Origami voting: a non-cryptographic approach to transparent ballot verification

Enka Blanchard, Ted Selker

Origami voting: a non-cryptographic approach to transparent ballot verification

Enka Blanchard[1] and Ted Selker[2]

[1] Digitrust, Loria, Université de Lorraine
Enka.Blanchard@gmail.com, www.koliaza.com
[2] bbbbUMBC
ted.selker@gmail.com, http://ted.selker.com/

Abstract. Over the past four 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 hard to understand cryptographic protocols, which can affect whether users actually verify their selections. Three-Ballot and Vote/Anti-Vote/Vote, two related systems among the few non-cryptographic end-to-end verifiable voting systems, made improvements in security while eliminating complex protocols. They unfortunately suffered from usability issues, and although they did not require cryptographic primitives, they still relied on electronic devices. To address this, we introduce three folded-paper based systems that allow verifiable voting and resist common attacks despite not relying on any cryptography or electronic devices. The proposals are based on 1) semi-translucent ballots, 2) masking tape, or 3) folding and punching. These Origami voting methods help users understand the underlying mechanisms and give them a direct geometric approach to verification.

Keywords: Usable security, Voting systems, Verifiable voting, Low-technology.

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 [24] to demonstrations with every manner of new technology — exemplified in recent years with blockchain voting, although its advantage over established verifiable voting systems remains to be proved, especially since the technology has not been around long enough to be thoroughly tested [5,34,50]. The introduction of new approaches for voting is often slow, as 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" [3]. 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*" [32]. 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 [24]. This proposed secrecy has been the source of arguments from both citizens and party leadership, sometimes aimed at keeping an elected official beholden to their promises [15], 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 re-counting ballots are well-publicised, leading to a slew of systems that produce both a mechanised or electronic tally and an auditable record ballot (that are rarely checkable or checked by voters), from lever machines to optical scan methods [6]. The design challenges of helping the voter secure voting systems though audits are evident in systems such as secret-ballot receipts [8], Scantegrity [9,10] — an end-to-end independent verification system that coexists with a normal ballot — or audio audit trails [41], which improve the usability of auditing. Others require changing the infrastructure by using electronic-only systems [17,27,22], sometimes not even requiring polling places but instead some forms of e-identification [43,49].

All the systems mentioned try to improve accuracy, integrity, and prevent coercion, miscounting, ballot box stuffing and related fraud, generally through difficult to understand means. Those problems have been central to election security since the late 19th century [33], but some of the focus has now shifted to other considerations[3] [16,29,2]. First, manipulation of voter registration lists [7], accessibility of voting [4] and turnout buying [29] can have stronger impacts than the previously mentioned problems [36,30,6]. Second, familiarity with the voting system is essential[4], and technological changes without adequate training generally come with a strong temporary increase in error rates [18,20].

With people being increasingly concerned with the threat of election hacking [31] — and legitimately so [43] — a number of experts have warned about the lack of adequate technology [37]. There is also a strong pressure to return to low-tech, non-electronic systems, as it is supposedly much harder for an external adversary to massively manipulate them [26]. Unlike the USA, some countries such as France or Switzerland did not mechanise their voting systems and still use paper ballots massively with little evolution in voting practice in more than a century [13]. Some European countries are also considering or implementing moratoriums on using electronic devices at any point in the voting process. Avoiding electronics and cryptography altogether poses a problem for most of the newly developed end-to-end verifiable voting systems that guarantee the authenticity and anonymity of all ballots.

To address these issues as well as the mechanical and cognitive difficulties of making correct selections, we propose origami voting, a set of systems inspired by Ron Rivest and Warren Smith's two related Three-Ballot and Vote/Anti-Vote/Vote (VAV) systems[5] [39]. Three-Ballot and VAV systems both use a set of three ballots to guarantee anonymity and verifiability. Those protocols have many variants, but the simplest — which we'll briefly describe — apply to 2-candidate races. 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 — two of which compensate for each other by giving votes to both candidates — the voter gets a receipt for one of them, showing who it is for and

[3] Luckily today, in most major elections in western democracies the error rate is generally at least one order of magnitude lower than the margin of victory [13]. Easily identifiable bold-faced fraud is still extant in many countries such as Russia [14], Honduras [16] or Albania [12]

[4] Co-existence of redundant systems is possible, as in Estonia, but have an adverse effect on the adoption rate [48].

[5] To be precise, the design of our Origami ballots is closest in appearance to VAV, but the underlying mechanisms are closer to the original Three-Ballot proposal.

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 Three-Ballot and VAV proposals 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 well studied in a variety of articles [1,19,46]. Although it poses a real risk in places with many concurrent races[6], many countries — such as Spain, Greece, France or Malawi [38] — don't have many concurrent elections, and this article will focus on this case (called the Short Ballot Assumption in the original articles).

A second weakness of Rivest and Smith's systems has been the high complexity and poor usability for the voter, not only in the practical implementation [25,45] but also because of the many steps necessary to correctly use the scheme — here requiring voters to accurately vote 3 times, once against their the candidate they favour – which is known to make it harder for voters to use correctly [44]. Finally, the system relies on the assumption that the ballots are all correctly filled and checked, which is dependent on the separate step of scanning and validating the ballots with a machine without storing them. This introduces a vulnerability coming from the use of potentially insecure hardware, and all the proposed solutions so far rely on external electronic remedies either through trusted hardware [47] or online services [40,28].

Contributions. We propose three candidate designs that enforce that the ballots are correct (and cast as intended) through mechanical and perceptual means. They extend previous non-cryptographic end-to-end verifiable voting approaches by reducing the selections to one step and removing the need to be checked by a separate device. The first protocol 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 protocol 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" [21]. As with the original schemes, 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 such external systems. 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 and proves that they are a registered voter (e.g. by showing the relevant ID).

[6] 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 [42].

- They are given instructions as to how to vote[7];
- Voters 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;
- They cast their ballot by inserting it into a ballot box.

Moreover, the protocols should satisfy the following constraints, in no specific order of importance (as some of these are equally necessary):

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 must be no way for a third party to find out a particular voter's vote, and allow no way for a voter to prove that they voted a particular way;
3. As a consequence of the previous constraint, if a receipt is given that indicates a specific vote, the vote indicated on it must 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 must have a constant probability of being able to find out and prove that there was a modification;
5. A voter must 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 must not depend on any single machine or human agent that could modify any ballot or count unnoticed [8].

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 must be comfortable with the ballot, with its use, and be reasonably confident whether they have used it correctly. They must also know how to spoil their ballot and get a replacement one if they make a mistake. Finally, they must have confidence in the fact that they voted correctly and that their vote is private and secure.

All the ballots in the protocols shown here also assume that there is a single election, and no concurrent races.

These constraints support the main goal: to optimise usability and simplicity while a voter creates an accurate verifiable ballot that requires no electronic devices.

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:

[7] As has been suggested [18], 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.

[8] 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.

- 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 barcode — 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.

One important thing to note is that the barcodes are not initially present on the ballot. Instead, during a preliminary phase before going into a voting booth, the voter receives the ballot sheet without barcodes, and a sheet of three pairs of identical barcode stickers. They can then choose which pair goes on the first ballot and the receipt, and paste them in the appropriate places, then take one from each other pair, paste them on the ballot sheet, and shred the two remaining stickers. The whole process should happen under supervision, just to make sure that the ballots are correctly pasted in a way that does not make the ballots identifiable, and that the receipt barcode corresponds to the one above.

The instructions for the voter are as follows:

- Select a pair of identical barcode stickers from the three pairs and stick them on the leftmost ballot and the receipt in the indicated region. Then take one from each of the other two pairs and stick them on the corresponding zones on the central and right ballots.
- Choose whether you want to audit your ballot for A or B, colour the corresponding cell on the left ballot. 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. Both cells will appear to be filled in.
- 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 barcode on the outside and a green dot visible in one corner.

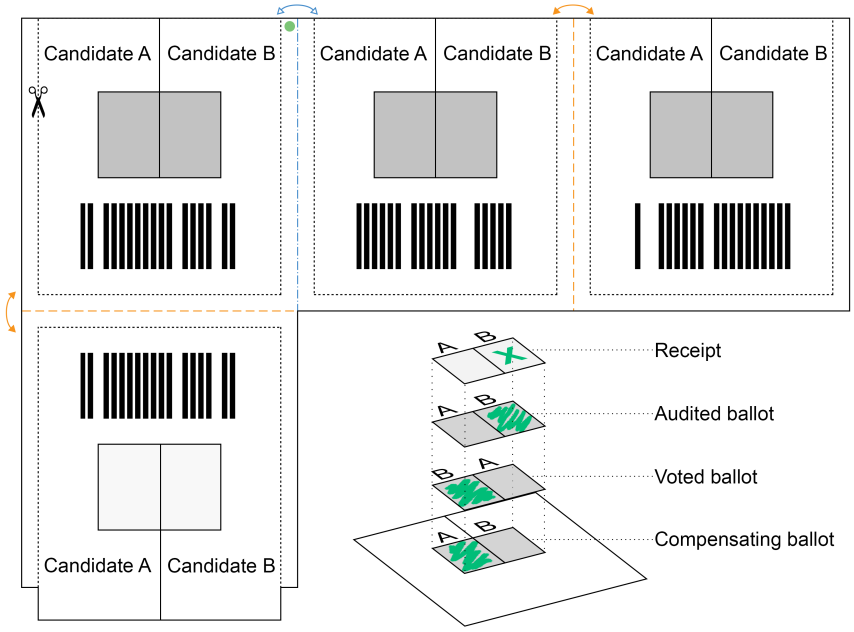

Fig. 1. The translucent ballot and on the bottom right a view of the superposition of the translucent rectangles when folded. The three ballots and the receipt are separated by solid lines which correspond to the folds. Once folded, all the cutting lines are aligned with the receipt sticking out, allowing 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.

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[9].

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.

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[10] and the voter keeps

[9] 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.

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

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, it is not possible to determine whether the central ballot is for A or B.

4) The receipt is a copy of the chosen ballot, with the same barcode. 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. The green dot, which identifies which ballot has a receipt, is discarded in the cutting process, after it is used to check the correctness of the folding.

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.

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 much harder to read and transcribe than even a long number. 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 anyone can do by aligning them. Finally, it should be very hard for the voter to keep receipts for all three ballots. If the unique identifiers were easy to read, to remember or to copy, it would be much easier to coerce the voter into keeping receipts for all three, for example, by writing them down discreetly[11]. Instead of the barcode, it would be possible to use alternative identifiers, as long as they are not easily readable by a human (like a string of characters) while being easy to compare to check that two such identifiers are indeed identical.

Having the barcodes as stickers on a second sheet is costly, but it prevents attacks from someone who has access to the ballot printing process. Knowing all the barcodes on the left-side ballot gives an adversary knowledge over which barcodes are safe to

[11] Some people have learned to read barcodes, but it is much harder to coerce and train someone into reading one, remembering the result or writing it down without error than with serial numbers.

modify and which aren't. As the barcodes are not easily readable, the method shown should be safe unless the process is systematically filmed with good cameras.

The green dot, could be replaced by any way to ensure that the receipt and the left ballot are on the same side (with both folds being performed correctly). Whatever this feature, it must later be absent on the ballots that are cast to prevent identifying which ballot has a receipt.

Unlike in the original schemes, 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 (this difference is analysed at the end of this article).

One potential usability issue is that it could be possible to partially attack the privacy of the vote if the cells are not fully coloured. Considering the existing difficulties in properly marking ballots even with weaker constraints, this could be problematic. This leads us to a second design that ensures a completely filled in ballot.

4 Taped ballot

4.1 Protocol

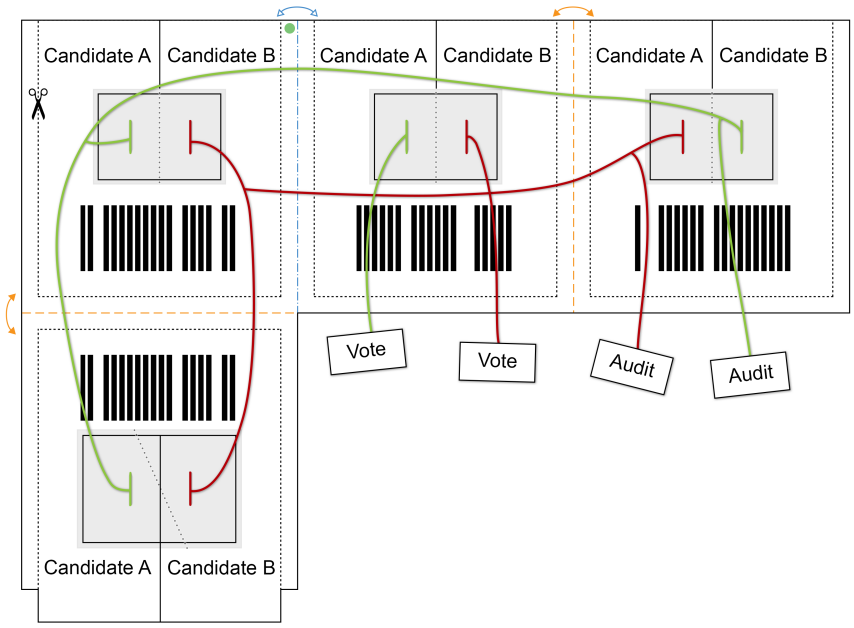

Fig. 2. The taped ballot. Four strings are visible (in different colours here for ease of understanding), attached to different pieces of tape covering holes in the ballots. The voter pulls on one of the two audit strings to remove a set of tapes. They then pull on one of the two voting strings before 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.

This is a variant of the previous ballot design but uses masking tape and string to help with the issue of completely filling the ballot. Instead of colouring multiple translucent cells independently, which can lead to making mistakes, guided by connected strings the voter tears off two sets of masking tape, as can be seen on Figure 2. The strings also operate as a memory aid and physical prosthetic to understanding the system and performing the procedure reliably.

The translucent rectangles of proposal one 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 and the ones it is attached to.

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.

Proposal 2, fulfils constraints 3), 4), 5) and 6) for the same reasons as proposal 1, but it also has different properties, analysed below.

4.3 Design choices

The main goal of proposal 2 is to reduce the selection actions to two, to lower the probability of making mistakes during the several selection actions required with such a multi-ballot system. 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 third proposal stems from a different idea and seeks to reduce the user burden by making it simpler for the voter. In this case, the voter makes a single selection action to

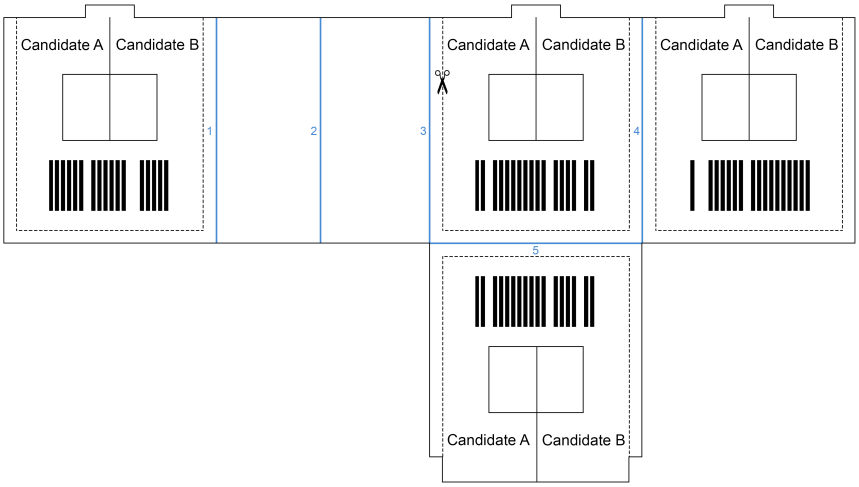

Fig. 3. The punched ballot before being folded. The voter starts by folding lines 4 and 5, in the order of their choice, leaving the central ballot on top. They can then fold either 2 behind the central ballot or 1 behind and 3 on top of the central ballot. They then end up with a stack of ballots with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

get their vote. In its simplest form, an already folded ballot (with barcode stickers pasted) 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.

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 folding : fold over line 5 and then line 4, each time leaving the central ballot on top. Two selection 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 vote 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 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 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.

Constraint 5) is satisfied as the receipt corresponds, by the necessity of the folding, to the central ballot.

Constraints 4) and 6) are satisfied in the same way as the previous two proposals.

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:
- Several steps have to be correctly followed to fold it correctly.
- It requires the officials to check for translucency.
- Both the previous drawbacks increase complexity, putting more pressure on polling stations and potentially increasing costs[12].
- Even when the voter isn't saddled with voting multiple times for a race, the folding confronts the voter with the complexity of Three-Ballot/VAV systems.
- 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 most 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 expensive and difficult to make ballots, and cannot be extended to concurrent races. Quality control in manufacturing the masked ballot could even 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.

[12] From the first author's experience in French polling stations, which already use paper ballots, the main choke-point generally lies with the identity verification process, so the additional time costs could be inconsequential.

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. The frame can aid a blind voter as well. However, there are known problems with punched ballots [20,6], 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 [19,11] 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 proposals 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.

Another attack can target all instances of Three-Ballot derivatives, as well as almost all low-tech paper-based systems. Suppose an adversary can insert some identifying mark in the paper that is not visible to the naked eye (on the fibre texture or with microdots for example). It then becomes possible to both track how someone voted, and find which are the non-tracked ballots that can be safely discarded. Of course, this requires not just the ability to make such marks, but also to check for them during the tallying or examination phases. A weaker version of this attack is also possible. It requires checking the cutting marks on the sides of the ballots to identify whether the ballot was on top or in the middle during the folding and cutting process. If this is reliably noticeable, there is an opportunity to identify tracked ballots. Rivest and Smith's article [39] already addressed this by stating that the ballot scans should be in low-definition. The exact position and orientation of the barcode stickers themselves could also facilitate this kind of attack, although the supervision makes it harder to implement this in practice.

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. This should happen after the barcode stickers are pasted onto 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 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 [21]. 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[13]. The first is allowing users to get back to the ballot distribution

[13] Some countries have tried to prevent such possibilities by banning cellphones in the polling stations and even — in the case of India [23] — in a small radius around them

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 require additional actions by the voter, 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/VAV left behind the initial non-cryptographic design (which was their main advantage) to use more involved electronic devices. The systems proposed in this article sought to provide an alternative that requires no technology more complex than a hole puncher. The proposals above have different properties, but they all seek to make the inner workings of a Three-Ballot/VAV style ballot take the fewest number of steps to be visible and understandable. They give the voter a better model of the process, which increases both compliance and performance when dealing with secure systems [35].

Three main questions remain:

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

The designs shown here can potentially be adapted to one or two more candidates, but with more candidates they will eventually get to the geometric limits of paper folding. The simplest solution to handle many races is to make voters select for each race on separate ballots. 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 we propose to push opportunities for secure ballots forward, opening the possibility of further designs which explore other folding and geometrical patterns. The other is that the protocols shown here present actual ballot designs that could be deployed today to increase the actual security and integrity of secret ballots for voters, even in places that forbid electronic voting. Our three approaches use simple physical actions as verification prosthetics to guide a voter to complete an algorithmic improvement in security and verification of the candidate selection. The original authors of Three-Ballot and VAV protocols were sceptical about the protocols' practicability. This article then celebrates that protocols can be made that help voters see how they made selections, compare their selections to their goals, and verify that the ballots were counted correctly afterwards. The protocols shows that even the very difficult goal of having a voter create and verify complex selections can be tested in a transparent manner by a voter themself. Origami voting is a first demonstration of using simple paper-folding technology to allow a user to successfully fill out a complex multi-ballot, with no use of cryptography or external devices. We are hopeful that this work will encourage many new schemes in this direction.

9 Acknowledgements

We'd like to thank L. Gabasova, the members of the VoteVerif workshop and especially Peter Roenne for their comments. We are also extremely grateful to Josh Benaloh and Peter Roenne for their help with improving this article. This work was supported partly by the french PIA project "Lorraine Université d'Excellence", reference ANR-15-IDEX-04-LUE.

References

1. Appel, A.W.: How to defeat rivest's threeballot voting system (2006), `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.116.5156&rep=rep1&type=pdf`
2. Beaulieu, E.: From voter id to party id: How political parties affect perceptions of election fraud in the us. Electoral Studies **35**, 24–32 (2014)
3. Blanchard, N.K., Selker, T.: 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)
4. Borghesi, C., Raynal, J.C., Bouchaud, J.P.: Election turnout statistics in many countries: similarities, differences, and a diffusive field model for decision-making. PloS one **7**(5) (2012)
5. Boucher, P.: What if blockchain technology revolutionised voting. Unpublished manuscript, European Parliament (2016)
6. Bullock, III, C.S., Hood III, M.: 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)
7. Carreras, M., İrepoğlu, Y.: Trust in elections, vote buying, and turnout in latin america. Electoral Studies **32**(4), 609–619 (2013)
8. Chaum, D.: Secret-ballot receipts: True voter-verifiable elections. IEEE security & privacy **2**(1), 38–47 (2004)
9. Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y., Shen, E., Sherman, A.T.: Scantegrity ii: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. EVT **8**, 1–13 (2008)
10. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., Vora, P.: Scantegrity: End-to-end voter-verifiable optical-scan voting. IEEE Security & Privacy **6**(3), 40–46 (2008)
11. Cichoń, J., Kutyłowski, M., Węglorz, B.: Short ballot assumption and threeballot voting protocol. In: International Conference on Current Trends in Theory and Practice of Computer Science. pp. 585–598. Springer (2008)
12. Donno, D., Roussias, N.: Does cheating pay? the effect of electoral misconduct on party systems. Comparative Political Studies - COMP POLIT STUD **45**, 575–605 (05 2012). https://doi.org/10.1177/0010414011427130
13. Enguehard, C., Graton, J.D.: 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)
14. Frye, T., Reuter, O.J., Szakonyi, D.: Hitting them with carrots: Voter intimidation and vote buying in russia. British Journal of Political Science pp. 1–25 (2018)
15. Giannetti, D.: Secret voting in the italian parliament. Secrecy and publicity in votes and debates pp. 108–130 (2015)
16. González-Ocantos, E., Kiewiet de Jonge, C., Nickerson, D.W.: Legitimacy buying: The dynamics of clientelism in the face of legitimacy challenges. Comparative Political Studies **48**(9), 1127–1158 (2015)
17. Hanifatunnisa, R., Rahardjo, B.: Blockchain based e-voting recording system design. In: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). pp. 1–6. IEEE (2017)

18. Hanmer, M.J., Park, W.H., Traugott, M.W., Niemi, R.G., Herrnson, P.S., Bederson, B.B., Conrad, F.C.: Losing fewer votes: the impact of changing voting systems on residual votes. Political Research Quarterly **63**(1), 129–142 (2010)
19. Henry, K.J., Stinson, D.R., Sui, J.: The effectiveness of receipt-based attacks on threeballot. IEEE Transactions on Information Forensics and Security **4**(4), 699 (2009)
20. Herron, M.C., Sekhon, J.S.: Overvoting and representation: An examination of overvoted presidential ballots in broward and miami-dade counties. Electoral Studies **22**(1), 21–47 (2003)
21. Horwitz, D.A.: A picture's worth a thousand words: Why ballot selfies are protected by the first amendment. SMU Sci. & Tech. L. Rev. **18**, 247 (2015)
22. Huszti, A.: A secure electronic voting scheme. Periodica Polytechnica Electrical Engineering **51**(3-4), 141–146 (2008)
23. Indian Election Commission: Maintenance of law and order and prevention of electioneering within the prohibited area around polling stations - instructions regarding use of cellular phones (1998), https://ceo.gujarat.gov.in/Pdf/23Feb2018013934PM.pdf
24. Jones, D.W., Hall, M.: Technologists as political reformers: Lessons from the early history of voting machines. In: Society for the History of Technology Annual Meeting, Las Vegas. vol. 13 (2006)
25. Jones, H., Juang, J., Belote, G.: Threeballot in the field (2006)
26. Ju, C.: "you can't hack a piece of paper": Jake braun talks us election security. Chicago Policy Review (Online) (2018), https://web.archive.org/web/20180408041605/http://chicagopolicyreview.org/2018/04/01/you-cant-hack-a-piece-of-paper-jake-braun-talks-u-s-election-security/
27. Juang, W.S., Lei, C.L.: A secure and practical electronic voting scheme for real world environments. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences pp. 64–71 (09 1997)
28. Kutylowski, M., Zagórski, F.: Scratch, click & vote: E2E voting over the internet. In: Towards Trustworthy Elections, New Directions in Electronic Voting. pp. 343–356 (2010). https://doi.org/10.1007/978-3-642-12980-3_21
29. Larreguy, H., Marshall, J., Querubin, P.: What is the effect of turnout buying? theory and evidence from mexico. Harvard University (Cambridge, MA). Unpublished manuscript (2014)
30. Levitt, J.: The truth about voter fraud (2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1647224
31. Maike, V.: The Portrayal of Russia in US Media in the Aftermath of the 2016 Election Hacking Scandal. Master's thesis (2018)
32. McKenna, M.: Building 'a closet of prayer" in the new world: the story of the 'Australian ballot' (2001)
33. Miller, W.R.: Harrison county methods: Election fraud in late nineteenth-century texas. Locus **7**, 111–28 (1995), http://archive.today/2019.02.18-013902/http://courses.missouristate.edu/bobmiller/populism/texts/harrison_county_methods.htm
34. Moura, T., Gomes, A.: Blockchain voting and its effects on election transparency and voter confidence. In: Proceedings of the 18th Annual International Conference on Digital Government Research. pp. 574–575. dg.o '17, ACM, New York, NY, USA (2017). https://doi.org/10.1145/3085228.3085263, http://doi.acm.org/10.1145/3085228.3085263
35. Mwagwabi, F., McGill, T., Dixon, M.: 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). vol. 00, pp. 3188–3197 (1 2014). https://doi.org/10.1109/HICSS.2014.396
36. Nichter, S.: Vote buying or turnout buying? machine politics and the secret ballot. American political science review **102**(1), 19–31 (2008)
37. Orman, H.: Secure voting: A call to arms. IEEE Internet Computing **21**(5), 67–71 (2017)

38. Reynolds, A., Steenbergen, M.: How the world votes: The political consequences of ballot design, innovation and manipulation. Electoral Studies **25**(3), 570–598 (2006). https://doi.org/https://doi.org/10.1016/j.electstud.2005.06.009, http://www.sciencedirect.com/science/article/pii/S0261379405000612
39. Rivest, R.L., Smith, W.D.: Three voting protocols: Threeballot, vav, and twin. In: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology. pp. 16–16. EVT'07, USENIX Association, Berkeley, CA, USA (2007), http://dl.acm.org/citation.cfm?id=1323111.1323127
40. Santin, A.O., Costa, R.G., Maziero, C.A.: A three-ballot-based secure electronic voting system. IEEE Security & Privacy **6**(3), 14–21 (2008)
41. Selker, T., Cohen, S.: An active approach to voting verification. Tech. rep., Caltech/MIT Voting Technology Project (2005)
42. Sled, S.M.: Vertical proximity effects in the california recall election. Tech. rep., Caltech/MIT Voting Technology Project (2003)
43. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, A.J.: Security analysis of the estonian internet voting system. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 703–715. ACM (2014)
44. Stewart, G., Lacey, D.: Death by a thousand facts: Criticising the technocratic approach to information security awareness. Information Management & Computer Security **20**(1), 29–38 (2012). https://doi.org/10.1108/09685221211219182, https://doi.org/10.1108/09685221211219182
45. Strauss, C.E.: A critical review of the triple ballot (3ballot) scheme, part 1 (2006), https://www.cs.princeton.edu/~appel/voting/Strauss-TroubleWithTriples.pdf
46. Strauss, C.E.: A critical review of the triple ballot voting system, part 2: Cracking the triple ballot encryption (2006), https://www.cs.princeton.edu/~appel/voting/Strauss-ThreeBallotCritique2v1.5.pdf
47. Uzunay, Y., Bicakci, K.: 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. pp. 534–539. IEEE (2014)
48. Vassil, K., Solvak, M., Vinkel, P., Trechsel, A.H., Alvarez, M.R.: The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. Government Information Quarterly **33**(3), 453–459 (2016)
49. Vinkel, P.: Remote electronic voting in estonia: legality, impact and confidence. TUT Press (2015)
50. Wang, B., Sun, J., He, Y., Pang, D., Lu, N.: Large-scale election based on blockchain. International conference on identification, information and knowledge in the internet of things **129**, 234–237 (2018). https://doi.org/https://doi.org/10.1016/j.procs.2018.03.063, http://www.sciencedirect.com/science/article/pii/S1877050918302874