the implementation of REV systems, since a feature is the reduction in the computational work required of the voter, sufficient that the polster may be dispensed with and the computations performed directly by the voter. Such schemes have the advantage of providing the voter with the opportunity to directly verify that the REV system is operating correctly.

A. Advanced Check Vectors

Malkhi et al, who initially noted the problems associated with trusting a polster, proposed the use of *advanced check vectors* as the mathematical basis for a polsterless REV scheme [12]. A dealer (the election registrar) delivers sets of vectors of values to intermediaries (the elector), along with a corresponding secret s for a group of the vectors (the candidates). In order to cast a vote, the intermediary sends a Vector V to a receiver (the tallier) who returns a check vector B to the intermediary. The elector then confirms $VB = s$ in order to obtain a receipt for the vote. The system requires the prior-establishment of *secure channels* between electors and the election authorities.

As may be noted, whilst the Malkhi scheme reduces the computational load for voters (particularly by avoiding the use of public key mathematics), there is still a considerable amount of computation for the voter to perform in order to verify that a vote has been correctly tallied. Disputes, disruptions or delays may, for example, arise when voters are unable to perform the vector computation accurately, even though the correct check vector has been received.

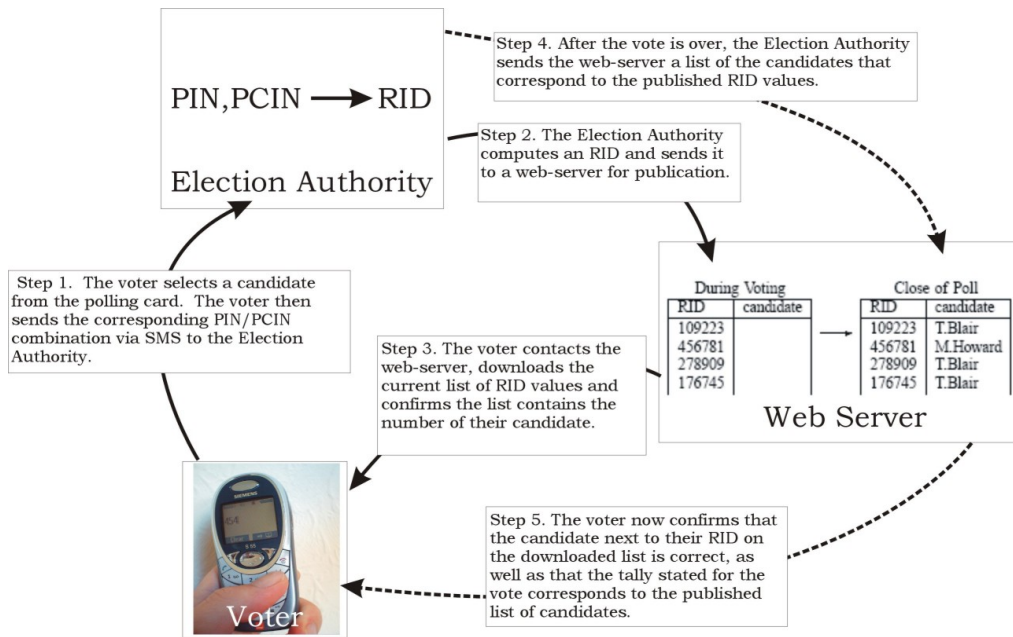


Fig. 2. The Modified CESG Remote Electronic Voting system.

B. The CESG Scheme

The UK Government's Communications and Electronics Security Group (CESG) proposed a polsterless REV scheme specifically for UK general elections [13]. In order to participate in the scheme, a voter must pre-register with the local authority conducting the election.

Once the nomination period for the election has ended (and assuming that more than one candidate has been nominated), the voter receives a *polling card* similar to that inset to figure 1. The CESG scheme anticipates that the polling card will be printed on secure payroll stationary (to deter tampering) and delivered to the voter by post. The polling card provides the voter with a *Personal Identification Number* (PIN) and details the candidates who have been nominated for the election. A *Personal Candidate Identification Number* (PCIN) and a *Return Identity number* (RID) is associated with each candidate. All the values described here are generated using cryptographic hash functions by the election authority. Although the scheme does employ cryptography, since the voter is not involved the computation, the polsterless property of the scheme is not violated.

To cast a vote using the CESG scheme, a voter transmits their PIN and PCIN to the election authority, using the Simple Message Service (SMS) on a mobile telephone, for example. The election authority then computes an RID and transmits this to the device that sent the original PIN/PCIN message. The voter then confirms that the received RID matches that of their selected candidate on the polling card. Figure 1 illustrates the vote casting process.

When the CESG scheme was initially proposed, the agency issued an accompanying consultation document with requests for responses. Of those who responded, the tone was distinctly

negative, in general implying that remote electronic voting itself was insecure and that the proposed scheme was inadequate to ensure a robust REV system [14], [15]. A more specific flaw identified is that though the receipt of an RID from the election authority re-assures the voter that their vote was correctly received, there is no guarantee that the election authority will process the vote correctly or include the vote in the tally. Further, the voter has no means of redress if they suspect their vote has not been counted, if their name does not appear on the marked roll, for example.¹ These circumstances are mirrored for the election authority, which cannot prove that a voter who states that they received an incorrect RID value is not behaving maliciously.

III. MODIFYING THE CESG SCHEME

Despite the flaws of the CESG scheme, it has a number of advantageous properties. Most notably, the scheme requires virtually no computation on the part of the voter, other than to compare values to check for equality. Therefore the CESG scheme overcomes the first limitation of cryptographic schemes, since the protocol can be conducted using any inter-networked device, as demonstrated in figure 1. Since the scheme does not provide voter verifiability however, the second limitation is not overcome, since the voter is still unable to independently ensure their vote was tallied correctly. A modification to the scheme described below provides for voter verifiability without violating the polsterless property.

A. Providing for Voter Verifiability

Figure 2 illustrates a modification to the CESG scheme that provides for voter verifiability, permitting a voter to ensure

¹The marked roll refers to the UK practice of publishing the names of those voters who cast a vote

that their vote was correctly included in the tally of votes, and permitting redress if the voter discovers a failure. As before, the voter receives a polling card printed on secure stationary, with the same format as for the original CESC scheme. The voter casts a vote as before, using whichever communication channel suits, in this case an SMS message.

However, rather than transmitting the RID value back to the voter, in step 3 the RID computed from the PIN/PCIN received is added to a list of publicly available RID values that have been computed from votes received. In figure 2, the list is published on a web server, where it is freely available for download by both voters and external observers. Note that the choice of a web-server for the example is not the only possibility for the publication of RID values. Alternatives may include digital or satellite television stations, that broadcast the RID lists. Indeed, there is no reason to use only a single medium for the publication of the RID values, since the intention is to disseminate them as widely as possible.

Prior to the close of the election, the voter may confirm that their RID has been included in the published list. If the RID value does not appear after some reasonable period of time, the voter should contact the election authority in order to determine whether a failure has occurred; whether they should re-cast a vote, or choose an alternative, non-electronic medium in the event of a serious failure in the system.

On the close of poll, the election authority publishes the names of candidates who correspond to the RID values on the web server. The voter may then confirm that the RID and candidate name tuple on the web server match that on the polling card. In the event of a discrepancy, the voter may demand that the identity of the candidate they voted for be changed, but not the RID value. This scheme therefore provides the voter with the ability to independently verify that their vote has been correctly tallied via a two stage process. The voter may directly verify their vote without employing a software polster, or alternatively, via reduced, but still complex computations as in [12].

Note that since the association the assignment of RID values to voters is a secret known to only the election authority and the respective voters, publishing the association between RID values and candidates does not compromise the secrecy of the election. Each voter may only verify that the RID they noted as being for the correct candidate prior to the close of poll is associated with the correct candidate after the close of poll.

B. Improving the Anonymity of Voting

Providing anonymity in an REV scheme is complicated by the requirements that exist in the UK context. UK electoral law requires that (a) a list of voters who participated in the election is made public; and (b) with respect to paper ballots, the *counter-foil* associated with each is marked with the electoral roll number of the respective vote [16]. These provisions ensure that whilst the choice of a voter is secret, whether they participated is not. Further, under certain conditions (when an election petition has been submitted stating that personation is suspected [17]) the association between a vote and a voter

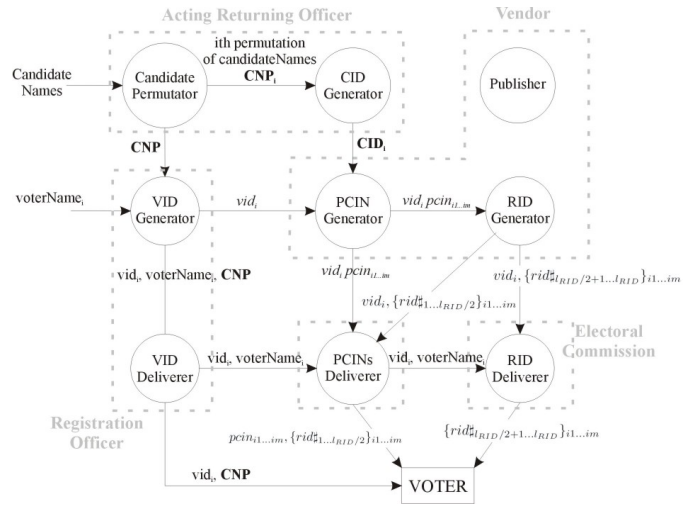


Fig. 3. Architecture of the modified CESC remote electronic voting scheme election authority. The diagram illustrates distributed polling card generation and delivery through the architecture.

may be discovered. It would seem that unless the requirements of the UK voting system change, an REV scheme must also provide this facility in the appropriate situation only.

The design of the election authority for the un-modified CESC scheme is somewhat monolithic in nature. Whilst an outline of a modular architecture anticipated for the election authority was provided in the original study, the operation of these modules and the need to generate the polling card as a single document imply the need for a single domain of control in which the modules must reside [13]. In the original scheme, the voter is required to trust that the single election authority does not use all the values it has generated in order to determine how individual voters have voted, or perform other attacks such as electronic ballot box stuffing.

Figure 3 illustrates an alternative architecture for the distribution of information in the modified CESC scheme. The principle behind the design of the scheme is that responsibility for the generation of different components of the polling card is distributed to a number of independent domains. The domains proposed in the modified architecture are intended to correspond to roles present in existing the UK electoral infrastructure.

For example, an *Acting Returning Officer* domain is responsible for the collection of candidate information and generation of candidate identity numbers (CIDs). CID values were used to generate anonymous tallies in the original CESC scheme by the election authority. Each anonymous tally would then be matched with a candidate's name [13]. Similarly, the *Registration Officer* domain collects voter information and generates the VID values for delivery. In addition, the role of generating PCIN/RID credentials from CID values is separated from the task of delivering the credentials to a voter. Therefore association between credentials and candidate names is explicitly prevented in the election authority.

As a result of the modification, the voter receives their

polling card as three separate documents – no domain in the election authority is able to utilise the information it collects in order to violate the anonymity of the voter’s choice. Further, *intelligent* ballot box stuffing is prevented, since no single domain knows how a given VID/PCIN combination corresponds to a particular choice of candidate for a voter. The same architecture may also be employed in the collection and tallying of votes.

A flaw of the modified scheme is that should collaboration occur between domains of the election authority occur, then several election authority attacks evident in the original CESG scheme are re-introduced, intelligent ballot-box stuffing by the collaborating domains for example. Such a flaw is perhaps greater than in certain cryptographic schemes, where the vulnerability to collaboration may be stated as a security parameter (the number of authorities needed to collaborate, for example) rather than a static value (2) as is the case here. The modification may still be regarded as a substantial improvement over the original monolithic election authority, since independent domains, based on independent actors in the UK electoral infrastructure, are required to collaborate prior to an effective attack being mounted. In addition, as noted above, collaboration between certain domains to discover the association between votes and voters may be necessary in certain circumstances within the UK’s electoral context.

IV. FUTURE WORK: USABILITY TESTING

During the design of the modified CESG system two particular usability issues were raised:

- 1) *What error rate can be anticipated for voters entering long PIN/PCIN values to cast a vote?* An advantage of more powerful, polster based voting devices, such as internet connected PC computers, is that a richer user interface may be provided. Should accurately entering a long string of digits prove too difficult for voters, the convenience of the scheme (despite its mobility) may be undermined.
- 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 possibility of the election authority attempting to “cheat” the election must be considered.
- 3) *Will voters trust the modified system to protect their anonymity?* Whilst the fact that a vote has been counted is demonstrable, the fact that a vote is secret is not. Tests will be needed to determine whether voters are satisfied with the secrecy of their vote.

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.

V. CONCLUSIONS

This paper outlines the limitations imposed on remote electronic voting schemes, by requiring that voters employ a software polster. A polsterless REV scheme is described, which is intended for use in UK elections. The modified scheme provides improved architectural defense against violations of vote anonymity without resorting to cryptographic mechanisms. Further, the scheme provides both independent voter verifiability of votes and the ability to cast votes on a range of inter-networked electronic devices that lack cryptographic capabilities, in order to maximise the penetration of a voting system that implements the scheme in the UK population.

ACKNOWLEDGMENT

This work is funded by Microsoft Research, Cambridge.

REFERENCES

- [1] L. Pratchett, *The Implementation of Electronic Voting in the UK*. LGA Publications, 2002.
- [2] A. Riera, “Design of implementable solutions for large scale electronic voting schemes,” Ph.D. dissertation, Autonomous University of Barcelona, Bellaterra, Spain, December 1999.
- [3] Z. Rjašková, “Electronic voting schemes,” Master’s thesis, Comenius University, Bratislava, 2003.
- [4] Ö. Murk, “Designing electronic voting,” June 2001. [Online]. Available: citeseer.nj.nec.com/murk01designing.html
- [5] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, February 1981. [Online]. Available: <http://world.std.com/~franl/crypto/chaum-acm-1981.html>
- [6] 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.
- [7] A. Fujioka, T. Okamoto, and K. Ohta, “A practical secret voting scheme for large scale elections,” in *Advances in Cryptology - ASIACRYPT ’92, Workshop on the Theory and Application of Cryptographic Techniques*, ser. Lecture Notes in Computer Science, J. Seberry and Y. Zheng, Eds., vol. 718. Gold Coast, Queensland, Australia: Springer Verlag, December 1992, pp. 244–251.
- [8] L. Cranor and R. Cytron, “Sensus: A security-conscious electronic polling system for the internet,” in *Proceedings of the Hawai’i International Conference on System Sciences*. Wailea, Hawaii: IEEE Computer Society Press, January 1997.
- [9] R. Joaquim, A. Zuúquet, and P. Ferreira, “Revs – a robust electronic voting system,” *IADIS International Journal WWW/Internet*, vol. 1, no. 2, pp. 47–63, December 2003.
- [10] A. Hevia and M. A. Kiwi, “Electronic jury voting protocols,” in *Latin American Theoretical Informatics*, 2002, pp. 415–429. [Online]. Available: citeseer.nj.nec.com/307249.html
- [11] J.-H. Lee, “The big brother ballot,” *Operating Systems Review*, vol. 33, no. 3, pp. 19–25, 1999. [Online]. Available: citeseer.nj.nec.com/246655.html
- [12] D. Malkhi, O. Margo, and E. Pavlov, “E-voting without ‘cryptography,’” February 2003. [Online]. Available: citeseer.nj.nec.com/malkhi02evoting.html
- [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] N. B. Fairweather, “CESG report on evoting security - response of the centre for computing and social responsibility,” 2002. [Online]. Available: <http://www.ccsr.cms.dmu.ac.uk/resources/general/responses/ppera2000.pri%nt.html>
- [15] R. Mercuri, “Response to formal request for comment by the CESG (UK) on internet voting,” October 2002.
- [16] “Representation of the People Act,” 1983, ch. 2.
- [17] R. Blackburn, *The Electoral System in Britain*. 175 Fifth Avenue, New York N.Y. 10010: St. Martin’s Press, 1995.