Usable paper-based verifiable voting systems

Your N. Here
Your Institution

Second Name
Second Institution

Abstract

Over the past two decades, fear of election manipulation and hacking has spurred the security technology community to propose a variety of voting systems to implement verifiable voting. Most of these rely on complex cryptographic protocols which are neither simple nor usable, nor compatible with paper ballots. One of the few paper-based end-to-end verifiable voting proposals, Three-Ballot, has been thoroughly analysed and expanded as it suffered from both usability and security weaknesses. However, all the improvements increase the dependence on electronic devices. To make Three-Ballot a plausible solution for single race elections, this paper proposes three different candidate physical implementations based on 1) translucent paper, 2) masking tape, or 3) paper folding. The methods shown are all resistant to the known attacks on Three-Ballot while not requiring any electronic device.

1 Introduction

Voting, whether it is on a proposal in parliament or to elect politicians, has been a driver of innovation for more than a century, from Edison's invention of the first electrical voting system in 1868 [22] to the recent blockchain-based voting system proposals [4,31,48]. Correspondingly, voter resistance to the technological changes has followed, starting with the 40-year delay in implementing the secret ballot in the USA after its successful introduction in Australia – from which stems the name "Australian ballot". This resistance has come first from elected officials wanting to keep the ability to influence and coerce, sometimes under the guise of defending the "*manly pride that scorns concealment, and the sturdy will that refuses to bend to coercion*" [29]. Many costly or complex systems were created specifically for dealing with votes within a parliament, offering a higher level of secrecy against the higher usability of the frequently used system of voting by raising one's hand [22]. This proposed secrecy has been the source of arguments from both citizens and party leadership, generally aimed at keeping an elected official beholden to their promises [14], as secrecy can both ruin transparency of a representative and create the possibility for coercion.

One of the main sources of research and debate on political reform has been the use of audits, and the technological tools to make them easier. Errors with counting and recounting ballots are well-publicised, leading to a slew of systems that produce both a mechanised or electronic tally and an auditable paper ballot, from lever machines to optical scan methods [5]. Some of the improvements proposed come in the form of small modifications to the voting process to make voting or auditing easier, such as secret-ballot receipts [7], Scantegrity [8, 9] – an end-to-end independent verification system that coexists with a normal ballot – or audio audit trails [39], which seeks to improve the usability of auditing. Others require changing the whole infrastructure by using electronic-only systems [16, 21, 25], sometimes not even requiring polling places but instead some forms of e-identification [41, 47].

All the systems mentioned try to improve accuracy, integrity, and prevent coercion, miscounting, ballot box stuffing and related fraud, generally through technologically complex means. While those were major problems up until the middle of the 20th century [30], their scale is nowadays dwarfed by other considerations [1]. First, manipulation of voter registration lists [6], accessibility of voting [3] and turnout buying [26] can be orders of magnitude above the previously mentioned problems [5, 27, 33]. Second, familiarity with the voting sys-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

[1] This is mostly true in western democracies where the error rate is generally at least one order of magnitude lower than the margin of victory [12], but they are still extant in many countries such as Russia [13], Honduras [15] or Albania [11]

tem is essential[2], and technological changes without adequate training generally come with a strong temporary increase in error rates [17, 19].

With people being increasingly concerned with the threat of election hacking [28] – and legitimately so [41] – a number of experts have warned about the lack of adequate technology [34], and there is a strong pressure to return to paper-based systems, as it is supposedly much harder for an external adversary to massively manipulate them [24]. Unlike the USA, some countries, such as France, are also still using paper ballots massively with little evolution in voting practice since the early 20th century [12]. Relying only on paper poses a problem for most of the newly developed end-to-end verifiable voting systems that guarantee the authenticity and anonymity of all ballots. The main exception is the Pret-A-Voter system [37] which is mostly paper-based, although it does rely on some cryptography for the decryption or re-encryption mixnets, requiring an election authority that can potentially be decentralised, but is still electronic.

To address these issues, we propose a system that is entirely paper-based – although it can be made more usable or efficient through limited electronic means – based on Ron Rivest's Three-Ballot system [36]. This ingenious system can be presented in many different equivalent ways, but the simplest corresponds to 2-candidate races – although it is generalisable to more than that. The advantage of the method is that it makes it easy to preserve anonymity while giving voters direct verifiability. It works by making the voters use three simultaneous ballots, while enforcing that they vote at least once for each candidate, thus giving at most a 1-vote advantage to the candidate of their choice. All the ballots feature a unique identifier, and are made public after the voting period ends. After casting three ballots – of which two cancel each other – the voter gets a receipt for one of them, showing who it is for and the corresponding unique identifier. As that receipt can be for any candidate, it is impossible to guess the voter's choice, but as the receipts are not public, modifying or removing ballots in the ballot box includes a high risk of discovery.

Unfortunately the initial proposal had vulnerabilities. First, when voting for more than a few different races, it made unique identifying voting patterns on ballots possible, reintroducing the risk of coercion and vote-selling. This effect and its probability of happening in real races has been studied well in a variety of papers [1, 18, 44]. Although it poses a real risk in places with many concurrent races[3], many countries – such as Spain, Greece, France or Malawi [35] – don't have many parallel elections.

A second weakness of the system has been its low usability, not only in the practical implementation [23, 43] but also because of the very complexity of the scheme – here requiring voters to accurately vote 3 times, once against their selection – which is known to make it harder for voters to use correctly [42]. Finally, the system relies on the assumption that the ballots are all correctly filled and checked, which is dependent on an optical scanning machine which scans and validates the ballots without storing them, introducing a vulnerability coming from the use of potentially insecure hardware. The proposed solutions so far all rely on electronic remedies either through trusted hardware [45] or online services [38].

The above problems motivate the three candidate solutions proposed below. They are all usable physical implementations of Three-Ballot that do not need to be checked by electronic devices. The first candidate relies on translucent paper, allowing a voting official to check that the ballot is correctly filled without knowing who the voter voted for. The second is similar but simpler for the voter, with the higher usability coming at the expense of increased manufacturing complexity and cost. The third candidate is based on folding and hole-punching and has multiple desirable properties, including resistance even to attacks where voters film themselves in the ballot booth, a practice sometimes authorised under the name of "ballot selfies" [20]. As with Rivest's original scheme, it is possible to use optical scanning machines to check the ballots. However, the fact that a voting official can check the ballots without gaining information means that one doesn't have to rely on those machines. The ideal system might be to have people randomly assigned to one or the other, with discrepancies indicating probable fraud.

2 Constraints

To limit the confusion of voters, the execution of any candidate protocol should be familiar, hence close to the following:

- The voter comes into the polling station, receives information and prove that they are a registered voter (e.g. by showing the relevant ID).
- They are given instructions as to how to vote[4];
- They obtain some physical objects if necessary (e.g. ballots, pens, envelopes, magnifiers);
- They move into a privacy booth where they can manipulate the ballot;
- If needed, a machine or a voting official checks that their ballot (or envelope) is correct;

[2] Co-existence of redundant systems is possible, as in Estonia, but have an adverse effect on the adoption rate [46].

[3] Linked to the problems with many parallel races, having many different candidates on a single ballot increases confusion and proximity errors, with smaller candidates adjacent to high-ranked ones getting an additional 0.4% of the latter's vote [40].

[4] As has been suggested [17], in the first few public uses of the system, all users should receive detailed instructions and a test experience to show how they can use the voting system and ask for support before they mark their actual ballot.

- They cast their ballot, either by inserting it into a ballot box or by any other method.

Moreover, the protocols should satisfy the following constraints, in decreasing order of importance:

1. It should not allow multiple voting: there should be no way for a voter to give a multiple vote advantage to a single candidate. This should hold even if some but not all other agents (such as voting officials) are corrupt;
2. There should be no way for a third party to find out a particular voter's vote, and there should be no way for a voter to prove that they voted a particular way, to prevent corruption and coercion;
3. As a consequence of the previous constraint, if a receipt is given, the vote indicated on it should be either chosen by the voter or close to uniformly distributed among all possibilities;
4. If some of the ballots are modified after being cast, voters should have a constant probability of being able to find out and prove that there was a modification;
5. A voter should not be able to prove there was a modification when there wasn't, even if their initial ballot was not correctly filled;
6. Finally, the whole system should not depend on any one electronic or human agent that could change the meaning of any ballot or count unnoticed [5].

The above constraints have to be supplemented by some additional concerns which are crucial to any voting system, not just the ones considered here. The voters should be comfortable with the ballot, with its use, and be reasonably confident whether they have used it correctly. They should also know how to spoil their ballot and get a replacement one if they make a mistake. Finally, they should have confidence in the fact that they voted correctly and that their vote is private and secure.

This forms a part of the main goal, which is then to optimise usability and simplicity while satisfying the constraints. With this said, we can present the first protocol.

3 Translucent ballot

3.1 Protocol

This first protocol uses a ballot on which voters can write. The design, as indicated in Figure 1, has three similar single ballots side by side, with one receipt under the left ballot. Each ballot has four different parts:

- A central translucent rectangle split in two cells, one of which the voter has to cover by marking over it;
- A legend over each cell, indicating which candidate it corresponds to;
- A single unique but not memorable ballot segment identification method – here a bar code – under the translucent rectangle;
- A single green dot in the top right corner of the left ballot.

The receipt has a fully transparent rectangle in the same position, but otherwise the elements are the same as in the left ballot with the vertical order reversed, with the bottom of the receipt being slightly narrower and longer. When folded over, rectangles should be aligned with each other, and the green dot should be visible, with the bottom of the receipt protruding, to be removed after the voter casts their ballots.

The instructions for the voter are as follows:

- Choose whether you want to audit your ballot for A or B, colour the corresponding cell on the left ballot, and make an X on the corresponding cell on the receipt. colour the cell corresponding to the other option on the right ballot.
- Choose whether you want to vote for A or for B, and colour the corresponding cell on the central ballot.
- Fold the three ballots horizontally, leaving the central ballot between the two others.
- Fold the receipt vertically on the same side as the ballot it's attached to.
- You should end up with a single stack of ballots, with no visible bar code and a green dot visible in one corner.

The instructions can be indicated directly on the ballot in the space left (if there is enough space, which depends on ballot size), both textually and diagrammatically to avoid language issues. Alternatively, it could also be printed on the remaining space if rectangular sheets are used, but that creates security risks if one isn't careful[6].

The ballot must have the following properties:

- On both ends of the stack, there is a single cell that is entirely coloured. This cell is different on each end. Other than the cell, ballots on each end aren't marked.
- On one side, an X is superimposed on the coloured cell, and a green dot is visible in the corner.

[5] We can reasonably assume that some voting officials should be honest, which introduces redundancy for counting, and each of the steps should be corroborated by a group such as one representative from each party and one election official.

[6] For example, having a full rectangle and not an L-shape makes the folding more complicated, and introduces the problem of how to handle having translucent cells inside the instructions. As those cells could be coloured or not, the complexity of the ballot and the number of variables to check to prevent double-voting increases.

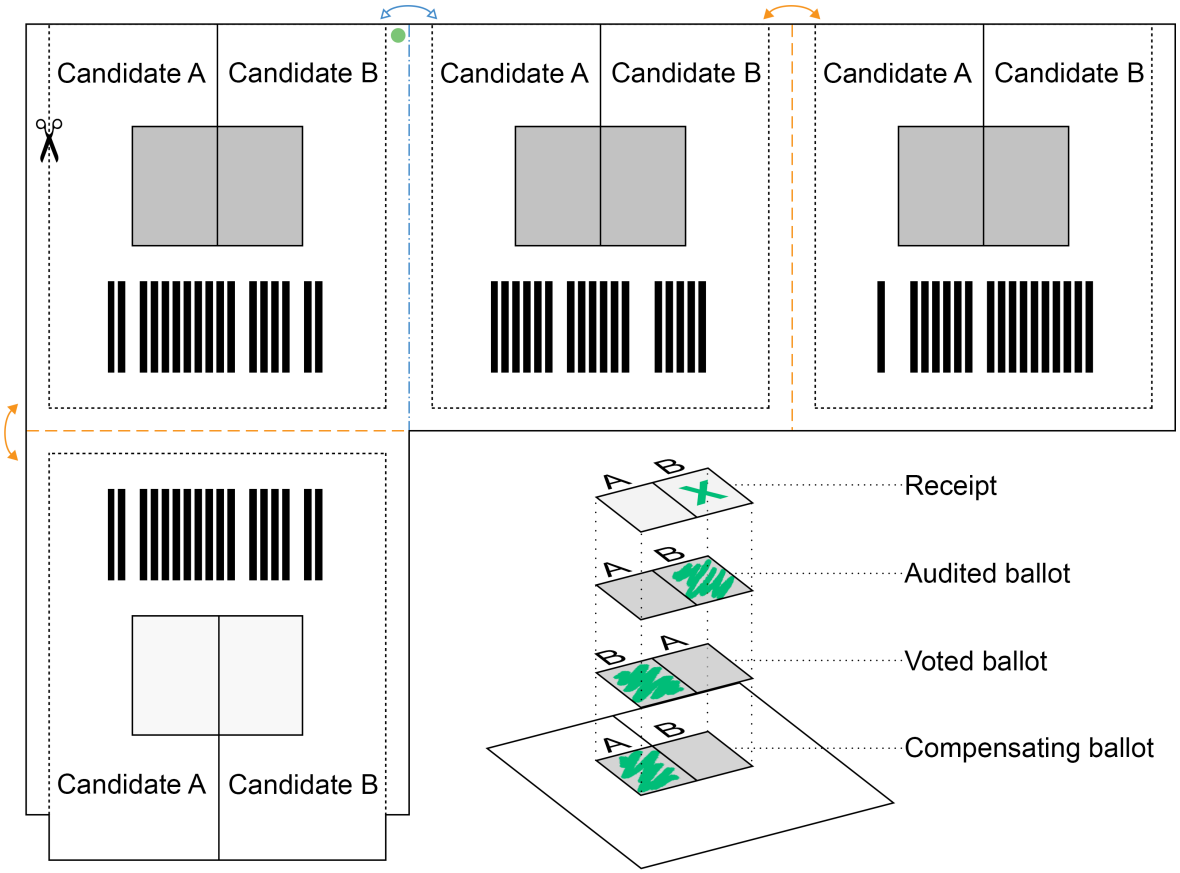

Figure 1: The translucent ballot and on the bottom right a view of the superposition of the translucent rectangles when folded. The three ballots and the receipt are separated by solid lines which correspond to the folds. Once folded, all the cutting lines are aligned with the receipt sticking out, allowing the voter to keep a receipt that allows them to know their ballot was included. The ballots are simultaneously cut and dropped in the ballot box. The only difference between the three ballots lies in the green dot which is cut off in this process.

Once this is done, the ballots are separated from each other with a paper guillotine, along the dotted lines. The ballots are all cast into a ballot box[7] and the voter keeps their receipt. The ballots are then all mixed and revealed to the public (which can be scaled by scanning them and putting them online, this electronic part being independent of the vote).

3.2 Constraint satisfaction

We can now check the six constraints:

1) To check the first property, the officials make sure that there is at least one ballot that is for A, and one for B. The last ballot doesn't matter, as it is either valid (a vote for one candidate), blank or entirely coloured, and the last two options make no difference. Thus, the voter can't give a 2-vote advantage to a candidate.

2) Because the rectangle is translucent and there is at least one fully coloured cell in the stack, if the correct materials are chosen, there should be no way to discern whether it is the second or the third layer that is coloured. Thus, finding whether the central ballot is for A or B should not be doable.

4) The receipt is a copy of the chosen ballot, with the same bar code. As long as ballots with receipts aren't identifiable from other ballots, if a ballot is modified, the receipt has a 1/3 probability of being able to prove as much.

3) and 5) The voter chooses whether they keep a receipt for A or B. However, because the green dot has to be visible, the X mark and the coloured cell right underneath have to correspond to the receipt and the left ballot.

Constraint number 6) is satisfied as there is no need for any device that could monitor or alter the vote, except potentially for the publication – which is partially independent of the vote – where it can be done in parallel to publicly accessible ballots.

[7] To prevent problems between those two steps, the guillotine can be integrated with the ballot box.

3.3 Design choices

Multiple design choices are relevant in this ballot, while some are of no importance. The first important one is the barcode, which can be considered poorly usable as it is not human-readable. However, this is a feature in this context, as the barcode is there to ensure three properties. The first is that every ballot should be unique (easily done with a barcode). The second is that it should be easy to check that the one on the receipt and on the corresponding ballot are identical, which is done here by aligning them. Finally, it should be very hard for the voter to keep receipts for all three ballots. If the unique identifiers were human-readable, and easy to remember or copy, it would be much easier to coerce the voter into keeping receipts for all three, for example, by writing them down discreetly[8]. Other kinds of unique identifiers could be used, as long as they verify those properties.

The green dot, on the other hand, can be changed, as long as there is one feature that ensures that the receipt and the left ballot are on the same side while not being present on the ballots that are cast in the end to prevent identifying which ballot has a receipt.

Unlike some versions of Three-Ballot, the voter does not choose which ballot to keep a receipt for, but instead has an imposed ballot with a receipt on which they vote however they want (there is a small difference analysed at the end of the paper).

4 Taped ballot

4.1 Protocol

This is a variant of the previous ballot design which uses masking tape and string. Instead of colouring multiple translucent cells independently, which can lead to making some mistakes, the voter has to tear off two sets of masking tape, the pieces in each set being linked by some string as can be seen on Figure 2. Like with the other systems in the paper, the strings also operate as a memory aid and a guide to understanding the system and performing the procedure reliably.

In this design, the translucent rectangles are replaced by rectangular holes in the ballot, covered by masking tape. The receipt has a slightly larger hole, with two strips of diagonal masking tape that shows both sides of the underlying rectangle when removed.

The instructions are simpler, as the voter has to make only two actions: choose and tear off the tape of their choice on the central ballot (corresponding to their vote), and choose and tear the one they want to audit as well as the ones it is attached to.

[8] Some humans can read barcodes, but it is quite harder to coerce and train someone into reading one without error and then remembering the result than into simply writing down a number.

4.2 Constraint satisfaction

When it comes to constraint 1), the official just has to make sure that, beneath the hole of the receipt, the left ballot only has the corresponding piece of tape removed, which is visible thanks to the fact that the tape covering the hole is not aligned with the tape underneath, being diagonal.

Constraint 2) is satisfied because the official can check that, on both sides of the ballot, a single piece of tape has been removed.

As this design is very similar to the previous one, it fulfils constraints 3), 4), 5) and 6) for the same reasons, but it also has different properties, analysed further down.

4.3 Design choices

The main goal of this design is to lower the probability of mechanical user error that comes from having a succession of actions to do in the previous design. The strings (which should be of a single colour, unlike on Figure 2) are but one method of linking together each set of masking tape. Once again, this seemingly non-optimal choice comes from the constraint of having all ballots indistinguishable when cast. Using alternatives like partially adhesive stickers or tear tape might make it simpler and more usable, but creating a tape pattern that links each set while keeping the ballots indistinguishable is a complex endeavour. Having symmetrical tape patterns on a recto-verso ballot is another option, but also decreases the usability. With this design, each ballot cast has a single piece of tape attached with a string that is cut at one end, not revealing whether it was a left ballot or not. It is important that the labels on each strings are indistinguishable (Audit or Vote, instead of Audit A/Audit B). This is to ensure that they can hang outside the ballot during the cutting/casting process, preventing the ballots inside from being distinguishable while not allowing officials near the ballot box to check what the voter chose.

5 Punched ballot

5.1 Protocol

This last ballot stems from a different design, that seeks to reduce the user burden by making it simpler for the voter. In this case, the voter makes a single action to get their selection. In its simplest form, an already folded ballot is given to the voter who goes in a privacy booth. There, they can examine it – and unfold/refold it if wanted – before inserting it in a metal frame. They then come out of the booth where an official checks that the frame is correct, before punching a hole in the zone corresponding to the candidate of their choice. The ballots are then separated and cast by cutting them away as with the previous methods, while the voter keeps their receipt.

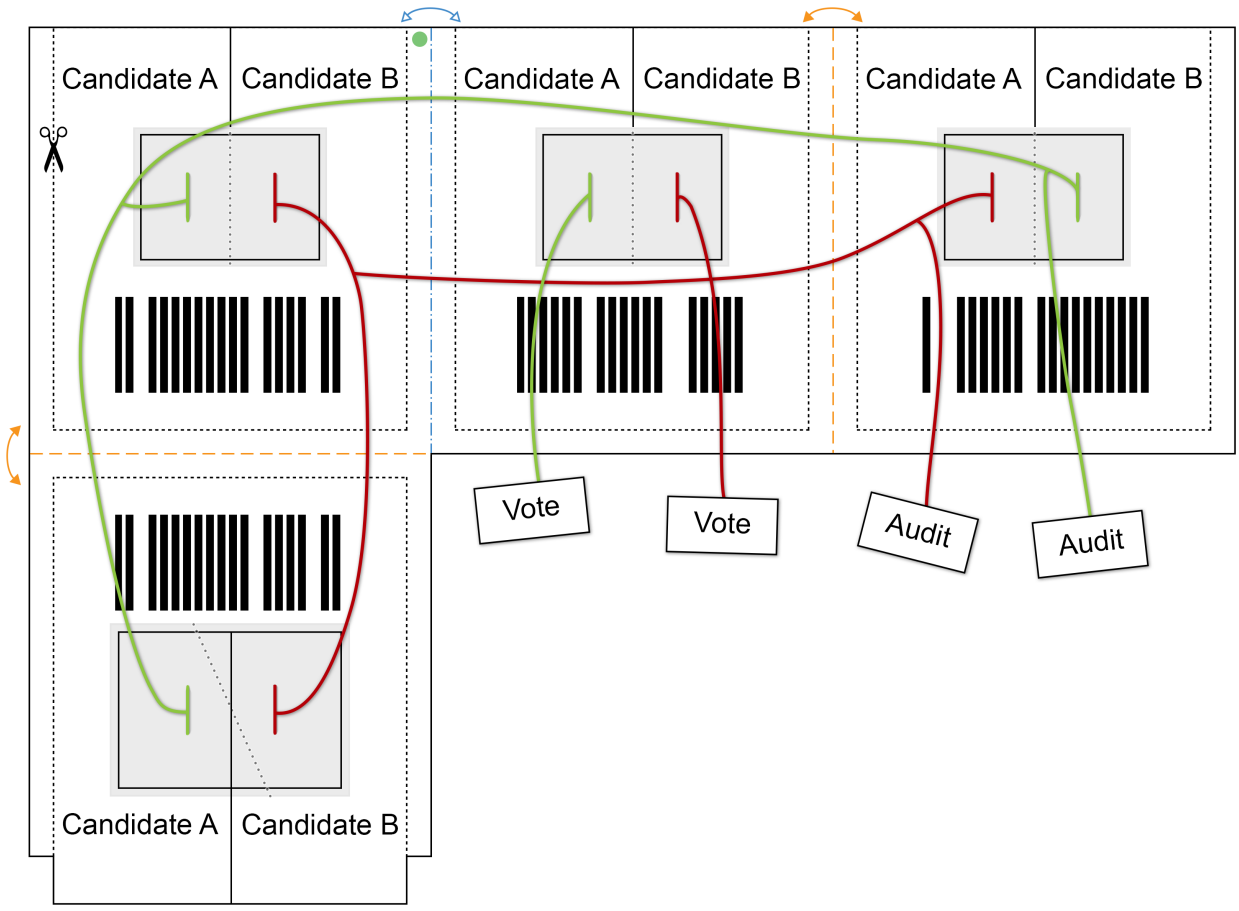

Figure 2: The taped ballot. Four strings are visible (in different colours here for ease of understanding), attached to different pieces of tape covering holes in the ballots. The voter picks one of the two audit strings and removes all corresponding tapes (by pulling the string), and does the same with one of the two voting strings before folding the ballot as in the previous protocol. As the holes in the receipt are bigger, it makes it easy to check that the receipt corresponds to the left ballot.

As the other two proposed candidates, the ballot has three main parts and the receipt. By folding along the lines, the voter can align the three ballots in two different ways, such that two ballots are facing one way or the other. This means that, when they punch a hole, they give two votes to one candidate or the other.

If the ballot does not come pre-folded, the voter starts by doing the mandatory folding (which corresponds to folding, in turn, over line 5 and then line 4, each time leaving the central ballot on top). Two options are then possible. Either the left ballot will be facing the same direction as the central ballot, in which case punching A on this side results in two votes for A, or it will be facing the other direction, in which case, because of symmetry, punching A results in two votes for B. For the first option, the voter starts by folding line 3 over the central ballot, and then line 1 to leave the left ballot on top. For the second option, they simply need to fold line 2 below the central ballot.

Voting with a folded ballot means that there is an excess of paper on one side, which is to be hidden by the metal frame (to preserve the secrecy of on which side there is an excess of paper, which indicates which way the ballot is folded).

5.2 Constraint satisfaction

Constraint 1) depends on the voter not having the opportunity to unfold the ballot and punch holes on the unfolded ballot inside the privacy booth. As long as this is true, a single hole is punched, which, because of the folding, creates at least one ballot for A and one for B. If it is possible to unfold the ballot and fold it differently (not aligned with the folding lines for example), it becomes necessary to check alignment with the metal frame. This can easily be done through the protruding bits at the top of the ballot.

Constraint 2) is satisfied as, once the ballot is folded and set

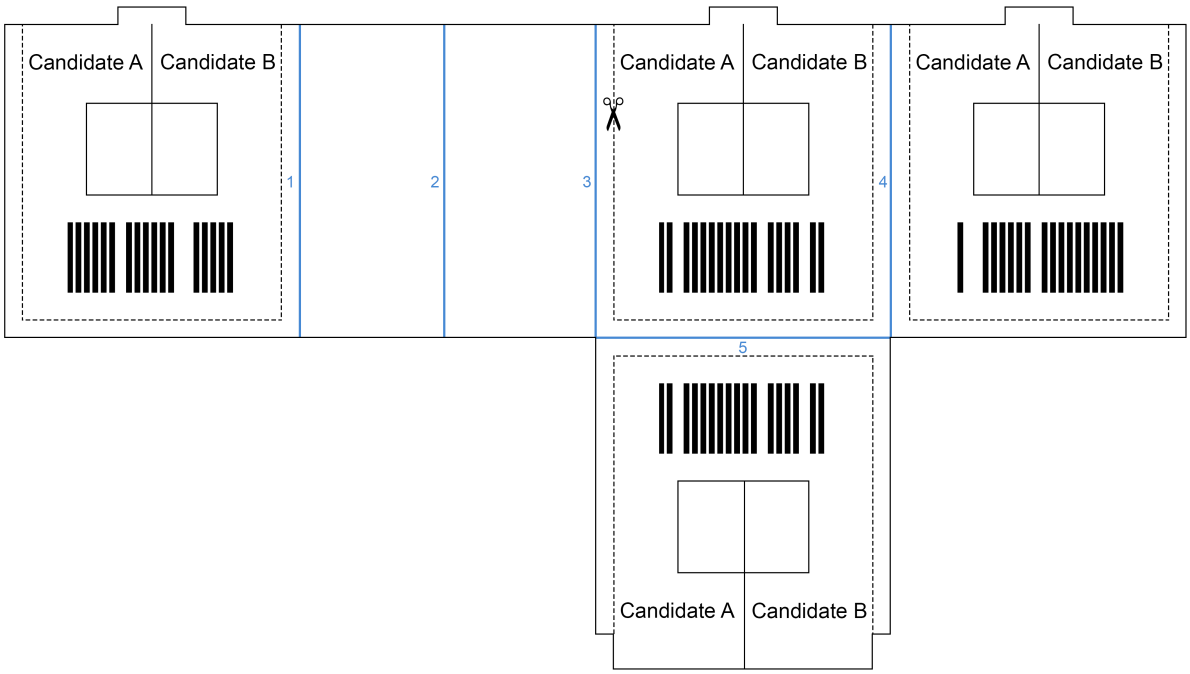

Figure 3: The punched ballot before being folded. The voter starts by folding lines 4 and 5, in the order of their choice, leaving the central ballot on top. They can then fold either 2 behind the central ballot or 1 behind and 3 on top of the central ballot. They then end up with a stack of ballots with the central rectangles aligned, the receipt sticking up at the top, and empty white paper on either the left or the right.

into the frame, there is no way to know how the third ballot hidden inside is oriented, and the visible holes are always one for A and the other for B.

Constraint 5) is satisfied as the receipt corresponds, by the necessity of the folding, to the central ballot. Constraint 3) is satisfied because the voter can choose to fold one way or another, which, combined with their choice of vote, determines which hole is punched on the receipt. The other constraints are satisfied as with the previous two solutions.

6 Advantages and drawbacks of the solutions proposed

The translucent design has multiple advantages:

- The voter can easily choose which ballot to audit, as with the masked ballot.
- It allows concurrent elections by having multiple voting rectangles aligned vertically (present on the receipt in reverse order).
- It is quite familiar to many voters – or at least more so than the masked ballot.
- The correctness of the ballot can be checked by a voting official or a machine that simply measures the intensity of light reflected through the translucent rectangle.
- It is easy to fold it correctly.

It also has a few drawbacks:

- The folding instructions are non-trivial.
- While the voter isn't saddled with voting multiple times for a race, the folding confronts the voter with the complexity of the Three-Ballot system.
- It requires the officials to check for translucency.
- If the rectangle is big, it might be possible to identify the vote if they are not entirely coloured.

The masked ballot has similar features, but removes some of the complexity by leaving two choices: vote A or B, and audit A or B, and pull the corresponding strings. The drawbacks are that it requires more complex (and expensive) ballots, and cannot be extended to concurrent races. Manufacturing issues for the masked ballot are nontrivial and could become a source of confusion and error if the adhesive or strings have any uncertainty. This approach is the most open to partially or completely unreadable ballots due to to problems such as hanging chads, as it depends on adhesives to work and strings not to be snagged incorrectly.

The punched ballot is – for the voter and the officials – the simplest of the three systems, requiring only one step to set up the ballot and one step to vote. It removes the direct choice of who to audit by making it dependent on the orientation of the frame. If it comes pre-folded, all there is to do is orient it carefully and punch the correct hole. However, there are known problems with punched ballots [5, 19], and this system also requires a bit more equipment.

7 Attacks on the proposed systems

The main attacks against Three-Ballot concern either multiple races on a single ballot [10, 18] or small numbers of voters [1]. The first is avoided here by having a single race per ballot – as is already the case in a number of voting systems. The second is mostly a matter of choosing where to use this technology.

However, the designs shown here make certain new attacks possible. For example, in certain cases, the receipt is easy to see for a voting official. However, even knowing which voter has what kind of receipt does not allow an adversary to arbitrarily change votes, as they still have no information on which ballot belongs to whom. It can only inform them when a very small proportion of voters kept a receipt for candidate A, making the attack shown in [1] a bit easier. This attack is especially relevant on the first two designs due to the green dot and the fact that the official is effectively checking whether the voter is auditing A or B. As they cannot simultaneously see the barcodes, it is a limited flaw.

A much more significant attack depends on the printing of the ballots. As the voter does not choose which ballot (and hence which unique identifier) gets a receipt, knowing all the barcodes on the left-side ballot gives an adversary knowledge over which barcodes are safe to modify and which aren't. There is thankfully a fix: when picking the ballot the official gives the voter three pairs of barcodes on stickers. They then watch as the voter puts both stickers from one pair on the left ballot and the receipt, and one sticker from each of the two other pairs on the remaining ballots, before shredding the two stickers left. As the barcodes are not human-readable, this method should be safe unless the process is systematically filmed with good cameras.

In parallel to this, to check that the printing process happened correctly, there should be the option of taking whatever ballot sheet is given to the voter and putting it in a pile to be audited (either by voter choice or randomly assigned), before giving them another ballot sheet. In the case of barcode sticker, this should happen after they are pasted on the ballots. The discarded ballots can be checked publicly after the election to make sure that they weren't manipulated, and should of course be held securely in the meantime.

This brings us to what is a real vulnerability that is generally hard to address: it is possible to prove that one voted one way by filming the whole process, which is becoming increasingly relevant in the age of ballot selfies [20]. There are once again solutions, as long as the voter – or the person spying on them – can't film continuously out of the privacy booth. The first is allowing users to get back to the ballot distribution table, spoiling their ballot, and start the whole process again (making what happened the first time in the privacy booth irrelevant). The second can be done with the third design, where only the folding and inserting of the ballot in the frame is done in the privacy booth. Once outside, the voter can easily flip the frame, and vote differently.

8 Discussion

Cryptographic solutions to improve security typically come at a huge cost to usability, and sometimes even at the cost of accuracy. They often require careful encoding and multiple confusing actions. Moreover, most of the systems based on Three-Ballot left behind the initial paper-based advantage to use more involved electronic devices. With the systems proposed in this paper, we sought to provide an alternative that requires no technology more complex than a hole puncher. The systems all have different properties, but they seek to make the inner workings of Three-Ballot more visible and understandable, to confront the voter and give them a better model of the process, which can increase both compliance and performance when dealing with secure systems [32].

Two main questions remain:

- How does one accommodate races with many different candidates while keeping usable simple ballots?
- What is the simplest way to handle many concurrent races?

For the former, the designs shown here can potentially be adapted to one or two more candidates, but one quickly gets to the geometric limits of paper folding. For the latter, the simplest solution is to make voters vote for each race independently, casting ballots and getting new ones repeatedly. There is also the possibility of having a long strip of ballots all attached to each other, but care has to be taken to prevent someone mixing and matching: parts of one ballot could be used to give a multiple-vote advantage on another race.

The exercise of designing such ballots is one way this paper proposes to push opportunities for secure ballots forward, opening the possibility of further designs which explore more complex folding and geometrical patterns. The other is that this paper presents actual usable ballot designs that could be deployed today to greatly increase the actual security and integrity of secret ballots for voters, although this is always a complex endeavour [2]. The original author of three ballot voting was sceptical about its practicability; this paper, then celebrates that Three-Ballot voting can be used by people in a simple and verifiable way.

References

[1] Andrew W. Appel. How to defeat rivest's threeballot voting system. 2006.

[2] Nikola K. Blanchard and Ted Selker. Improving voting technology is hard: the trust-legitimacy-participation loop and related problems. In *2018 Workshop on Socio-Technical Aspects in Security and Trust, STAST , San Juan, Puerto Rico*, 2018.

[3] Christian Borghesi, Jean-Claude Raynal, and Jean-Philippe Bouchaud. Election turnout statistics in many countries: similarities, differences, and a diffusive field model for decision-making. *PloS one*, 7(5), 2012.

[4] Philip Boucher. What if blockchain technology revolutionised voting. *Unpublished manuscript, European Parliament*, 2016.

[5] Charles S. Bullock, III and M.V. Hood III. One person - no vote; one vote; two votes: voting methods, ballot types, and undervote frequency in the 2000 presidential election. *Social Science Quarterly*, 83(4):981–993, 2002.

[6] Miguel Carreras and Yasemin İrepoğlu. Trust in elections, vote buying, and turnout in latin america. *Electoral Studies*, 32(4):609–619, 2013.

[7] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE security & privacy*, 2(1):38–47, 2004.

[8] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L Rivest, Peter YA Ryan, Emily Shen, and Alan T Sherman. Scantegrity ii: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. *EVT*, 8:1–13, 2008.

[9] David Chaum, Aleks Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan Sherman, and Poorvi Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46, 2008.

[10] Jacek Cichoń, Mirosław Kutyłowski, and Bogdan Węglorz. Short ballot assumption and threeballot voting protocol. In *International Conference on Current Trends in Theory and Practice of Computer Science*, pages 585–598. Springer, 2008.

[11] Daniela Donno and Nasos Roussias. Does cheating pay? the effect of electoral misconduct on party systems. *Comparative Political Studies - COMP POLIT STUD*, 45:575–605, 05 2012.

[12] Chantal Enguehard and Jean-Didier Graton. Machines à voter et élections politiques en france: étude quantitative de la précision des bureaux de vote. *Cahiers Droit, Sciences & Technologies*, 4(4):159–198, 2014.

[13] Timothy Frye, Ora John Reuter, and David Szakonyi. Hitting them with carrots: Voter intimidation and vote buying in russia. *British Journal of Political Science*, pages 1–25, 2018.

[14] Daniela Giannetti. Secret voting in the italian parliament. *Secrecy and publicity in votes and debates*, pages 108–130, 2015.

[15] Ezequiel González-Ocantos, Chad Kiewiet de Jonge, and David W. Nickerson. Legitimacy buying: The dynamics of clientelism in the face of legitimacy challenges. *Comparative Political Studies*, 48(9):1127–1158, 2015.

[16] Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting recording system design. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pages 1–6. IEEE, 2017.

[17] Michael J. Hanmer, Won-Ho Park, Michael W. Traugott, Richard G. Niemi, Paul S. Herrnson, Benjamin B. Bederson, and Frederick C. Conrad. Losing fewer votes: the impact of changing voting systems on residual votes. *Political Research Quarterly*, 63(1):129–142, 2010.

[18] Kevin J. Henry, Douglas R. Stinson, and Jiayuan Sui. The effectiveness of receipt-based attacks on threeballot. *IEEE Transactions on Information Forensics and Security*, 4(4):699, 2009.

[19] Michael C. Herron and Jasjeet S. Sekhon. Overvoting and representation: An examination of overvoted presidential ballots in broward and miami-dade counties. *Electoral Studies*, 22(1):21–47, 2003.

[20] Daniel A. Horwitz. A picture's worth a thousand words: Why ballot selfies are protected by the first amendment. *SMU Sci. & Tech. L. Rev.*, 18:247, 2015.

[21] Andrea Huszti. A secure electronic voting scheme. *Periodica Polytechnica Electrical Engineering*, 51(3-4):141–146, 2008.

[22] Douglas W. Jones and MacLean Hall. Technologists as political reformers: Lessons from the early history of voting machines. In *Society for the History of Technology Annual Meeting, Las Vegas*, volume 13, 2006.

[23] Harvey Jones, Jason Juang, and Greg Belote. Threeballot in the field. 2006.

[24] Changwook Ju. "you can't hack a piece of paper": Jake braun talks us election security. *Chicago Policy Review (Online)*, 2018.

[25] W.-S. Juang and Chin-Laung Lei. A secure and practical electronic voting scheme for real world environments. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, pages 64–71, 09 1997.

[26] Horacio Larreguy, John Marshall, and Pablo Querubin. What is the effect of turnout buying? theory and evidence from mexico. *Harvard University (Cambridge, MA). Unpublished manuscript*, 2014.

[27] Justin Levitt. The truth about voter fraud, 2007.

[28] Verlaat Maike. The portrayal of russia in us media in the aftermath of the 2016 election hacking scandal. Master's thesis, 2018.

[29] Mark McKenna. *Building 'a closet of prayer" in the new world: the story of the 'Australian ballot'*. 2001.

[30] Worth Robert Miller. Harrison county methods: Election fraud in late nineteenth-century texas. *Locus*, 7:111–28, 1995.

[31] Teogenes Moura and Alexandre Gomes. Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th Annual International Conference on Digital Government Research*, dg.o '17, pages 574–575, New York, NY, USA, 2017. ACM.

[32] F. Mwagwabi, T. McGill, and M. Dixon. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In *2014 47th Hawaii International Conference on System Sciences(HICSS)*, volume 00, pages 3188–3197, 1 2014.

[33] Simeon Nichter. Vote buying or turnout buying? machine politics and the secret ballot. *American political science review*, 102(1):19–31, 2008.

[34] Hilarie Orman. Secure voting: A call to arms. *IEEE Internet Computing*, 21(5):67–71, 2017.

[35] Andrew Reynolds and Marco Steenbergen. How the world votes: The political consequences of ballot design, innovation and manipulation. *Electoral Studies*, 25(3):570–598, 2006.

[36] Ronald L. Rivest and Warren D. Smith. Three voting protocols: Threeballot, vav, and twin. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, EVT'07, pages 16–16, Berkeley, CA, USA, 2007. USENIX Association.

[37] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE transactions on information forensics and security*, 4(4):662–673, 2009.

[38] Altair O. Santin, Regivaldo G. Costa, and Carlos A. Maziero. A three-ballot-based secure electronic voting system. *IEEE Security & Privacy*, 6(3):14–21, 2008.

[39] Ted Selker and Sharon Cohen. An active approach to voting verification. Technical report, Caltech/MIT Voting Technology Project, 2005.

[40] Sarah M. Sled. Vertical proximity effects in the california recall election. Technical report, Caltech/MIT Voting Technology Project, 2003.

[41] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and Alex J. Halderman. Security analysis of the estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715. ACM, 2014.

[42] Geordie Stewart and David Lacey. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1):29–38, 2012.

[43] C. E. Strauss. A critical review of the triple ballot (3ballot) scheme, part 1. 2006.

[44] C. E. Strauss. A critical review of the triple ballot voting system, part 2: Cracking the triple ballot encryption. 2006.

[45] Yusuf Uzunay and Kemal Bicakci. Trusted3ballot: Improving security and usability of three ballot voting system using trusted computing. In *Intelligent Systems, Modelling and Simulation (ISMS), 2014 5th International Conference on*, pages 534–539. IEEE, 2014.

[46] Kristjan Vassil, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel, and Michael R. Alvarez. The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. *Government Information Quarterly*, 33(3):453–459, 2016.

[47] Priit Vinkel. *Remote electronic voting in estonia: legality, impact and confidence*. TUT Press, 2015.

[48] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. Large-scale election based on blockchain. *International conference on identification, information and knowledge in the internet of things*, 129:234–237, 2018.