Improving the Farnel Voting Scheme

Roberto Araújo[1], Peter Y. A. Ryan[2]

[1]Department of Computer Science, TU-Darmstadt
Hochschulstrasse 10, D-64289 Darmstadt, Germany
rsa@cdc.informatik.tu-darmstadt.de

[2]Centre for Software Reliability, Newcastle University
Newcastle upon Tyne NE1 7RU UK
peter.ryan@ncl.ac.uk

Abstract: Farnel is a voting scheme which first introduced the concept of a ballot box to exchange votes. Recently, Araújo et al. improved this concept to accomplish a voter-verifiable scheme in which voters receive copies of receipts of one or more randomly selected previous cast votes. The scheme, however, relies on a strong requisite to achieve security: trustworthy talliers. With the goal of removing this requisite, in this paper we propose a Prêt-à-Voter style receipt for this scheme. In addition, we present a novel way to initialize the Farnel box and a new scheme based on combining Farnel with Prêt-à-Voter style encoding of receipts.

1 Introduction

Voter-verifiability is a novel security feature provided by several recent voting systems, such as Prêt-à-Voter [Rya04, CRS05] and Punch Scan [PH06]. It allows voters to verify that their votes are accurately counted by means of *protected receipts* and so gives more confidence to the election process. The voters, however, cannot use their receipts to compromise their privacy, even if they are prepared to cooperate with the coercer.

High-assurance voting systems typically rely on cryptography to achieve security and to implement voter-verifiability. Such technology makes the security of modern systems comparable or even better than traditional paper-based elections. However, systems that employ cryptography are not easily grasped by the average voter and so voters need to rely on the assurances of experts.

With the goal of making such schemes more understandable, Randell-Ryan [RR06], Rivest [Riv06, RS07], and Araújo et al. [ACvdG07], introduced voter-verifiable schemes that do not rely on cryptography. These schemes are simple and can be more easily understood by the voters. However, they do not achieve the same levels of assurance as the cryptographic systems. In the scheme proposed in [Riv06], the ballot secrecy is not perfect and it may reveal statistical indications of voting results before the voting end. The proposals of Araújo et al. and of Randell-Ryan require trustworthy talliers or additional mechanisms to counter threats during the vote tabulation.

In this paper we introduce improvements for the scheme of Araújo et al. Especially, we propose a Prêt-à-Voter style receipt in order to detect manipulation of votes by adversaries, including malicious talliers. In addition, we present a novel way to initialize the Farnel box and a new scheme based on combining Farnel [ACvdG07, Cus01] with Prêt-à-Voter style encoding of receipts. Our proposals make use of cryptography to overcome the drawbacks of the previous non-cryptographic solutions.

This paper is organized as follows: in the next section we describe the elements of the Farnel mechanism. In Section 3 we introduce a new ballot form for the scheme of Araújo et al. Then, in Section 4, we show a new scheme based on Farnel that employs only one ballot box. Finally, we present our conclusions in Section 5.

2 Preliminaries

We present here the basic elements of the Farnel approach. The Farnel type voting schemes [ACvdG07, Cus01] are based on the observation that to achieve voter-verifiable it is not necessary for the voter to carry away a receipt corresponding to their own vote. The Farnel approach then is to provide voters, when they cast their votes, with copies of receipts of one or more randomly selected previous cast votes.

This idea has a number of attractive features: ballot secrecy is achieved up front and does not have to be provided by anonymising mixes, etc. during tabulation. In fact, plaintext receipts can be used in contrast to the encrypted receipts of many other voter-verifiable schemes, e.g. [Rya04]. Furthermore, any fears that voters might have that their vote is not truly concealed in an encrypted receipt is mitigated. The Farnel mechanism also mitigates randomization style attacks.

2.1 The Farnel Ballot Box

The Farnel is a concept of ballot box that was first introduced by Custódio [Cus01]. This ballot box performs differently from a conventional one. It is able to shuffle its contents and is initialized with elements (e.g. votes). After receiving elements from voters, it returns to them elements that correspond to randomly selected, previously cast votes. Recently, Araújo et al. [ACvdG07] improved the Farnel concept in order to accomplish a voter-verifiable scheme. In the improved concept, besides shuffling its elements, the Farnel box should be able to copy some elements and to remove scratched surfaces.

We describe the enhanced Farnel box as follows: it is a box that has mechanisms to remove scratch surfaces, and to shuffle and to copy elements in a memoryless way. The box has an initial set of elements cast before the voting. At the time of voting, it is able to receive an element, to shuffle its contents, to copy one or more randomly selected elements from its set, to output the copies, and to add the element received to its set. The box elements may be votes or receipts.

Although the requisites of the Farnel box seem difficult to implement, a tombola (i.e. a raffle drum) normally used in lottery games to shuffle tickets could form the basis of an implementation of the box.

The Farnel box was never formally specified. This way, we introduce now a specification of the box in the process algebra CSP.

Let Init denote the initial set of dummy ballots (say votes or receipts) with which the box is initialized. Let l denote the number of receipts to be output to each voter when they cast their votes and ballots the set of all possible ballots. Then the Farnel box will start in state Farnel (Init) and its subsequent behavior is defined recursively as:

$$Farnel_l(X) := cast?\ b{:}Ballots \rightarrow \Box receipt!\ r{:}\wp_1(X) \rightarrow Farnel_1(X \cup \{b\})$$

We have used the notation $\wp_l(X)$ to denote set of subsets of X of cardinality l.

Thus, the Farnel ballot box is parametrised by the integer l and its initialization *Init*. At any point, the box can accept a ballot b, after which it outputs a set of ballots in size l chosen at random from its current set X. After this, the new ballot is added to X and the box is ready to receive the next ballot.

2.2 The Initialization Process

The initialization process takes place before the election and is performed by the authorities in a public session. The main objective is to cast a predefined number of votes (or receipts) into the Farnel ballot box and to publish the number of elements cast per option on the bulletin board.

The elements cast before the election are necessary mainly for ensuring the anonymity of the early voters. As the Farnel receives an input from each voter and outputs copies of random elements, it must have an initial set of elements to choose from. Otherwise, after receiving inputs, the Farnel would not have enough elements to select at random and to make the copies.

For the schemes that we describe here, it is necessary to ensure that ballots cast during the initialization are well formed in some way. This will typically involve some form of random auditing. Thus, for example, we might require that 2x blank ballots be created beforehand. The authorities perform the following steps to initialize the ballot box:

(1) Select x blank ballots at random and audit them as necessary. Ballots audited are discarded; (2) Mark the other x unaudited blank ballots according to the number of votes per option specified in advance; (3) Cast the x marked ballots (or receipts) into the Farnel box and publish the number of elements cast on the bulletin board.

Notice that in schemes which employ a conventional and a Farnel box (e.g. [ACvdG07]), the conventional box is initialized with votes and the Farnel is initialized with the corresponding receipts. Also, for schemes using plaintext ballots, the auditing for well-formedness is not necessary and would be omitted.

In order to prevent manipulation, the initialization process should be scrutinized by helper organizations. They should check that the ballot box is empty before it is initialized, as well as verify that all procedures above are performed correctly. Further, the ballot box should be sealed and continually supervised by third parties after the initialization. The seal is removed when the voting starts.

2.2.1 Initialization of the Farnel box with Void Ballots

Where we are using encrypted receipts we have an alternative way to initialize the Farnel box: we include a void option on the ballots and initialize the box with ballots representing votes for the void option. This has the advantage that we do not have to keep a log of the actual votes cast for each candidate during initialization. We do need a robust mechanism to ensure that all initializing votes are cast for void, but it seems likely that this is easier to enforce than maintaining a record of an initial tally. We can use this approach for the Prêt-à-Voter and ThreeBallot style ballots, but not where plaintext receipts are used.

2.3 The Parameters of the Farnel Box

The Farnel box is initialized with a number of elements (votes or receipts) before the voting starts and outputs copies of its elements during the voting, as described. The initial elements ensure the voter's anonymity while the copies are handed to the voter as her receipt. The number of initial elements, as well as the number of receipts given to each voter, compose the parameters of the box.

In order to preserve the voters' anonymity, the initial elements and the voters' elements cannot be distinguished through the copies output by the Farnel box. The number of initial elements is fundamental for guaranteeing this. As the Farnel box outputs elements for each voter, the elements of the early voters have more chance to be output. Hence, these elements may be distinguished from other elements. Depending on the number of initial elements, however, the chance of distinction may be negligible as the initial elements may also be output.

To achieve verifiability while maintaining anonymity, the number of initial elements and the number of receipts should be defined such that:

(1) The voter's anonymity is preserved even if the Farnel box is able to output a copy of her element; (2) An individual receipt or a set of them do not provide enough information to distinguish elements; (3) The number of copies of elements in all receipts is sufficient to detect accuracy problems with an acceptable probability (i.e. the probability that the corruption of any given vote is detected is at least 50%).

We require that the voter should not be able to obtain any information other than her choice when casting her element.

Taking into account these requisites, we have a number of possible strategies for initializing the box: ballots marked at random (with the totals carefully recorded), a predetermined number of votes per option, votes for a void option, or a combination of these methods. If we adopt an initialization with votes for void, we must include a minimal number of votes for the other options. Otherwise, the first voter may vote and receive a copy of her own vote as receipt. An initialization purely with void votes only works if we have mixes during the tabulation. This might seem like overkill since anonymity is already provided by the Farnel mechanism. However, it might still be useful in some contexts and does provide an extra layer of protection.

Note that in the specification of the Farnel box presented before, the box is not able to output the element it receives.

3 A New Ballot Design for the Farnel Variant Scheme

The Farnel scheme was proposed by Custódio [Cus01] (see [ACvdG07] for a description). The scheme employs an original Farnel ballot box and relies on physical signatures. However, it is not voter-verifiable. Recently, Araújo et al. [ACvdG07] introduced a variant of the Farnel scheme. In contrast to the original version, the scheme is voter-verifiable and does not employ signatures. It relies, though, on trustworthy talliers to tabulate the votes.

With the goal of removing this requisite, we introduce in this section a new ballot design for Araújo et al.'s proposal.

3.1 An Overview of Araújo et al.'s Farnel Variant Scheme

The scheme employs a ballot form composed of two halves that are linked by a unique ID and that are separated by perforations. More specifically, the ballot has an options half composed of the voting options as well as an ID and an ID half that contains the same ID of the options half (see Figure 1). These IDs are covered by scratch surfaces.
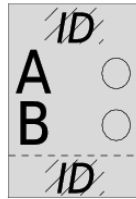
Figure 1: The ballot form of the Farnel variant scheme.

Besides the unusual ballot form, the scheme depends on two ballot boxes. One of them is conventional and the other is a Farnel box. These boxes are initialized before the voting. That is, the conventional box receives dummy votes (i.e. marked option halves) and the Farnel box receives the ID halves (i.e. receipts) corresponding to the votes. The scratch surfaces in the halves are detached during the initialization and at the end the number of votes cast is published on a bulletin board.

At time of voting, the voter receives a blank ballot and detaches its scratch surfaces. She then compares the IDs on the halves and if they match, she marks her option. After that, she separates the two halves of her ballot, casts the option half into the conventional box, and the other half into the Farnel box. Upon receiving the half, the Farnel box shuffles its ID halves and copies a set of them as receipt to the voter. As alternative to avoid comparison of IDs, the scheme may have an auditing process to check ballots before the voter receives her blank ballot and require the voter to cast her vote without removing the scratch surfaces. The Farnel box then removes the scratch of the half that it receives.

After the voting, the authorities publish the content of both ballot boxes on the bulletin board and count all votes from the conventional box. The dummy votes are then subtracted from the total of votes to obtain the results.

In order to verify the votes published on the bulletin board, voters and observers compare the ID halves with the IDs in the options halves. The voters can also match the IDs on their receipts with the options halves on the board.

3.1.1 Drawback

Due the receipt style employed, the proposal requires trustworthy talliers. These authorities should supervise the votes strictly after opening the ballot boxes. On the contrary, an adversary (e.g. a malicious tallier) is able to compromise the voting results as follows.

According to the scheme, the two halves of all ballots are published after the voting. This way, they can be compared to verify the exactness of the voting results. Before publishing the options halves, though, an adversary could replace a vote (i.e. a marked option half) by a new one marked to a different option, but that contains the same ID of the replaced vote. This substitution would not be detected by voters and observers, as they only compare IDs.

3.2 Combining the Farnel Variant Scheme and Prêt-à-Voter

The main problem of the receipt used in Farnel variant is that it does not depend on the option chosen. This way, an adversary is able to replace votes without being detected. In order to detect such a problem, a receipt should contain some information related to the option selected. However, this information should not reveal the option itself before the voting closes and should still be able to detect replacement of votes. Otherwise, the receipt can leak statistical information about the voting results as the Threeballot scheme [Riv06, RS07] (see [ACvdG07] for details). We introduce now a new ballot design for the Farnel variant that satisfies these requirements.

3.2.1 The Ballot Form

Our ballot form is based on the Prêt-à-Voter [Rya04, CRS05] ballot and is inspired by the ideas of Randell-Ryan [RR06] and of Scratch-and-vote [AR06]. Differently from the original Prêt-à-Voter ballot design, however, the ballot here does not include a mixnet onion.

The ballot is composed of two pages that are overlaid initially. The top page has a list of voting options in a random order with a selection bubble beside each option. The top page also includes a commitment to the list of options and its respective decommitment value. The bottom page contains the same bubbles and the same commitment as the top page. The commitment printed on both pages, as well as the value to open it on the top page, are covered by scratch surfaces. A carbon mechanism transfers the selections from the top page to the bottom page (see Figure 2 for an example of this ballot form).

Formally, the new ballot form is described as follows: Let C be a set of options available, π_C a permutation of C, H a secure hash function used here as commitment, and r a random number from a large (key) space. π_C, $H(\pi_C, r)$, r, and bubbles to select an option compose the top page. The bottom page contains *only* $H(\pi_C, r)$ and the bubbles in same position of the top page.
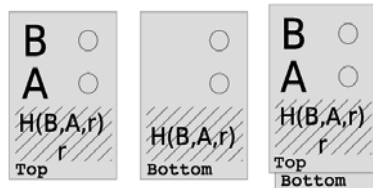

Figure 2: The proposed ballot form for the Farnel variant scheme.

The new ballot form satisfies the requisites above. The votes now are tabulated from the top pages and the receipts are made from the bottom pages (without the scratch surfaces). Because each bottom page contains the same selections of its corresponding top page and also includes the commitment to the options on the top page, an adversary cannot replace a top page by another with a different permutation or with a selection for a different option, without being detected. Moreover, since the bottom page does not include the option selected, an adversary cannot use receipts to obtain indication of the results before the voting closes.

3.2.2 New steps for the Initialization, the Voting, and the Tallying phases

Due the modification of the ballot form, the initialization, the voting and the tallying steps in the original scheme need to be adapted.

Before the Voting

The conventional box and the Farnel box are now initialized with marked top pages and with bottom pages, respectively (see also Section 2.2). Before initializing the boxes, however, the officials publicly audit ballots as follows: they separate the pages of each ballot and scratch off their surfaces; they then hash the options and the random number on top page, and compare the result with the hashes on both pages. Ballots audited are discarded.

Voting

In the voting phase, upon proving her eligibility to the voting authorities, the voter receives a sealed envelope with a blank ballot. If required by the voter, her ballot can be audited (as above) and she receives a new blank ballot. The voter performs the following steps to vote:

1.   (Selecting the option) In the voting booth, the voter marks her choice on the top page and it is transferred to the bottom page.

2.   (Verifying the ballot) She then inserts her ballot into a special envelope, which has transparent borders and a window to show just the scratch surface. After this, she hands the envelope to the authorities. They verify that the surface on the top page is intact and that the voter did not separate the two pages.

3.   (Casting the top page) The voter separates the pages of the ballot and casts the top page into the conventional ballot box.

4.   (Obtaining the receipt) She casts the bottom page into the Farnel box. The box shuffles its contents and outputs copies of randomly selected bottom pages as receipts.

Observe that the special envelope prevents the authorities to learn the voter's choice while verifying the surfaces, and the pages were not separated before.

Tallying and Verifying the Votes

As the Farnel variant scheme, the contents of the two ballot boxes are published on a bulletin board in the tallying phase. Now, the scratch surface on the top pages should be removed before publishing the ballots and the commitments should be decommited to verify the ballots. That is, the random number and the options on the top page are hashed together and the resulting hash is compared with the hash on both pages.

From the pages published on the bulletin board, everyone can perform the same procedures as the talliers to verify the votes. The voters, especially, match their receipts with the corresponding bottom pages on the board.

4 Single Box Farnel Scheme

The design presented above is awkward in several respects: it requires two ballots boxes and the vote casting procedure is rather complicated and vulnerable to certain threats. We present here an improved version of the Farnel variant that requires just one ballot box and uses a simpler vote casting procedure.

4.1 Requisites

The ballot form
As the design presented in Section 3.2.1, the ballot here is composed of two pages that are initially overlaid. The top page, though, contains *only* the options in a random order along with bubbles to select them. The bottom page contains the same bubbles as the top page and an index. Also, it includes one commitment to the options of the top page and the index. The index indicates the options' order and helps the authorities to identify the order in the tallying process. The commitment and the index are printed at the foot of the page, on the left and on the middle, respectively. In addition, the bottom page includes the corresponding decommitment that is printed close to the index. The commitment is covered by a scratch surface apart from the index and from the decommitment.

More formally, let C be a set of options available, I a set of positive integers, π_C a permutation of C, H a secure hash function used as commitment, i an index that is a unique number in I, and r a random number from a large (key) space. The top page is composed of π_C and bubbles to select the options. The bottom page contains $H(\pi_C, r, i)$, r, i, and the same bubbles of the top page (see also Figure 3).

The list of possible permutations (i.e. options' orders) for all ballots and the index corresponding to each permutation are published on the bulletin board before the voting.

The Ballot Box

The scheme employs just a Farnel ballot box that is initialized (see Section 2) with marked bottom pages before the voting starts; the corresponding top pages are destroyed.

4.2 The Scheme

Before the Voting

As required by the Farnel box, we define a number of copies l that each voter receives as receipts and initialize the box with a number of dummy votes (Section 2 details this process).

For the initialization as well as for the voting phase, we require an auditing process. The audit is necessary to detect malformed ballots and is performed as follows: the authorities select a set of ballots at random, separate the two pages of each ballot, and detach their scratch surfaces. In order to verify a ballot, the authorities hash the options on the top page along with the random number and the index printed on the bottom page. They then compare the resulting hash with the value $H(pC,r,i)$ also on the bottom page. Moreover, the authorities verify that the randomization on the top page corresponds to that one indicated by the index i. In the voting phase, helper organizations assist the voter to audit ballots in the same way.

Voting

The voting authorities hand a blank ballot to the voter in a sealed envelope after verifying her eligibility. The voter can either use the blank ballot to vote or ask the authorities to audit it. In the latter case, the authorities publicly detach the scratch surfaces on the ballot and check the commitment (as before) through a computer. This procedure can be performed again by helper organizations that would employ their own computers. Assuming that the ballot is verified as well-formed, it is discarded and the authorities hand a new blank ballot to the voter. In principle, we could allow the voter to opt to audit a number of ballots before accepting one to use to cast her vote. If any ballot fails the audit checks, then recovery mechanisms need to be invoked. Discussion of this is beyond the scope of this paper.

To cast her vote, the voter performs the following steps (see also Figure 3):

1.   (Selecting the option) In the voting booth, the voter chooses her option and marks the corresponding bubble on the ballot (a).

2.   (Verifying the ballot) She separates the two pages of her ballot (b) and adds the bottom page into an envelope to make visible only the scratch surfaces. After this, she destroys in public the top page by means of a paper shredder (c) and hands the envelope containing the bottom page to the officials. They verify that the surfaces are whole.

3. (Casting the vote) The voter removes the bottom page from the envelope and casts it publicly into the Farnel box (d).

4. (Obtaining the receipt) After receiving the bottom page, the Farnel box removes the scratch surface that covers only the commitment value on the left side, shuffles its set of bottom pages (e), and copies one of them. The copies are held by the voter as her receipt (f).

Note that the scheme may employ a mechanism to prevent voters from destroying top pages other than their own. For example, the ballots could be numbered in a similar way as in the case of preventing chain voting attacks (see Jones [Jon05] for details).
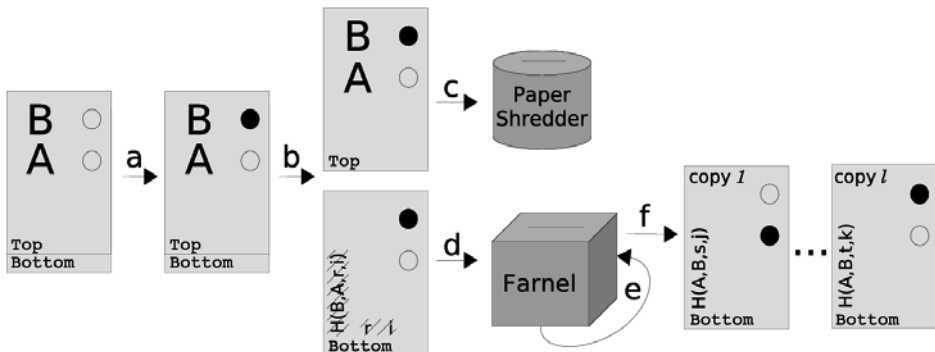

Figure 3: The main voting steps of the single box Farnel scheme.

Recovering and Tallying the Votes

In order to tally the votes, the talliers open the Farnel box, detach the scratch surfaces on all votes, and publish the votes on the bulletin board. Then, the talliers start the process to recover the votes. In this process, they compare the index on the vote with the index on the bulletin board to identify the permutation of the options; remember that the permutations as well as their indexes were previously published. From the permutation identified and the mark on the ballot, the talliers determine the option chosen by the voter. After recovering the votes, the authorities open all commitments using the random numbers and the indexes. In this step, they hash the random number and the index along with the permutation identified before, and compare the resulting hash with the hash on the vote. Now, the talliers count the votes in the same way as Farnel, that is, all votes are counted and the votes cast during the initialization phase are subtracted from this sum.

Verifying the Votes

Voters can, as usual, visit the bulletin board and confirm that their receipts appear accurately, and complain if they are not. Particularly, they verify the commitments and the marks on their receipts correspond to those on the votes published on the board. Helper organizations and observers verify that the talliers performed their work correctly.

4.2.1 Human Readable Paper Audit Trail

In the manner of Ryan [Rya07], the scheme could be adapted to provide a HRPAT by employing a conventional ballot box as alternative to the paper shredder. This way, instead of destroying the top page in a paper shredder, this page may be cast into the conventional ballot box. The box would store the top pages as an audit trail so that the votes can be counted without depending on the votes from the Farnel box.

5 Conclusions

We have presented a new ballot design for the scheme of Araújo et al. and a new voter-verifiable scheme based on Farnel. The solutions rely on the Prêt-à-Voter style ballots and cryptography to achieve security. Despite employing cryptography, the proposals require only a hash function and the voters perform simple steps to verify the votes corresponding to their receipts. That is, they just match numbers (i.e. hashes) and the marks on their receipts with the votes on the board. Helper organizations perform a more thorough verification of the hashes.

Moreover, we have introduced a novel way to initialize the Farnel box that employs void ballots. This initialization, however, only works with the ballot forms that give rise to protected receipts with a void option, e.g., Prêt-à-Vote style ballots. The new process would be easier to monitor and verify than having to maintain and record the total of the various votes cast in the initialization phase. Even so, ensuring only void votes are cast during the initialization phase is still challenging and will require carefully designed monitoring procedures.

Implementing the concept of the Farnel box in a way that requires minimal trust in the mechanism or procedures remains challenging. Rivest employed the original Farnel idea to overcome the reconstruction attack in the version of the Threeballot proposed in [Riv06]. In his scheme, a copy of a vote is made in advance and then it is exchanged by means of Farnel. This may be proved easier to implement with less trust assumptions. However, to prevent any possibility of the voter wandering off with her original receipt, the two steps (i.e. copy and exchange) need to be performed in close proximity.

An interesting feature of the Farnel mechanism is that it may help counter certain psychological style attacks on voter-verifiable schemes in which voters are convinced that the secrecy of their vote is not guaranteed. Using Farnel, the voters do not retain their own receipts, so any fear that the vote can be extracted should be mitigated. The down-side is that voters may be less motivated to check receipts if the receipt they hold is not their own. This may be offset by ensuring that voter helper organizations are on hand to perform the checks on behalf of the voters. If voters are given more than one receipt each this should also help as long as a reasonable proportion of voters are diligent enough to check all or many of their receipts.

Besides helping counter psychological attacks, the Farnel idea also mitigates randomization style attacks. These attacks were introduced by Schoenmakers [Sch00]. To perform a randomization attack, the adversary instructs the voter to generate a receipt that has a certain property. The adversary will not know what vote will be encoded, this is effectively random. The effect then is to force voters to vote for a random candidate, so nullifying their right to vote freely. The attack can be applied to Prêt-à-Voter and to Punch Scan schemes as the voter receipt in these schemes contain the position chosen by the voter. This way, an adversary may ask the voter to place her X in a specific position and to show him afterwards the receipt marked in this position. By means of the Farnel idea, however, the voter exchanges her receipt before leaving the voting place. Thus, the adversary cannot verify that the voter followed his instructions.

References

[ACvdG07] Roberto Araújo, Ricardo Felipe Custódio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel. IAVoSS Workshop On Trustworthy Elections (WOTE'07), June 2007.

[AR06]   Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pages 29–40, New York, NY, USA, 2006. ACM.

[CRS05]   David Chaum, Peter Y. A. Ryan, and Steve A. Schneider. A Practical Voter-Verifiable Election Scheme. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, ESORICS, volume 3679 of Lecture Notes in Computer Science, pages 118–139. Springer, 2005.

[Cus01]   Ricardo Custódio. Farnel: um protocolo de votação papel com verificabilidade parcial. Invited Talk at Simpósio Segurança em Informática (SSI), November 2001.

[Jon05]   Douglas   W.   Jones.   Chain   Voting,   August   2005. http://vote.nist.gov/threats/papers/ChainVoting.pdf.

[PH06]   Stefan Popoveniuc and Ben Hosp. An Introduction to Punchscan. IAVoSS Workshop On Trustworthy Elections (WOTE'06), June 2006.

[Riv06]   Ronald   L.   Rivest.   The   ThreeBallot   Voting   System. http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pd%f, October 2006.

[RR06]   Brian Randell and Peter Y.A. Ryan. Voting Technologies and Trust. IEEE Security and Privacy, 04(5):50–56, 2006.

[RS07]   Ronald Rivest and Warren Smith. Three Voting Protocols: ThreeBallot, VAV, and Twin. Electronic Voting Technology Workshop (EVT'07), August 2007.

[Rya04]   P.Y.A. Ryan. A Variant of the Chaum Voting Scheme. Technical Report CS-TR-864, University of Newcastle upon Tyne, 2004.

[Rya07]   P.Y.A. Ryan. Pret a Voter with a Human-Readable, Paper Audit Trail. Technical Report CS-TR-1038, University of Newcastle upon Tyne, 2007.

[Sch00]   Berry Schoenmakers. Personal communication, 2000.