

Prêt à Voter: a Systems Perspective

Peter Y. A. Ryan and Thea Peacock

September 20, 2005

Abstract

Numerous cryptographic voting schemes have been proposed in recent years. Many of these have highly desirable formal security properties. However, as with all security systems, even a well-designed technical system can be undermined by implementation details or environmental factors, typically including human users, that violate (often implicit) assumptions of the design and evaluation.

In ‘Cryptographic Voting Protocols: a System Perspective’ [11] Karlof et al perform a systems-based analysis of the Chaum [5] and Neff [17], [18], [19] schemes. They identify a number of vulnerabilities and discuss possible mitigations and counter-measures.

In this paper, we examine the extent to which these vulnerabilities carry over to the Prêt à Voter scheme [6]. In addition, we describe some further systems-based vulnerabilities not identified in [11]. We also discuss some further threats, such as chain voting attacks, which do not apply to the Chaum or Neff schemes but to which Prêt à Voter is vulnerable, unless appropriate countermeasures are deployed.

It turns out that Prêt à Voter is remarkably robust to most of the vulnerabilities described in [11] and here.

1 Introduction

Numerous cryptographic voting schemes have been proposed in recent years. Many of these offer highly desirable security properties: publically verifiable accuracy along with ballot secrecy and minimal dependence on components. However, as with all security systems, even well-designed technical systems can be undermined by poor implementation details or by unanticipated characteristics of the environment.

Voting systems are the bedrock of democratic societies, and date back several millennia. While many different mechanisms for voting exist [10], they all share a similar set of goals. These include [13], [7]:

- Ballot secrecy: only the voter should know how she voted.
- Legitimacy: only registered voters may vote, and only once.

- Individual verifiability: the voter should be able to check that her vote is accurately recorded for tabulation.
- Universal verifiability: the final tally should be verifiable by any third party.
- Accuracy: the final tally should reflect the true count of all legitimate, cast votes.
- Coercion resistance: a coercer should not be able to determine how a voter cast their vote, even with the co-operation of the voter. Put differently, the voter should not be able to prove how she voted to a third party.

It is often the case, however, that a particular voting system may only satisfy these requirements to a certain extent. In others, one or more requirements may not be satisfied at all. It is also possible that in certain contexts some of these requirements are not necessary, for example, secrecy is often not required in parliamentary referenda.

In an attempt to improve efficiency and accessibility of the election process, governments have invested in various automated voting systems that increase speed and accuracy of ballot counting. Arguably, some of these new mechanisms offer greater secrecy, and in the case of remote systems, increased voter participation. However, these attempts have been fraught with problems, many of which are due to reliance on computer hardware and software performing as intended. (See for example [3], [1], [12], [14]).

Recent proposals for cryptographic voting systems promise to resolve some of these problems by introducing transparency in the voting process, i.e. the protocols can be verified at intermediate points. Notable examples are the FOO [7], Chaum and Neff schemes and Prêt à Voter [6]. These strive to provide assurance of secrecy and accuracy without any reliance on the underlying technical system. Rather, the assurance is derived from a high degree of transparency in the vote recording and counting stages.

While it is important to analyse the core protocol in order to assess its security [4], [13], it is also essential to consider its interaction with the surrounding system, e.g. computer hardware and software, voters and voting officials, that previously undetected weaknesses may become apparent. Collusion between parties can make the attacks more difficult to detect and resolve. In the case of the Chaum scheme, this was argued in [21]. More recently, in their exemplary paper [11], Karlof et al have demonstrated this by taking the systems perspective in their examination of the Chaum and Neff schemes.

In this paper, we analyse Prêt à Voter from the systems perspective, and in doing so, find that it is remarkably robust to most of the vulnerabilities described in [11]. In addition, we identify some further vulnerabilities not mentioned in [11], and offer mitigation strategies, particularly where they may apply to Prêt à Voter.

The structure of the paper is as follows. In Section 2 we briefly describe the Chaum and Neff schemes. In Section 3, we recall the possible weaknesses identified in [11]. In Section 4, we present an outline of the Prêt à Voter scheme. Section 5 examines whether the attacks of [11] also apply to Prêt à Voter scheme. Following this, in Section 6, we identify further possible attacks and suggest mitigations. In Section 7 some other vulnerabilities of Prêt à Voter are described, along with some novel countermeasures. Finally, we summarise and conclude in Section 8.

2 The Chaum and Neff Voting Schemes

Due to space constraints we cannot go into details of the Chaum and Neff schemes here. However, for completeness and ease of understanding, we summarise their key features and refer the reader to [6], [4], [18], [19], or to [11], for accessible descriptions of both schemes.

We assume that an authority has undertaken the pre-election set-up, for example, generating and certifying public keys as appropriate. Once authenticated at a polling station, the voter engages in the first stage of casting a vote: receipt preparation. This takes place in a booth and involves participation in a cryptographic protocol with a machine, referred to in [11] as a *direct recording device* (DRE), during which the voter’s choice is encoded in a receipt produced by the DRE. The voter is given the opportunity, in the booth, of verifying that their vote is correctly encoded in the receipt, after which the receipt is posted to a *Web bulletin board* (WBB), together with an identifier generated by the DRE, which is called the *Ballot Sequence Number* (BSN) in [11]. The voter retains a copy of their encrypted ballot receipt, which they can subsequently check on a WBB to make sure that the receipt has been posted correctly.

The BSNs are then stripped off, and the receipts are shuffled and decrypted in a series of anonymising mixes to ensure that no link remains between the encrypted ballot receipts and final decrypted vote values. The results of each stage of the mix process are posted to the WBB. Intermediate stages of the mix can be subjected to random, partial auditing to detect any attempted fraud during the mix/decryption process.

Aside from the details of cryptographic primitives involved and the way that the anonymising mixes are performed and verified, the essential difference between the two schemes is in the format of the receipt. Both schemes employ cut and choose style protocols to allow the voter to detect attempts by the vote recording devices to incorrectly encode their selection in the receipt.

In the Neff scheme, the receipt consists of a matrix of *ballot mark pairs* (BMPs), which are El Gamal ciphertexts of the digits ‘0’ or ‘1’. Each row of the matrix corresponds to a candidate, and in the case of a chosen candidate, the BMPs encode either ‘00’ or ‘11’. In the unchosen candidate rows, either ‘01’ or ‘10’.

To verify the receipt, the DRE issues a pledge bit, p , and the voter, a challenge, c_i , for the chosen candidate. The DRE ‘opens’ each BMP in row, i , of

the matrix, by decrypting either the left or right BMP according c_i , and the voter checks that it matches p . The process is repeated for each row, the DRE opening the BMPs according to some random challenge. To prevent coercion, the voter can optionally issue challenges for the unchosen rows.

In the Chaum scheme, the voter's choice is represented using visual cryptography [16] to generate a ballot image. The image is split between two encrypted layers, each of which, viewed separately, comprises random pixel patterns. The image can only be reconstructed by correctly superimposing the two layers. The voter selects either the top or bottom layer to retain as a receipt, so without knowledge of the encryption, the receipt does not reveal the voter's choice.

The DRE also prints other information on the transparent layers, in particular the two *dolls*, D_l, D_b , which carry details on how to decrypt, respectively, the top or bottom layers. The details are encoded by successive encryptions, each one with the public keys corresponding to a single stage of the mix.

Outside the booth, the voter can perform well-formedness checks on her receipt, which serves to deter any attempt by the device to cheat by incorrectly encoding the voter's selection in the receipt.

In both schemes, although anyone can verify that the final tally accurately reflects the votes cast, the voter cannot directly check to what vote value her receipt has been decrypted. This is essential in order to avoid the possibility of coercion or vote buying.

3 Cryptographic Voting Protocols: Chinks in the Armour

The attacks considered in [11] essentially fall into four main categories: those due to subliminal channels, human unreliability in cryptographic protocols, denial of service and implementation of the system itself. In this section, we briefly recall each of these vulnerabilities and how they may apply to the Chaum and Neff schemes.

3.1 Subliminal Channels

Subliminal channels can arise if the DRE is able to produce alternative valid encryptions so as to communicate alternative or extra bits of information that can be used in subversive ways. Public viewing of the WBB makes this a viable threat. There are two ways in which subliminal channels may be introduced. They are described as follows.

The Neff scheme makes use of randomised cryptographic primitives, e.g., El Gamal, in the creation of the ballot receipt. This opens up the possibility of a subliminal channel: by judicious selection of random values, extra information could be encoded in the encrypted receipt [11]. Any agent with knowledge of the strategy, possibly in collusion with a malicious DRE, could then gather this information by observing the posted receipts.

The Chaum scheme, on the other hand, does not use randomised encryption but rather deterministic algorithms such as RSA. Randomised subliminal channels therefore do not arise. However, the Chaum scheme is potentially vulnerable to *semantic* subliminal channels, which can occur if alternative representations of the ballot image are valid. The DRE could then subtly alter representation of the voter’s selection in the ballot image in such a way as to convey certain information.

Note that in the Neff scheme, the subliminal information is encoded in variations in the ciphertext. Thus the potential channel would presumably be used to leak information about the vote value before the receipts are sent through the mix process. In the Chaum scheme, the channel results from the variations in plaintext of the decrypted receipt that emerges from the mix. Such a channel would therefore presumably be used to leak information about the voter identity.

3.1.1 Mitigation

Countermeasures for random subliminal channels are tricky, since the randomness may be essential for security properties. Karlof et al suggest that the same properties could be achieved using zero-knowledge proofs, but point out that most ZKP schemes also require randomness [11].

Another possibility is to pre-determine the randomness [11], i.e., the random bits are generated ahead of time and the DREs are required to use this entropy rather than any fresh entropy generated at run time. The difficulty here is that it then has to be ensured that this randomness is actually used, i.e., it must be verified that the DRE has to be monitored or suitably constrained to ensure that it does not depart from this pre-determined entropy.

The Chaum scheme can be implemented so as to be fully deterministic. Chaum suggests that the BSNs be sequential. The cryptographic seed material is then generated deterministically from the BSNs using the DRE’s signature. The validity of these signatures is randomly checked, at least on the layer chosen by the voter for retention. Thus the DRE’s adherence to this requirement is (partially) randomly verifiable. All postings to the WBB can be required to be in numerical order. Thus, the shuffles applied by the tellers during the mix stages are pseudo-random and deterministic. Note that the teller’s adherence to this requirement is fully and universally verifiable.

The Chaum scheme uses *randomised partial checking* (RPC) [9] for auditing the decryptions performed during mix. Each teller involved in the mix-net reveals only a proportion of input-output links, which are then checked to verify the decryptions. The selection of links to be opened for audit is constrained to ensure that no complete links can be traced through the net. Tellers should not know in advance which links to reveal, otherwise there is opportunity for undetected vote-altering.

The selection of links for audit can in fact also be made deterministic by applying suitable cryptographic functions to the data posted, see [9]. This is not so much to counter the possibility of a subliminal channel, the auditors

presumably do not have any voter privacy information to leak, but rather to counter any possible collusion between the tellers and the auditors. Such collusion might allow a teller to know in advance that it will not be asked to reveal certain links and so would be able to corrupt those links with impunity.

There may still be possibilities for subliminal channels. For example, the assignment of BSNs, and this should be monitored with care.

Karlof et al [11] suggest trusted hardware as another possible mitigation against subliminal channels, for example, to enforce the DRE’s conformance with pre-determined entropy. This, however, as they note, is unsatisfactory, as the hardware and the software being used need verification and monitoring to detect any tampering. Furthermore, the idea is contrary to the principle of transparency and minimal dependence which the Chaum, Neff and Prêt à Voter (see later) schemes aim to achieve.

Semantic subliminal channels could be mitigated by establishing official unambiguous ballot representations [11], e.g. the font to be used for the ballot image, the positioning of the image etc. Similar to the case of pre-determined randomness, the ballots would need to be checked for conformance to these rules.

The above discussion bears an interesting relationship to the definition of non-interference based on low determinism [20], i.e., the low user’s observations are made completely deterministic so as to eliminate the possibility of any covert channels due to high-level resolution of non-determinism visible to low.

3.2 Voter Participation in Cryptographic Protocols

Both the Chaum and Neff schemes require quite complex multi-step interactions between the voter and the DRE. The sequence of steps is often highly significant, e.g. in the Chaum scheme it is essential that the DRE commits to the dolls before it knows which layer the voter will choose to retain. Similarly, in the Neff scheme the DRE should not know in advance whether the voter will choose a ‘basic’ or ‘detailed’ receipt. A ‘detailed’ receipt has some BMPs opened as described in Section 2. This is to prevent a malicious DRE constructing receipts that do not encode the voter’s true intention. In other words, it is essential that a cut and choose, and not a choose and cut protocol is executed.

In [11], there are several examples which illustrate how, by re-ordering the steps in the protocol, or introducing extra ones, the DRE could learn in advance which layer or type of receipt the voter will select. Voters may not notice or appreciate the significance of such changes in the protocol execution.

In the same vein, the DRE could feign an error and re-boot after it learns the voter’s choice. Relying on the voter making the same choice in the second round of the protocol, the DRE then constructs a receipt for a different candidate. If the voter changes her mind, the DRE re-boots again to avoid detection [11].

Another possible vulnerability of the Chaum scheme, not identified in [11] but mentioned in [21], is as follows. The DRE attempts to corrupt the vote value by incorrectly constructing one of the layers. If the voter chooses the other layer for retention, checking this will go undetected. However, if the voter

chooses the corrupted layer, the DRE could try to fool the voter by printing ‘destroy’ instead of ‘retain’ on the layer that the voter chose as the receipt. If the voter fails to notice this, or simply ignores it, the corruption will again go undetected. This is another way that a corrupt DRE could undermine the cut and choose element of the protocol. Even if the voter does notice the switch and is sure that they are right, it may be difficult to demonstrate this to a voting official.

3.2.1 Mitigation

Many of the problems discussed above arise because the voters are required to participate in a fairly complex, multi-step protocol. The security of the scheme depends on the voters following the steps and performing the relevant checks, etc. In practice, it may be unreasonable to expect voters to spot any discrepancies in the execution or to appreciate their significance, especially as voting is an infrequent activity. Many otherwise correct technical systems are let down by a failure to take proper account of human fallibility. The tendency of Enigma cipher clerks to reuse the same message indicators and to use predictable preambles is an excellent example.

A possible mitigation is to educate voters on the procedures and their significance. As suggested in [11], the effectiveness of voter education in preventing such attacks is limited, especially if the protocols are lengthy and complicated.

A further possible mitigation is parallel testing during the election: to have auditors cast test votes and observe a device’s behaviour. This is also problematic. Such auditors would also need to be acutely familiar with the voting protocol. Steps would be needed to prevent confusion between the test and real votes in such a way as to avoid signalling to the device any distinction between real and test votes. Furthermore, the DREs could evade the auditing by altering the protocol only intermittently.

Arguably, a better solution is to make the voter experience much simpler. This is a characteristic of the Prêt à Voter scheme as we describe later.

3.3 Denial of Service

Karlof et al [11] describe several possibilities for DoS attacks that could disrupt or invalidate an election. For example, the DRE could falsify receipts, either duplicating them or submitting votes of its own choice. The former can be detected by officials scanning the WBB, but identifying the forged votes is more difficult.

DREs, possibly in collusion with an outsider, or tellers colluding with each other could stage a DoS. This could be global or more selective, for example, only in constituencies for which the pattern of votes goes against some chosen candidate. In both the Chaum and Neff schemes, the DRE necessarily ‘learns’ the voter’s choice during receipt construction. Hence, a selective DoS instigated by the devices is a feasible threat.

For all these attacks, adequate error-handling and recovery strategies need to be in place. In addition, some form of back-up is desirable, e.g. a *voter-verifiable paper audit trail* (VVPAT) [15]. Essentially, the authority retains paper copies of the ballot receipts in case re-counting is necessary.

We return to these attacks in Section 5, in which we examine the vulnerabilities of Prêt à Voter. Further attacks are described in Section 6.

4 The Prêt à Voter Scheme

We now present an overview of the Prêt à Voter scheme. For full details see [6]. Prêt à Voter is based on the Chaum scheme, but uses a radically different mechanism to represent the encrypted vote value in the ballot receipt. In place of the visual cryptographic techniques of the Chaum original, the voters are provided with a familiar-looking ballot form. An example is shown below.

Nihilist	
Buddhist	
Anarchist	
Sophist	
Solipsist	
	<i>7rJ94K</i>

The voter makes her selection in the usual way by placing a cross against the candidate of choice. Thus a vote for the Sophist candidate is indicated thus:

Nihilist	
Buddhist	
Anarchist	
Sophist	X
Solipsist	
	<i>7rJ94K</i>

To cast the vote, the voter now separates the right hand (RH) and left hand (LH) strips. The LH strip should be destroyed, by, for example, feeding it into a shredder. The RH strip is placed under an optical reader or similar device. This records the information on the RH strip: the random-looking value at the bottom of the strip and the position of the *X*, i.e., the numerical representation of the cell into which it has been entered. The RH strip is now returned to the voter to retain as her receipt:

X
<i>7rJ94K</i>

The ballot forms would be augmented with various anti-counterfeiting devices, and a digital signature applied to the receipt when the vote is cast.

Thus far, aside from the retention of a receipt, the process of casting a vote is entirely familiar, to a UK voter at least. Now, an objection at this point is that possession of a receipt would open up the possibility of coercion or vote-buying. The trick that sidesteps this is that the order of candidate lists on the ballot forms are randomised. Choose a ballot form at random, and the order in which the candidates are shown will be unpredictable. Clearly, as long as the LH strip is removed, the RH strip alone does not indicate which way the vote was cast.

Now the problem is how the votes will be extracted and counted. This is where the random value printed on the bottom of the receipt and known as the ‘onion’, comes into play. Buried cryptographically in this value is the information needed to reconstruct the candidate list shown on the LH strip and visible to the voter when they cast their vote. This information is encrypted under the secret keys of a number of tellers. Thus, only the tellers acting in consort are able to reconstruct the candidate order and so interpret the vote value encoded on the receipt.

One way of thinking about this is that, in contrast to other voter-verifiable schemes, the vote value is not directly encrypted to form the receipt. Rather, the (randomised) frame of reference, i.e., the order of the candidate list in which the vote is represented, is encrypted.

Once the election has closed, all the receipts are transmitted to a central tabulation server which posts them to a secure WBB. This is a write-only, publicly visible facility. Only the tabulation server can write to this and, once written, anything posted to it will remain unchanged. Voters can visit this WBB and confirm that their receipt appears correctly.

After a suitable period in which voters can verify that their receipt has been correctly posted, the set of tellers take over and perform a robust, anonymising, decryption mix on the batch of posted receipts. We omit the details of this here, but they can be found in [6].

All this is fine as long as all the steps are performed faithfully. If we are prepared to trust the entities executing this process then we can be confident that the election will be accurate and the vote values kept secret. However, the aim of schemes like the ones devised by Chaum and Neff and Prêt à Voter is to achieve these goals without the need to place such trust in any of the components of the scheme. We now outline very briefly the mechanisms used to detect any malfunction or misbehaviour by the devices or processes that comprise the scheme.

Leaving aside for the moment problems that might arise in the surrounding system, there are basically three places where things might go wrong with respect to the accuracy requirement:

- Ballot forms might be incorrectly constructed in that the information buried in the cryptographic value on the receipt might not in fact correspond to the candidate order shown on the LH strip. Clearly if this were the case, the subsequent decryption of the receipt would lead to the wrong vote value being output.
- The receipt might be incorrectly recorded or transmitted to the WBB.
- The tellers might fail to correctly decrypt the receipts.

For all of these there are mechanisms in place to (probabilistically) detect any malfunctions or corruption. For further details, see [6].

5 Systems-based Analysis of Prêt à Voter

We now relate the vulnerabilities identified in [11], to the Prêt à Voter scheme, some of which were and discussed in Section 3.

5.1 Subliminal channels

Random subliminal channels appear to be somewhat less of a problem for Prêt à Voter. Firstly, the DRE only scans the ballot receipts and posts digital copies of them to the WBB. Thus, in contrast to the Chaum and Neff schemes, a correctly implemented device does not learn the voter's choice, and is therefore unable leak this information. Secondly, the kind of subliminal channels that could occur in the Chaum and Neff schemes do not occur in Prêt à Voter.

Strictly speaking, for the first assertion to be valid, we need to ensure that the device does not get sight of the candidate list. There are various ways to achieve this, but they have to be balanced against the issue of enforcing the destruction of the LH strip, i.e., the candidate list. We will return to this later.

The absence of subliminal channels in Prêt à Voter is due to the fact that the ballot forms are generated in advance and allocated randomly to voters. Thus the cryptographic commitments are made before any linkage to voter identities or vote choices are revealed. This feature is made possible by the way that Prêt à Voter encodes the voter choice in the receipt: rather than directly encrypting the vote value, Prêt à Voter encrypts the encoding of the frame of reference, i.e., candidate list, in which the vote value is represented.

Regarding semantic subliminal channels, suitable implementation should ensure that the digital representation of a Prêt à Voter receipt for a given vote value and ballot form is unique, for example, the onion value and the number indicating the chosen cell on the LH column. Hence, there should be no possibility of a semantic subliminal channel. So, even if the device were able to learn

the voter’s choice, it would have no subliminal channels with which to leak this information.

It is feasible that a corrupt authority could introduce subliminal channels in the ballot forms, but has a high chance of being caught during auditing. In any case, with random selection of ballot forms for both auditing and voting, the authority cannot meaningfully predict when or by whom the forms will be used. Furthermore, certain ballot forms may end up being used for auditing or dummy voting. It would seem that there is little incentive for the authority to corrupt the ballot forms in this way.

Like the Chaum scheme, Prêt à Voter utilises decryption mix-nets with random partial checking, so the same mitigations as previously described in Section 3.1.1, i.e., ensuring determinism in all the the tellers’ operations, etc., would apply here as well.

5.2 Protocol Attacks

In Prêt à Voter, the voter does not engage in a multi-step protocol with the DRE. In the booth, the voter simply marks her ballot form, detaches the LH strip, and inserts the RH strip into the recording device. Finally, the voter retains the digitally signed, franked receipt and exits the booth. In fact, the RH strip could be automatically detached and destroyed before the receipt is fed into the recording device. From the voter’s point of view, the process should appear fairly straightforward.

Thus, voter interaction at the polling station is vastly simpler than in either the Chaum or the Neff schemes, and there is no opportunity for message re-ordering or social engineering on the part of the DRE as described in [11] and Section 3.2.

It is worth noting that in Prêt à Voter, the analogue of the cut and choose component of the Chaum or Neff schemes lies in the auditing of the ballot forms, i.e., before any voter involvement. The authority commits to the cryptographic material on the ballot forms ahead of the election. A random selection of these are checked by the auditors for well-formedness. Assuming that they pass the checks, the forms are then destroyed. Forms that fail the checks would be retained for forensic purposes.

5.3 Denial of Service

Although DREs do not create receipts in Prêt à Voter, a faulty or malicious device could still duplicate them, causing a DoS. Another possibility is for the DRE to post the wrong onion values to the WBB. Recovery can be tricky. Duplicated receipts could be deleted if the onion values and candidate choices are identical, but more problematic if the latter turn out to be different. In the case of erroneous onion values, voters would not be able to confirm the correct posting of their receipts, and likewise, recovery could be difficult.

Selective DoS by colluding tellers, as described in Section 3.3, is also possible threat. Like the Chaum and Neff schemes, recovery and error-handling

strategies are required.

A possible enhancement of Prêt à Voter, to be detailed in a forthcoming paper, is to replace the decryption mixes with re-encryption mixes. This has a number of advantages, one being that recovery from DoS failures is much easier. There are a number of reasons for this:

- The mix and decryption stages are separated and we now have mix tellers that perform the mix stage and decryption tellers that perform the decryption once the anonymising mix has been performed.
- The mix tellers do not need secret keys, they simply re-randomise the encryption. A failed mix teller can therefore simply be replaced without all the unpleasantness of having to surgically extract keys.
- The mix and audit can be independently re-run. With (deterministic) decryption mixes, the selection of links for audits cannot be independently selected on the re-run of the mix without compromising secrecy.

However, corruption of (decryption) teller’s keys could result in failure to decrypt the votes, [11]. The use of threshold encryption schemes here would help foil DoS attacks by ensuring the the failure of a proportion of the (decryption) tellers could be tolerated.

In [6], a VVPAT style mechanism is suggested as an extension to the Prêt à Voter scheme. The DRE scans the voter’s receipt, and generates an extra copy, perhaps viewed by the voter under glass in the manner of the Mercuri Method [15]. Once this copy has been verified by the voter, it is entered into a sealed box. This provides a back-up record of receipts cast should recovery mechanisms need to be invoked.

We note that VVPAT style mechanisms work rather better for voter-verifiable, encrypted receipt schemes. A critique of conventional VVPAT in which a paper record of plaintext ballots is kept, is that it may introduce ballot privacy concerns. The most straightforward implementation of VVPAT is to print the copies of the ballots onto a paper roll. The difficulty with this is that this preserves the order in which they are cast, and could be linked to any record of the order in which voters entered the booth. A counter-measure is to cut each ballot copy before it is dropped into the audit box. This however is mechanically more complex and error prone. With encrypted receipts, the possibility of linking receipts to voters should be unproblematic.

Other recovery and error-handling strategies are subjects for further research.

5.4 Discarded Receipts

Like the Chaum and Neff schemes, carelessly discarded receipts could be a problem in Prêt à Voter, as this could indicate which receipts will not be checked on the WBB [11]. This gives malicious colluding parties an opportunity to

delete or alter the corresponding ballots, possibly also injecting votes of their own choosing into the system.

As with the Chaum and Neff schemes, one mitigation is voter education [11], but again the effectiveness is questionable. A more effective approach might be to introduce a VVPAT style mechanism, as described above. This would produce a physical record of all receipts cast at each booth. Independent authorities could then check the correspondence between this record and the contents of the WBB. This would supplement the voter checks, and also ensure that an adversary cannot be sure that alterations to discarded receipts will not be caught by subsequent checks. This has the added advantage that voter checks on the WBB can be supplemented by auditor checks between the VVPAT and the WBB. Hence, less reliance need be placed on voter's diligence in carrying out this task.

5.5 Invalid Digital Signatures

In the Chaum scheme, receipts are digitally signed by the DRE. This counters the use of fake receipts to discredit election integrity, providing the system with a defense against dishonest voters. However, false signatures could be used to discredit voters, leaving them without a way to prove a dishonest system [11].

In the Chaum scheme it is suggested that, after casting their vote, voter be provided with devices capable of checking the well-formedness of the receipts, including the the digital signature. Such devices could be provided by various independent organisations, such as the Electoral Commission etc. Any DRE that is producing invalid signatures should therefore be readily detected. Similar measures could be utilised for Prêt à Voter.

In [6], it is suggested that physical signatures or stamps could be applied to authenticate ballot receipts. While this removes dependence on trusted devices, there should ideally be some precaution against faked signatures and stamps.

5.6 Insecure Web Bulletin Board

Like the Chaum and Neff schemes, Prêt à Voter also relies on a secure WBB, which, aside from it having read-only access, is, similarly, otherwise unspecified. In [11], Karlof et al. describe a possible attack that can arise from a poorly implemented WBB. For example, it may be possible for the WBB to arrange for the voter to see a correct record of her ballot receipt, which, in collusion with the mix-net, has been deleted. As a result the voter will believe that her vote has been counted, when in reality it has not.

A suggested mitigation [11] is that data storage should be robust against hardware and software failure and also malicious attacks, such as the one described above. In addition, only authorised parties should be able to append data to the contents of the WBB. However, we note that this is still vulnerable to corruption.

Similar mitigations also apply to Prêt à Voter in order to ensure that the WBB is secure.

6 Further Vulnerabilities

In this section we discuss other possible vulnerabilities of the Chaum and Neff schemes not identified in [11]. We also suggest appropriate mitigation strategies.

6.1 Doll Matching Attack

The Chaum scheme requires the voter to check that the pair of dolls printed by the DRE on the two layers match. Failure to check this match could allow the DRE to construct fake receipts without detection. It might appear difficult for the DRE to construct the layers in such a way as to alter the voters intention whilst producing dolls with so little difference that it escapes visual comparison. However, this should be considered a potential vulnerability.

The counter-measures would presumably aim to ensure that visual matching of the dolls is as easy to perform as possible. Thus, for example, the dolls might be encoded in vertically aligned bar codes on either side of the central perforation. any mismatch would then show up as a misalignment of the bars.

This style of attack is not relevant to the Neff scheme or to Prêt à Voter.

6.2 Undermining Public Confidence in the Secrecy of Encrypted Receipts

Another style of attack against schemes employing encrypted receipts that might serve to coerce some voters is as follows. The voter is persuaded that there is some way to extract her vote from the encrypted receipt, even though the coercer has no such capability. If a sufficient number of voters were convinced by such a claim and influenced to alter their vote, it may be possible to undermine the outcome of the election. This might be achieved in various ways. For example, the coercer might launch a publicity campaign urging voters to submit their receipts and claiming that the "correctness" of the choice would be checked. Some reward, e.g., entry into a lottery, would be provided to all receipts that passed the supposed checks. For example, it could be claimed that receipts that passed the checks would be entered into a lottery.

It appears to be quite difficult to counter such a psychological attack other than by careful voter education.

7 Prêt à Voter Specific Vulnerabilities

In analysing Prêt à Voter from the system perspective, we also identified some other possible vulnerabilities that are specific to the scheme, i.e., do not apply to either the Chaum or Neff schemes. We discuss them and suggest possible mitigations.

7.1 Chain Voting

A style of attack that can be quite effective against some conventional paper ballot schemes is chain voting. In this attack, the coercer smuggles an unused ballot form out of the polling station and marks his preferred candidate. He intercepts a voter as they enter the polling station and presents them with the marked ballot form. The voter is told that if they emerge with a fresh, unmarked form they will be rewarded appropriately. The fresh form can then be marked again and passed to the next voter.

The attack is fiendishly effective against election systems in which, as in the UK system, the ballot forms are a controlled resource (voters are given a ballot form when they register at the polling station) and it is difficult for voters to exit the polling station without casting a ballot. In this situation the voter is under duress to cast the form marked by the coercer and to retain the fresh form that they are provided with when they register. Of course, the fact that the procedures make it difficult for voters to leave the polling station without being observed to cast a ballot arguably makes it harder for the coercer to initialise the attack. However, a determined attacker would certainly find a way, for example by bribing an official, or placing a fake form in the ballot box. Once the attack is initialised, the procedure works in the coercer's favour.

A possible counter-measure for conventional pen and paper systems is to adopt a system along the lines of that used in, for example, French elections. Here the ballot forms are not a controlled resource: they are freely available in the polling stations. The voter identity is checked at the moment that they cast their vote rather than at the time that they collect a ballot form. Here, when a voter emerges with a fresh form, the coercer cannot be sure that their marked form was actually used to cast a vote. Consequently, the motivation for the attack is undermined.

Neither the Chaum nor the Neff schemes, in which the ballot forms and receipts are generated on demand in the booth, are vulnerable to this style of attack. Prêt à Voter is, however, potentially vulnerable, and the counter-measure that is effective in conventional pen and paper systems does not work here. This is because the cast receipts are posted to the WBB and these can be checked by the coercer.

7.2 Mitigation

The threat is that the coercer may be able to induce a voter to use a ballot form that he has seen, and hence knows the onion/candidate list association. Various counter-measures can be envisaged. Clearly, this is a special case of the more general point that the information on ballot forms has to be carefully protected. We will return to this shortly. For the moment, we concentrate on the chain voting threat.

Firstly, we observe that the voter does not, in fact, need to see the onion in order to be able to make their selection on the form. This suggests that we could put in place mechanisms that will ensure that the onion value is only revealed

after the ballot has been cast.

A further observation is that, in a scheme using encrypted ballot receipts, only the step of marking a selection needs be done in the privacy of a booth. The actual casting of the ballot receipt could be performed in the presence of an official.

Putting these two observations together suggests the following possible countermeasure to the chain voting attack: the onion is concealed by a ‘scratch strip’, similar to that used in lottery tickets commonly found in the UK. A possible procedure would then be for the voter to register and collect a fresh ballot form, with scratch strip intact. The voter then goes to the booth and marks her selection, and detaches and destroys the LH strip. She then exits the booth and takes her receipt to an official who checks her identity, scores off her name from the electoral list and checks that the scratch strip is intact. The strip can now be removed to reveal the onion and the receipt recorded as previously described in Section 4.

Steps would need to be taken to ensure that the scratch strips cannot be scanned with some device to read the concealed onions. This has reportedly been done using the laser photo-acoustic effect [8]. A laser beam is used to line-scan the strip while a microphone picks up the acoustic waves caused by differential absorption of the light. By adjusting the effect to the appropriate depth, the printing below the covering strip can apparently be read. Obtaining and operating the necessary equipment would, however, require expense and technical know-how on the part of the attacker. Nevertheless, it should be considered a possible threat.

In [6], vote casting in the presence of an official was suggested as a countermeasure against double voting. The above suggests another reason why this might be desirable.

7.3 Authority knowledge

In the current version of Prêt à Voter, the authority has knowledge of ballot form information, i.e. the cryptographic primitives used to generate the candidate offsets, hence the onions, and, in particular, the association between these values. This could be problematic as the authority has to be trusted not to leak this information. Even if the authority is entirely trustworthy in this respect, there is always a danger of this information being leaked during distribution or storage of the ballot forms.

This suggests that we should arrange for the ballot form material to be constructed in a distributed fashion, in such a way as to ensure that no single entity knows the association of onions and candidate lists. As noted previously, it is not necessary for the voter to see the onion at the time of marking her selection. For this, she only needs the candidate list. So it should be possible to devise mechanisms that allow the voter to make her choice, cast her vote and later check her receipt on the WBB, without the onion and candidate list ever being exposed simultaneously.


The challenge in this task is to guarantee that the candidate list and, later, the onion that is shown to the voter are correctly linked, i.e., the onion does correspond to the candidate list. Once again, we would like to achieve this guarantee without having to place trust in any devices or individuals. Currently, this is ensured by the fact that the authority commits to the association in print and this is randomly audited.

We now outline a possible scheme for distributed ballot form construction. It is based on onions encrypted using El-Gamal, or a similar randomised encryption algorithm. The ballot form material is generated by a number of entities that we refer to as ballot clerks. The first clerk generates a large quantity of El Gamal onions, which then enter a re-encryption pre-mix involving the other clerks. The last clerk collects the resulting permuted, random onions and, for each one, produces two re-encryptions. These paired onions are now printed onto ballot forms, one at the bottom of the LH column, the other on the bottom of the RH column.

A proto-ballot form could be as follows:

	7rJ94K
jH89Gq	

These two onions should yield the same candidate list. The RH onion is now concealed with a scratch strip to give:

	
jH89Gq	

Finally, for each form, the last clerk sends off the visible, LH onions are despatched to the tellers, who send back the corresponding candidate list. This step is similar to the dummy voting process of the original Prêt à Voter. The candidate list is now printed in the LH column and the LH onion is removed. This results, finally, in the familiar Prêt à Voter ballot forms, but with the onion blocked out:

Sophist	
Bhuddist	
Anarchist	
Solipsist	
Alchemist	
	onion

Note that no single entity now knows the association of onion and scratch strip. Strictly speaking, the last two clerks acting in collusion could form the association, but a scheme could be devised to raise the collusion threshold. Interestingly, we note also that, even though these two clerks in collusion know the onion/candidate list association, they cannot prove this knowledge to a third party as they do not know the necessary cryptographic primitives. All the stages of the above ballot form generation can be randomly audited to catch any misbehaviour. In particular, a random selection of forms could be made by auditors, the scratch strips removed and checks performed as before. If any corruption needs to be traced back to individual tellers, then random audits at various stages of the process might be necessary.

Another possible counter-measure against single entity knowledge, as suggested in [6], is to incorporate various sources of entropy and generate ballot forms on demand. This, for example, the entropy derived from optical scanning of randomly distributed fibres in the paper used as a source of entropy.

Details of such enhancements are beyond the scope of this paper and are the subject of future research.

7.4 Enforcing the Destruction of the Left-hand Strips

After the voter has marked her choice on the ballot form, it is important that the left-hand strip be destroyed. If a voter manages to leave the polling station with this, she could use it to prove her vote to a third party. Clearly, this lays the system open to coercion.

Several mitigations against this are possible. The voter could be required to destroy the left-hand strip in the presence of an official, preferably in some mechanical shredding device. This could perhaps be done at the time of casting the ballot form, as suggested above. However, care would have to be taken to ensure that the official is not able to record the association of the receipt and candidate lists.

Another possibility is to make ‘decoy’ left-hand strips freely available in the booths, so the voter cannot convince the coercer that the one she emerges with is genuine.

A further possibility is to print the onion vertically in the LH column of the ballot form. This is covered by a scratch strip over which the candidate list is printed. The voter would make their selection with the scratch strip intact, then remove it to reveal the onion and cast the vote as before.

A fuller exploration of this topic is beyond the scope of this paper and is a subject of future research.

7.5 Confusion of Teller Modes

As previously mentioned in Section 4, the tellers perform an anonymising decryption mix on the receipts posted to the WBB. However, they also have a role in checking the construction of ballot forms, both by auditors and voters [6]. In auditing, the onions are sent to the tellers, who return the corresponding germ values. The auditors then re-compute the onion values and candidate offsets and check that they are correct. In voter checking, the tellers return the candidate ordering corresponding to the onion value sent by the voter.

It is important that checked forms are then discarded, as either the seed/onion or onion/candidate ordering associations have been revealed. If the forms were then re-used to cast votes, there would be a threat to ballot secrecy. Conversely, it should not be possible to run a check on a form that has been used to cast a vote.

To mitigate this, ballot forms could be checked by voters in the presence of an official, who then ensures that used forms are discarded. Forms could be invalidated once used. The scratch strip mechanism, described in Sections 7.1, 7.3 and 7.4, would prove useful here as well. An authentication code, for example, could be overprinted on the scratch strip that would be necessary to enable the checking mode. Revealing the onion would destroy the scratch strip and this code along with it, ensuring that the form could not be reused later.

8 Conclusion

It has been recognised that even the most sophisticated secure system can be undermined by vulnerabilities in the surrounding system. The point is made in Anderson's paper [2], which shows that failures of banking systems are often due to implementational and human factors, rather than flawed cryptographic protocols. This is equally true of voting systems. [21] and [11] illustrate this nicely for the Chaum and Neff schemes.

In this paper, we have extended the analysis of [11] with some further systems based attacks, and considered the applicability of these vulnerabilities to the Prêt à Voter scheme.

We have shown that Prêt à Voter is remarkably resilient to most of the vulnerabilities discussed in [11], many of which stem from voter interaction with devices and generation of entropy at the time of voting. On the other hand, Prêt à Voter, is potentially prey to chain voting attacks, which do not apply to schemes in which the cryptographic material is generated on demand. In fact, as we have discussed, this style of attack is particularly virulent in the context of voter-verifiable schemes with pre-prepared ballot forms. We have presented some counter-measures to this style of attack.

We have also identified some further attacks not mentioned in [11], some of which are specific to Prêt à Voter, but also some which could apply to other voting schemes. Possible mitigations against these attacks have also been suggested.

Overall, we conclude that, as with any secure system, voting schemes require great care in the design and evaluation of the surrounding system. Analysis from a system perspective has provided valuable insight into the way forward for Prêt à Voter, and some of the planned future extensions have been mentioned. It has also underlined the need for adequate error-handling and recovery strategies, and that a VVPAT, as suggested in [6], would be highly desirable.

Provided that a systems perspective is taken into consideration during the design and evaluation phases, as advocated in [21] or [11], then there should be every reason to suppose that cryptographic, voter-verifiable voting schemes may provide high assurance elections.

9 Acknowledgements

The authors would like to thank Michael Clarkson, Michael Jackson, Steve Kremer, Andrey Povyakalo, Mark Ryan and Luca Vigano for fruitful discussions and DSTL and the EPSRC DIRC project for partial funding of this work.

References

- [1] The trouble with technology. *The Economist*, Sept 16 2004.
- [2] R. Anderson. Why cryptosystems fail. In *Conference on Computer and Communications Security*. ACM, 1993.
- [3] J. Bannet, W. Price, A. Rudys, J. Singer, and D. Wallach. Hack-a-vote: Security issues with electronic voting systems. *IEEE Security and Privacy*, 2(1), Jan/Feb 2004.
- [4] J. Bryans and P.Y.A. Ryan. A dependability analysis of the chaum voting scheme. Technical Report CS-TR-809, University of Newcastle upon Tyne, 2003.
- [5] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, January-February 2004.
- [6] D. Chaum, P.Y.A. Ryan, and S. Schneider. A practical, voter-verifiable election scheme. Technical Report CS-TR-880, University of Newcastle upon Tyne, 2004.
- [7] A. Fujioka and T. Okamoto and K. Ohta. A practical secret voting scheme for large scale elections. In *Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, pages 244–251. ACM, 1992.
- [8] E. Gerck. Instant lottery cards too, re: reading pins in ‘secure’ mailers without opening them, 2005. <http://www.mail-archive.com/cryptography>

- [9] M. Jakobsson, A. Juels, and Ronald Rivest. Making mix nets robust for electronic voting by randomized partial checking. In *USENIX Security Symposium*, pages 339–353, 2002.
- [10] D. W. Jones. A brief illustrated history of voting, 2003. <http://www.cs.uiowa.edu/~jones/voting/pictures>.
- [11] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In *USENIX Security Symposium*, number 3444 in Lecture Notes in Computer Science, pages 186–200. Springer-Verlag, 2005.
- [12] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *Symposium on Security and Privacy*. IEEE, 2004.
- [13] S. Kremer and M. Ryan. Analysis of an electronic voting protocol in the applied pi-calculus. In *European Symposium on Programming*, number 3444 in Lecture Notes in Computer Science, pages 186–200. Springer-Verlag, 2005.
- [14] T. W. Lauer. The risk of e-voting. *Electronic Journal of e-Government*, 2(3), Dec 2004.
- [15] R. Mercuri. A better ballot box? *IEEE Spectrum Online*, October 2002.
- [16] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology*, number 950 in Lecture Notes in Computer Science, pages 1–12. Springer-Verlag, 1994.
- [17] A. Neff. A verifiable secret shuffle and its application to e-voting. In *Conference on Computer and Communications Security*, pages 116–125, 2001.
- [18] A. Neff. Practical high certainty intent verification for encrypted votes, 2004. <http://www.votehere.net/documentation/vhti>.
- [19] A. Neff. Verifiable mixing(shuffling) of el-gamal pairs, 2004. <http://www.votehere.net/documentation/vhti>.
- [20] A. Roscoe, Jim Woodcock, and L. Wulf. Non-interference through determinism. *Journal of Computer Security*, 4(1):27–54, 1994.
- [21] P.Y.A. Ryan. Towards a dependability case for the chaum voting scheme, 2004. DIMACS Workshop on Electronic Voting – Theory and Practice.