

Gesellschaft für Informatik (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into the fields of

- Seminar
- Proceedings
- Dissertations
- Thematics

current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

ISSN 1617-5468

ISBN 978-3-88579-225-3

The 2008 Conference on Electronic Voting took place in Castel Hofen near Bregenz at the wonderful Lake Constance from 6th to 9th August.

This volume contains 17 papers selected for the presentation at the conference out of more than 30 submissions. To assure a scientific quality, the selection was based on a strict and anonymous double-blind review process.



Robert Krimmer, Rüdiger Grimm (Eds.): Electronic Voting 2008

GI-Edition

Lecture Notes in Informatics

Robert Krimmer, Rüdiger Grimm (Eds.)

3rd international Conference on **Electronic Voting 2008**

**Co-organized by Council of Europe,
Gesellschaft für Informatik and E-Voting.CC**

**August 6th- 9th, 2008
In Castle Hofen, Bregenz, Austria**

Simple and Secure Electronic Voting with Prêt à Voter

David Lundin

University of Surrey, Guildford, Surrey, UK
d.lundin@surrey.ac.uk

Abstract: Prêt à Voter is an electronic voting system with very high security properties. We aim to make the system truly usable and applicable in elections with many races and candidates by allowing the vote to be formed using a voting machine and by printing a minimalistic receipt. We also introduce the procedure/technology mix concept to describe the use of procedures, people and technology to secure electronic voting systems.

1 Introduction

Implementing Prêt à Voter as it is described in a series of papers [Rya05, CRS05, RP05, RP06a, RS06a, Rya07b, LTR+06a, LTR+06b, XSH+07, LR08] has an associated set of fairly hard problems not envisaged by the authors, such as reliable optical character recognition (OCR), multi-page ballot forms in elections where there are many candidates contending many different races, chain of custody issues relating to pre-printed ballot forms, key distribution problems relating to on-demand printed ballot forms, and so forth.

Anecdotal evidence suggests that politicians and civil servants, in Europe and perhaps around the world, are concerned with the accessibility and applicability of electronic voting systems to a higher degree and cutting-edge security technology to a lesser degree than seemingly realised by researchers in the electronic voting field. Consider, for example, the impossibility for a civil servant in a country in continental Europe where there may, for example, be 28 candidates in each of seven races contended on the same ballot form to implement Prêt à Voter 2005 or 2006—the ballot form is simply too large to be scanned.

Further, anecdotal evidence suggests that a major contributor to decisions to use electronic voting in Europe is to simplify the process. For example, when the City of Hamburg, Germany, changed its electoral law it almost became a necessity to use some form of electronic counting of the votes as this would take days and weeks to do by hand [VV06]. The decision was taken to implement a completely new system based on Anoto pens and although this system was very accessible and had some procedures to safeguard the accuracy of the election, it seems it lacked sufficient technical guarantees.

This paper proposes a configuration of the Prêt à Voter electronic voting system in its later guises with emphasis on usability, accessibility and simplicity. Due to limitations to the length of this paper it has been necessary to leave out some technical detail but references provide this detail where necessary.

2 Preliminaries

In this section we describe the properties of end-to-end verifiable systems and introduce the procedure/technology concept.

2.1 End-to-End Verifiability

The will to elect leaders and representatives stems from a mass of people, equal, who have organised and created states and institutions to serve the population. From this philosophical point of view, some may say that once leaders were first democratically elected, they created election authorities and thus these are trustworthy and able to run fair elections for the people. Others are more reluctant to place such trust with such authorities. Consider, for example, some of those states in the world today that wish to disguise an undemocratic rule by holding unfair general elections. The most effective weapon against this at the disposal of the world's truly democratic nations is election observation.

However, election observation is a very blunt instrument with tremendous organisational and budgetary requirements. Although essential, election observation can only function as an audit of the procedures in place to safeguard the election and it is impossible to know, or prove, that the audit is sufficiently complete to allow conclusions to be drawn about the secrecy and fairness of the election.

This suggests that it would be more beneficial, if possible, to audit the election as a whole rather than some subset of the procedures involved. The ability to audit the whole election and (perhaps mathematically) prove that the outcome is exactly as indicated by the voters on election day has been given the name end-to-end verifiability and there exist many systems aiming to do this [AR06, ABBD04, ACvdG07, BFP+01, BT94, Cha04, CRS05, CGS97, FCS06, FOO92, JCJ05, LBD+03, NA03, OMA+99, Pun, Riv06]. There may be other ways of achieving this but we consider end-to-end verifiability a combination of two other: *voter verifiability* and *public verifiability*.

Voter verifiability The voter is given a receipt which she can use to check after the close of the election that her vote has been included in the tally. In order for the system to be coercion resistant, the receipt must not reveal the vote.

Public verifiability Any interested person or organisation can, perhaps using software, check that all the encrypted receipts are properly decrypted into plain text votes and that these are tallied correctly.

2.2 The Procedure/Technology Mix

We confess that we would rather employ a technological solution to security issues in electronic voting systems than a procedural one, but here feel obliged to introduce the *procedure/technology mix*. This is simply the mix of technology, procedures and people that constitutes any electronic voting system.

In the previous section, we claimed that the use of end-to-end verifiability would render the auditing of procedures and people obsolete. This is certainly true regarding the correctness of the outcome of the election; it is simply possible to prove whether the reported outcome is correct or not and if not, find the source of the error.

However, the *secrecy* of the election is, of course, a kind of property that once leaked cannot be “proven” back to secrecy. Furthermore, end-to-end verifiability is unfortunately very hard to achieve with technology only. Consider, for example, a theoretical system, the accuracy and secrecy of which depends on each voting device having its own secret private key. The distribution of these keys is, in fact, a procedural solution to both the accuracy and secrecy problems!

It therefore seems logical that the secrecy of the election is safeguarded by some mix of technology and procedures and we advocate a use of procedures to increase the accessibility of the system where a technological solution would reduce it.

3 Simpler Prêt à Voter

3.1 Motivation

Our work with the first Prêt à Voter implementation and the subsequent demonstrations have resulted in the identification of two main problems impeding the progress toward the running of a general election:

1. *OCR*. The Optical Character Recognition (*OCR*) used in the first version of the system was not very robust and in order to interpret the marks as successfully as possible, it required the voter to use a seven segment display (like those you see in *LED* clocks) and a thick pen. Although all agreed that the success rate of the *OCR* can be increased, there was strong opposition from those with particular experience of implementing voting schemes against the seven segment display. It was felt that these were too cumbersome and hard to understand. We realise that this is not acceptable in a general election as such a voting system is used rarely by voters and this would introduce a large proportion of errors.

2. *Scanning*. The sheet-feed scanning of the ballot form is evidently very hard to use in elections where there are a number of races and/or a large number of candidates — election law may also stipulate that all races and candidates are printed on a single sheet, making this sheet immensely large. Furthermore, the layout of the ballot form would require that all candidates and their “boxes” were printed along the vertical axis of the paper, further limiting the number of races and candidates that can be printed on any piece of paper. Unfortunately, although that version of the Prêt à Voter implementation did support many concurrent different ballot forms, it did not support the spanning of a single race over more than one ballot form.

The motivation for this configuration of Prêt à Voter is thus simplicity, accessibility and the accommodation of a very large number of candidates. This introduces some procedural safeguards where technological safeguards have previously been envisaged [RS06b, Rya07b]. We argue that this is not only necessary but that it is so important to include as many voters and introduce as few errors as possible in the voting process, and that the procedure/technology mix must be adjusted.

3.2 The Voting Ceremony

In the polling station there are a certain number of voting machines placed in voting booths. The secrecy of the election is based on these voting booths providing proper privacy to the voter and the voting machine similarly being unable to leak the intention of the voter. Thus, there are poll station workers and guards keeping the area under surveillance in order to ensure that the machines cannot be tampered with.³²

The voter is able to enter the polling station without first identifying herself to the poll station staff and she can enter a voting booth so as to interact with the voting machine. It is important that she not be required to identify herself before she can interact with the machine because this makes it harder for the poll station staff or machine to connect the will expressed in the interaction with the machine to a particular voter.

The main purpose of the voting machine is to help the voter express her will in the election, the difficulty of which depends on the election system in place and the abilities of the voter. As the voter is interacting with a computer to make her choices, the accessibility of the system is in itself an important area of research. It thus serves little use to go further into the details of how the voter interacts with the system to indicate her choices and it is sufficient to say that she may do so using her sight, touch and/or hearing and a touch screen, mouse, voice or other input device(s). At the end of the interaction the voting machine prints a vote in plain text (see Section 4.4) which the voter takes away and casts.

³² Note that the accuracy is not threatened by this leak of information: but the privacy of the election is.

Interacting with the machine in the voting booth, the voter is able to produce some maximum number of votes. This must be a number greater than one so that the voter is able to create one vote that correctly captures her intention and some number of other votes that she can choose to audit, see below. The voting machine does not, therefore, know whether a vote it helps to construct will be audited or if it will be cast. It should therefore be disinclined to cheat (or malfunction) because there is some likelihood that it will be found out and taken out of commission. In order to stop voters from occupying voting booths too long and thus stopping others from voting, election law may stipulate some maximum number of votes, such as five or ten, which would be quite sufficient for the purpose.

When the receipt is printed by the machine, the voter can read it through and ensure that it is the vote she indicated to the machine. She turns the vote she is going to cast into an encrypted receipt (see below). Any or all of the other votes she may have created she is able to have audited by approaching an auditing desk. The barcodes on these ballot forms are scanned in by poll station workers and the forms are decrypted and the information printed. The voter is now able to check that the printed information does correspond to the vote she has just audited, indicating this vote was correctly formed. If so, she will grow more confident that the vote she will submit is also correctly formed.

Finally, the voter approaches a submission desk with the encrypted receipt she wishes to submit. She identifies herself to poll station workers and the barcode on the encrypted receipt is scanned and the contents of it are electronically submitted to a central repository (and may be noted next to the name of the voter who has cast it). Note that no submitted data need be kept secret to safeguard the secrecy of the election; it is already encrypted. After the close of the election, this, and all other encrypted receipts, will be decrypted as described in Section 4.7. A stamp is placed on the encrypted receipt by officials, indicating it has been submitted.

The voter can now leave the poll station with her encrypted receipt, and after the close of the election she can use a website to check for the inclusion of her vote in the tally. She does this by entering the serial number of her encrypted receipt and comparing the image of the receipt served by the website with the actual receipt. If the marks on these match exactly she can be confident that her vote is included in the tally.

4 Technical Foundation

4.1 Coping with Single Transferable Vote

In order to support Single Transferable Vote (STV) [Wik07, Soc07] and other schemes where the voter expresses a ranking or awards votes to more than one candidate, we employ the multiple-onion approach introduced by [Hea07]. We provide an overview of the scheme here.

A numerical representation of a candidate is encrypted under a probabilistic threshold public key cryptography scheme. There are many different such encryptions for each candidate and as these are encrypted under a probabilistic scheme they do not look alike. We call these encryptions onions. A set of onions are associated with each ballot form and the voter's choices, as expressed on the ballot form, are translated into an ordering of these onions. If the voter wishes to cast a vote for the candidates in the order C, E, A, D, B then this is encoded by ordering the constituent onions thus:

$$O_C;O_E;O_A;O_D;O_B;O_{\text{stop}}$$

Note that these are encryptions and which candidate they represent is therefore hidden. The stop onion O_{stop} is used to ensure that the length of the vote is not dependent on the number of choices expressed by the voter. A vote only for candidate C, for example, is thus constituted by an onion O_C , the stop onion, and thereafter all other onions in a random order:

$$O_C;O_{\text{stop}};O_A;O_E;O_D;O_B$$

After the close of the election, the first constituent onion of each cast vote is decrypted and the vote given to the indicated candidate. This initiates the applicable STV protocol, which removes candidates and redistributes the votes according to the next choice in order in a number of rounds until the required number of candidates has been elected. Each time the vote is redistributed the next choice is decrypted. In our example, the first candidate is decrypted thus:

$$C;O_E;O_A;O_D;O_B;O_{\text{stop}}$$

If candidate C is subsequently eliminated and his or her votes redistributed, the onion representing candidate C is appended, the plaintext representation of C removed and the next onion decrypted, thus:

$$E;O_A;O_D;O_B;O_{\text{stop}};O_C$$

This is now a vote for E. When a decryption reveals the stop onion, the vote is removed from further redistributions. Each redistribution round contains a re-encryption shuffle so as to hide the ordering of the candidates in the vote; please see [Hea07] for details. This configuration thus limits the impact of an attack popularly called the Italian attack [Hea07] where the ordering of the candidates carries some message to a coercer.

4.2 Pre-Creation of Onions

A source of potential threats to the secrecy of the election pointed out in early papers describing end-to-end verifiable systems [Rya05, BR03, RP05, KSW05, RP06a, RS06a, RP06b, Rya06, Rya07a] was that the voting machine must select random values and errors or predictability in the pseudo-random number generator may render the cryptography useless. Furthermore, the voting machine might use “random” values from a list shared with a culprit or values such that a hash thereof would signal to a culprit the contents of the vote and/or the identity of the voter. To remove this problem, we do not require the machine to select the randomness used in creating the candidate list but employ the distributed pre-creation technique detailed in [RS06a].

4.3 Touch Screen Interface

To accommodate for elections with many races and/or races with many candidates, the proposed configuration of Prêt à Voter has two major differences to previous versions: (a) the receipt is created by a voting machine and (b) the receipt is printed in the *minimal* form presented in the next section.

4.3.1 Creating a Vote with the Machine

This is an example of a possible interaction with the voting machine. The steps involved can be different in appearance, order and number and are adapted to the election. Approaching an idle voting machine, the voter is greeted with a message asking her to touch the screen to initiate the voting process.

Springfield Local Election Tap screen to start

A list of races is shown with indicators to whether or not a vote has been created in each race. The voter selects a race by tapping the screen³³.

Select race	
Mayor	Not voted
Sanitation Commissioner	Not voted

A list of the candidates in the selected race is shown and the voter is able to tap a single candidate or a number of candidates in the preferred order. A “Clear” button is available on the screen, which clears all choices made and allows the voter to start over. A “Proceed” button allows the voter to return to the list of races.

³³ Or using some other input method, depending on the abilities of the voter.

Vote for Sanitation Commissioner	
Shmoikel Krusotsky Apu Nahasapeemapetilon Ray Patterson Homer Simpson	

Selecting her favourite candidate, the voter completes the vote for the race and clicks the “Proceed” button to return to the race selection screen.

Select Race	
Mayor Sanitation Commissioner	Not Voted Voted

The voter is able to return to any race and re-create her vote. A “Proceed” button on the race selection screen allows her to go to a summary screen. Here the voter can select either of two buttons: “Go back” or “Print vote”.

Summary of your vote	
Mayor Sanitation Commissioner	Not voted Homer Simpson

When the voter is finished and presses the “Print vote” button, the machine displays a final message whilst printing the vote.

Thank you Please take your printed vote
--

4.4 The Minimalistic Encrypted Receipt

The purpose of the minimalistic encrypted receipt is to enable the printing of many races on the same receipt and to aid the voter in checking the receipt on the web bulletin board. To achieve this we wish to print as few candidates as possible on the vote. We first introduce the traditional Prêt à Voter ballot form and its associated encrypted receipt before showing the alterations we propose to these.

4.4.1 The Prêt à Voter Ballot Form and Encrypted Receipt

The ballot form in Prêt à Voter consists of two columns: in the left the candidates are printed in a random order (based on randomness unique for the form) and in the right the voter makes her marks in a grid corresponding to the candidates in the left column. For example:

Ballot form	
Sanitation Commissioner	
Homer Simpson	
STOP	
Apu Nahasapeemaptelon	
Ray Patterson	
Smoikel Krustofsky	
	lk3j92784

If a voter makes her marks in the right hand side grid and then detaches and destroys the left hand column, the remaining encrypted receipt does not reveal her vote. However, a value called the onion, printed at the bottom of the grid, can be decrypted to reveal the vote. In this example an encrypted receipt may be:

2
3
1
lk3j92784

It has been envisaged that the Prêt à Voter is a single page, which contains all races in the election and all the candidates in each of those races. The voter makes her mark on the paper and detaches and destroys half, producing an encrypted receipt which is subsequently scanned and then handled electronically. It is quite clear that in an election with many races and many candidates, it is not possible to print all on one piece of paper that can also be fed through a scanner after the marks have been made by the voter.

4.4.2 The Minimalistic Encrypted Receipt

The traditional Prêt à Voter ballot form is printed onto paper before the election (or on demand before they are used [RS06a, LR08]) and as the voter uses a pen to fill out her choices, naturally all candidates must be available on the ballot form. In the scheme presented here a computer is used to create the vote after which the ballot form is printed. Therefore, it is possible to print only the candidate(s) that the voter has indicated a vote for. In our example, when the voter makes her marks using the touch screen she may indicate her choices thus (note that the candidates are listed in the alphabetical order on the screen):

Vote for Sanitation Commisioner	
Shmoikel Krustofsky	
Apu	
Nahasapeemapetilon	
Ray Patterson	1
Homer Simpson	2

When the voter presses the “Print receipt” button the voting machine retrieves the necessary onions and decrypts these (see above) to find the ordering of the candidates. Let us assume in our example that the machine retrieves the onions with serial number 27344, decrypts these and finds that the candidate list has the following order:

27344
Homer Simpson STOP Apu Nahasapeemapetilon Ray Patterson Shmoikel Krustofsky

The machine now prints the following filled-out Prêt à Voter ballot form, note that only the candidates which the voter has indicated are printed and that these are printed in the order dictated by the onions:

Ballot form	
Sanitation Commissioner	
Homer Simpson	2
STOP	3
Ray Patterson	1
	1,2,4 27344

In this example we are only able to avoid printing two candidates, but in a race with many more candidates the same number of choices made by the voter would drastically reduce the number of candidates that must be printed. The index numbers 1; 2; 4 of the candidates printed are displayed at the bottom right together with the serial number 27344. These values can be printed in the form of a barcode (see below) which allows them to be read in quickly. Note that these numbers together with the choices indicated above by the voter is all that is needed to represent the vote. The voter now checks that the printed vote is truly a representation of her intended vote. If it is not she can discard the vote (by shredding it for example) and produce another. If she is happy with the vote and wishes to cast it, she detaches the two columns from each other and destroys the left hand one. What remains is an encrypted receipt:

2
3
1
1,2,4 27344

The voter approaches a desk manned by poll station staff, identifies herself and allows the barcode on the encrypted receipt to be scanned. When poll station staff are satisfied that the barcode has been scanned and electronically transmitted to the web bulletin board they stamp the encrypted receipt with an official stamp so as to indicate that it is the receipt of a vote that has been cast in the election. A mark is placed in the register to indicate that this voter has cast her vote³⁴. All votes submitted in this way are collected on the web bulletin board.

4.4.3 The Barcode

All previous versions of Prêt à Voter has required an encrypted receipt to be scanned in and interpreted to form a digital representation that could subsequently be decrypted. This OCR process has been shown to be a significant weakness to the scheme: it results in many errors³⁵.

In this scheme we reduce the amount of work in the scanning process to the recognition of a barcode. These are printed in such a way as to be simple to read and recognise and they can contain check numbers etc to aid the correct interpretation of them. In order to record a vote the system must read the following information from the encrypted receipt:

³⁴ In some constituencies, such as the United Kingdom, the law requires that the ballot form serial number is noted against the name of the voter: that is quite possible to do in this scheme.

³⁵ Note that these errors did not mean that a vote was cast for a different candidate than indicated by the voter—but that the vote had to fill out another ballot form as the first could not be correctly understood by the system.

1. The serial number (27344)
2. Which candidates are shown on the ballot form (1; 2; 4)
3. The marks made by the voter (2; 3; 1)

To enter this information into the barcode, we simply concatenate them:

27344|1; 2; 4|2; 3; 1

When this information is scanned by poll station staff it is submitted to the web bulletin board. Here the appropriate constituent onions are retrieved:

27344
<input type="radio"/> _{RSimpson} <input type="radio"/> _{RSTOP} <input type="radio"/> _{RNahasapeemepetilon} <input type="radio"/> _{RPatterson} <input type="radio"/> _{RKrustofsky}

The appropriate onions are selected (numbers 1, 2 and 4 in our example) and re-ordered in the correct order as indicated by the choices (2, 3 and 1) — thus the onions are placed in the following order:

27344
<input type="radio"/> _{RPatterson} <input type="radio"/> _{RSimpson} <input type="radio"/> _{RSTOP}

Note that of course the contents of these onions are unknown! Therefore, the system now holds an encrypted vote submitted by this voter.

4.5 Auditing a Vote

We here argue that it is safe to allow a voter to use a voting machine to create the vote, because she may create any number of votes and audit some of these. If the voting machine attempts to cheat, it cannot be sure that the vote will not be audited and its cheating thus found out. A malfunctioning machine will thus be found with a high probability and taken out of commission.

The first audit that a voter makes out of a vote printed by the voting machine is simply to read it. If the machine has committed an error (or something worse) then the marks printed would not match the intention of the voter. If this is the case, she can simply destroy the vote and create another one — until she receives one that correctly indicates the vote she wishes to cast. Note that the voter may have performed some “human” error while interacting with the machine and not spotted this until the vote has been printed: this gives her another chance to spot such a mistake and to rectify it.

The second audit of the ballot form that can be performed on any vote is the checking of the barcode. This is simply done by the voter allowing the barcode to be scanned by a machine available in the polling station, which shows the contents of the barcode in a human readable form. Such machines can also be supplied by independent organisations — or run as a small piece of software on the voter’s camera-enabled mobile phone. The voter then simply checks that the information shown by the reader corresponds to the information printed in the right column of her vote.

Finally, if the voter decides to audit a created vote then the constituent onions shall be retrieved from the web bulletin board (where they are marked as audited, ensuring that no vote can subsequently be cast with these onions) and decrypted by the tellers. The full candidate list is then displayed to the voter who compares it to the printed vote.

The purpose of this audit is first to find any machine that may malfunction or that has been compromised. Secondly, the audit functions to convince voters that the system is working correctly and that the vote will be decrypted correctly.

4.6 Checking the Receipt

The voter is allowed to take home the scanned and stamped encrypted receipt. She can then, at any time, visit the web bulletin board on the web and search for the serial number printed on the receipt. When she calls up her receipt she should see an exact replica of the receipt she holds in her hands. If this is the case then the voter can be certain that her vote has been included in the final tally. If the receipt is not found on the web bulletin board or if the version she finds there does not match the one she has in her hand, she can accuse those in charge of running the election of malfunction or fraud and she has proof in her receipt that she has cast a vote which is now missing or has been changed.

4.7 Decryption and Tallying

At this stage the web bulletin board contains a list of all encrypted votes that have been cast, in the form of a number of ordered onions. We are unable to describe the decryption here because of limitations to the length of this paper but a detailed specification is available in [Hea07].

4.8 Note on Securing the Machine using Procedures

It is important to note that the accuracy of the election, that is to say, the trustworthiness of the outcome of the election, is safeguarded not by procedures but by the cryptographic properties of the system. The result of the election is thus as trustworthy as in previous configurations of Prêt à Voter [CRS05, RS06a], because they all rely on the same verifiability.

5 Discussion

The main advantages of the proposed scheme is that the voting machine is able to guide the voter through a potentially very complex voting procedure involving any number of races and any number of candidates in those races. The voter turns the plain text vote into an encrypted receipt and the scanning of this receipt is very fast because only a barcode has to be scanned. The main disadvantage to this configuration of Prêt à Voter is that the voting machine must learn the voter's intention in order to produce the printed vote. The secrecy of the election is thus safeguarded simply by procedures that ensure that the machine does not leak any information. As discussed in the introductory sections of this paper, there is a necessity to alter the procedure/technology mix so that it is possible to make the system more accessible and remove a large proportion of the errors associated with the filling out of the ballot form.

5.1 Acknowledgements

Thanks to the anonymous EVOTE08 reviewers for their feedback. Thanks also to Peter Ryan, Steve Schneider, James Heather, Roger Peel, Zhe Xia, Kieran Leech, Roberto Araújo and Jacques Traore, who listened to a presentation of initial ideas.

References

- [ABBD04] R. Aditya, Lee B, C. Boyd, and E. Dawson. An efficient mixnet-based voting scheme providing receipt-freeness. Proceedings of TrustBus'04, pages 152–161, 2004. LNCS 3184.
- [ACvdG07] Roberto Araujo, Ricardo Filipe Custodio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel. Proceedings of Workshop On Trustworthy Elections (WOTE 2007), 2007.
- [AR06] B. Adida and R. Rivest. Scratch & Vote: self-contained paper-based cryptographic voting. Proceedings of the fifth ACM workshop on Privacy in electronic society, pages 29–40, 2006.
- [BFP+01] O. Baudron, P.-A. Fouque, D. Pointcheval, J. Stern, and G. Poupard. Practical multicandidate election system. Proceedings of the twentieth ACM Symposium on Principles of Distributed Computing (PODC'01), pages 274–283, 2001.
- [BR03] J. Bryans and P. Y. A. Ryan. A Dependability Analysis of the Chaum Digital Voting Scheme. Technical Report, University of Newcastle, CS-TR:809, 2003.

- [BT94] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections (extended abstract). Proceedings of the twenty-sixth Symposium on Theory of Computing (STOC'94), pages 544–553, 1994.
- [CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multiauthority election scheme. Advances of Eurocrypt'97, pages 103–118, 1997. LNCS 1233.
- [Cha04] D. Chaum. Secret ballot receipts: true voter-verifiable elections. IEEE: Security and Privacy Magazine, 2(1):38–47, 2004.
- [CRS05] D. Chaum, P. Y. A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. Proceedings of the tenth European Symposium on Research in Computer Science (ESORICS'05), pages 118–139, 2005. LNCS 3679.
- [FCS06] K. Fisher, R. Carback, and T. Sherman. Punchscan: Introduction and System Definition of a High-Integrity Election System. In PRE-PROCEEDINGS, pages 19 – 29. IAVoSS Workshop On Trustworthy Elections, 2006.
- [FOO92] A. Fujioka, T. Okamoto, and K. Ohta. A Practical Secret Voting Scheme for Large Scale Elections. Advances of Auscrypt'92, pages 244–251, 1992. LNCS 718.
- [Hea07] J. Heather. Implementing STV securely in Prêt à Voter. 20th IEEE Computer Security Foundations Symposium (CSF'07), pages 157–169, 2007.
- [JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pages 61–70, 2005.
- [KSW05] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: a systems perspective. Proceeding of USENIX Security Symposium, pages 186–200, 2005. LNCS 3444.
- [LBD+03] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. Proceedings of ICISC'03, pages 245–258, 2003. LNCS 2971.
- [LR08] D. Lundin and P. Y. A. Ryan. Human readable paper verification of Prêt à Voter. Technical Report at the University of Surrey, CS-08-03, 2008.
- [LTR+06a] D. Lundin, H. Treharne, P. Y. A. Ryan, S. Schneider, and J. Heather. Distributed creation of the ballot form in Prêt à Voter using an element of visual encryption. Proceedings of Workshop On Trustworthy Elections (WOTE 2006), pages 119–125, 2006.
- [LTR+06b] D. Lundin, H. Treharne, P. Y. A. Ryan, S. Schneider, J. Heather, and Z. Xia. Tear and destroy: chain voting and destruction problems shared by Prêt à Voter and Punch-Scan and a solution using visual encryption. Proceedings of Workshop on Frontiers in Electronic Elections (FEE 2006), 2006.
- [NA03] C. A. Neff and J. Adler. Verifiable e-voting: indisputable electronic elections at polling places. VoteHere Inc, 2003.
- [OMA+99] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. Information Security'99, pages 225–234, 1999. LNCS 1729.
- [Pun] Punchscan. <http://www.punchscan.org>.
- [Riv06] R. Rivest. The ThreeBallot voting system, 2006. <http://crypto.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf>.
- [RP05] P. Y. A. Ryan and T. Peacock. Prêt à Voter: a system perspective. Technical Report of University of Newcastle, CS-TR:929, 2005.
- [RP06a] P. Y. A. Ryan and T. Peacock. Putting the human back in voting protocols. Technical Report of University of Newcastle, CS-TR:972, 2006.
- [RP06b] P. Y. A. Ryan and T. Peacock. Threat analysis of cryptographic election schemes. Technical Report of University of Newcastle, CS-TR:971, 2006.

- [RS06a] P. Y. A. Ryan and S. Schneider. Prêt à Voter with re-encryption mixes. Proceedings of ESORICS, 2006. LNCS.
- [RS06b] P. Y. A. Ryan and S. Schneider. Prêt à Voter with re-encryption mixes. Technical Report of University of Newcastle, CS-TR:956, 2006.
- [Rya05] P. Y. A. Ryan. A variant of the Chaum voter-verifiable scheme. Proceedings of the 2005 Workshop on Issues in the Theory of Security, pages 81–88, 2005.
- [Rya06] P. Y. A. Ryan. Verified encrypted paper audit trails. Technical Report of University of Newcastle, CS-TR:966, June 2006.
- [Rya07a] P. Y. A. Ryan. The computer ate my vote. Technical Report of University of Newcastle, CS-TR:988, 2007.
- [Rya07b] P. Y. A. Ryan. Prêt à Voter with Paillier Encryption. Technical Report of University of Newcastle, CS-TR:1014, 2007.
- [Soc07] Electoral Reform Society. 2007. <http://www.electoral-reform.org.uk/>.
- [VV06] M. Volkamer and R. Vogt. New Generation of Voting Machines in Germany — The Hamburg Way to Verify Correctness. In PRE-PROCEEDINGS, Hamburg, Germany, 2006. Frontiers of Electronic Elections (FEE 2006).
- [Wik07] Wikipedia. Single transferable vote, 2007. [http://en.wikipedia.org/wiki/Single transferable vote](http://en.wikipedia.org/wiki/Single_transferable_vote).
- [XSH+07] Z. Xia, S. Schneider, J. Heather, P. Y. A. Ryan, D. Lundin, R. Peel, , and P. Howard. Prêt à Voter: all in one. Proceedings of Workshop On Trustworthy Elections (WOTE 2007), 2007.