Boardroom Voting: Practical Verifiable Voting with Ballot Privacy Using Low-Tech Cryptography in a Single Room

Redacted for anonymous submission

Redacted institutes

Abstract. A *boardroom election* is an election that takes place in a single room—the boardroom—in which all voters can see and hear each other. We present the first practical protocol for boardroom elections with ballot privacy and voter verifiability that uses only "low-tech cryptography" without any computers. The protocol combines several practical building blocks in novel ways, including existing ones (e.g., invisible and revealing inks, ink stamps, scales) and a few we introduce. These new building blocks include "foldable ballots" that can be rotated to obfuscate the alignment of ballot choices with voting marks, and "visual secrets" that are easy to remember but hard to describe. Although closely seated participants in a boardroom election have limited privacy, the protocol ensures that no one can determine how any individual voted. Moreover, each voter can verify that their ballot was correctly cast, collected, and counted, without being able to prove how they voted, providing assurance against undue influence. In contrast with traditional paper ballot voting methods typically used in today's boardrooms, our protocol provides an alternative that offers higher outcome integrity and ballot privacy while remaining usable and paper based.

Keywords: Applied cryptography, boardroom voting, high-integrity election systems, usable security.

1 Introduction

Most research on election technology has focused on mass elections conducted in person using precincts or kiosks, or at distance using mail-in ballots or the Internet. Many important elections, however, take place with a relatively small number of voters (say, less than 40) voting in person in the same room. For example, a board of directors might vote whether to adopt a new corporate policy; a committee of professors might vote whether to grant tenure to a colleague; or shareholders might decide on a business action.

Typically, boardroom elections take place with traditional paper ballots with no guarantees of ballot privacy or outcome integrity. It is often easy for a voter to see how their neighbour votes. There is no assurance that ballots were not modified prior to counting them. Although the boardroom setting presents challenges for ballot privacy, it also offers some advantages: one could prevent non-voters from entering the room, and everyone in the room can observe each other.

Scrutiny of boardroom election procedures goes back centuries, with a 1274 decree specifying the procedures for bishops to elect the next pope. But such procedures and modern proposals either lack ballot privacy or outcome integrity, or require advanced technology (e.g., complex cryptography carried out on computers).

We present the first practical protocol, BVP1, for such "boardroom elections" with ballot privacy and voter verifiability that uses only "low-tech cryptography" without any computers. Our simple low-tech paper-based solution avoids the need for computers running complex software. It simplifies the trust model and does not require the sophisticated cryptographic audits integral to most *End-to-End (E2E)* systems, such as Scantegrity [11,8,12,9] or Prêt-à-Voter [33,32,19]. The independence from electronic tools also ensures limited cost and improved availability in a wide variety of settings, while assuaging widespread concerns about election hacking.

With this protocol, no one can determine how any individual voted, even when observing from close proximity a voter marking their ballot. Each voter can verify that their ballot was correctly cast, collected, and counted. No voter can prove to anyone else how they voted, providing assurance against undue influence. Each voter can be convinced of any malfeasance involving their vote. In the basic version of BVP1, the voter cannot prove such malfeasance to anyone else. We also present a variation of BVP1 in which objecting voters can prove such malfeasance at the cost of some degradation of ballot privacy.

In the rest of this paper we define boardroom elections, explain our assumptions and adversarial model, briefly review prior work on boardroom elections, present practical building blocks (new and existing), propose a new protocol for boardroom voting that combines selected building blocks in novel ways, analyse the protocol, and discuss our conclusions.

This paper's contributions include:

- A new practical protocol for boardroom voting that offers ballot privacy and voter-verifiable outcome integrity.
- New building blocks for boardroom elections, including "foldable ballots" that can be rotated to obfuscate the alignment of ballot choices with voting marks, and "visual secrets" that are easy to remember but hard to describe.

2 Boardroom Elections

A *boardroom election* is an election that takes place with all voters present in a single room, which we shall call the *boardroom.* A crucial property of such elections is that all voters can see and hear each other. While there is no rigid maximum number of voters, we imagine a typical boardroom election to involve approximately four to forty voters. The election is administered by an untrusted voter or their untrusted assistants, also present in the room, which we shall call the *Election Authority (EA).* The election begins and ends in the boardroom. The process might be supported by some materials, such as paper ballots, marking devices, tape, stamps, and other objects which can be acquired in advance.

We seek solutions that are simple and practical, afford ballot privacy, and provide outcome integrity verifiable by the voters present. In particular, we seek solutions that do not require the use of complex technology, such as laptops or sophisticated cryptographic software. These requirements do not exclude the use of cryptography, but require that any cryptography be carried out in a "low-tech" fashion (e.g., implementing a cryptographic commitment by covering a character string with black photographic tape).

The system should satisfy the security requirements of *ballot privacy* and *outcome integrity*. Ballot privacy means that no one should have the ability to link a marked ballot to the voter who cast it, not even with the cooperation of corrupt voters. Ballot privacy protects against undue influence, including vote selling and coercion. Outcome integrity [3] means that the voters can verify that (1) They cast their ballot as intended; (2) The ballots were collected as cast; and (3) The ballots were counted as collected. We distinguish between two types of outcome verifiability: *Weak verifiability* means that a voter can convince themselves if outcome integrity is violated. *Strong verifiability* means that the voter can additionally convince others of such malfeasance.

Ideally, the system should resist delay and disruption, and it should not be possible for a corrupt voter to convince other voters with a false claim of malfeasance (that is, the system should resist *discreditation attacks*).

3 Assumptions and Adversarial Model

We explain our assumptions and adversarial model, including characteristics of the room and the adversary's motivations, capabilities, access, resources, and risk tolerance.

3.1 Assumptions

We assume the boardroom has sufficient size, light, and acoustics that the voters can be all present in the room, see each other, and hear each other. Cameras and electronic devices—including cell phones—are not permitted, and we assume that none are hidden or otherwise present in the room. Similarly, we assume that it is not possible to peer into the room from outside, for example, using a telescope aimed through a window.

The situation, however, is sufficiently crowded and cosy that each voter can see what nearby voters are doing or writing at their seat. There can be a place in the room that offers privacy—for example, by using a privacy screen—where voters can go, one at a time, to carry out certain voting steps.

The only people present in the room are the voters and, possibly, a few people acting as the election authority. Neither the voters nor the election authority are trusted. For example, some voters may wish to sell their votes, try to discredit an outcome they dislike, or discredit the election authority.

During the election, communications among people in the room are not allowed beyond those required for the election procedure. We acknowledge, however, that it would be impossible to prevent all such communications completely, possibly including ones sent through covert channels (e.g., hand gestures). We assume that such illicit communications are either detected or have limited bandwidth.

3.2 Adversarial Model

The adversary's goals may include any of the following: influence the result of the election; find out how certain voters voted; prevent, delay, or discredit the election; or frame a specific voter for trying to disrupt the election.

The adversary might be a voter or member of the election authority. There might be multiple adversaries acting in concert, or each for a different—and potentially opposed—goal. Regardless, the adversaries have complete knowledge of the election system and all procedures.

To achieve their goals, the adversary has access to financial and technical resources. We assume they have copies of the materials used in the election—at least for materials that are not unique. They can try to bribe or coerce one or more of the voters. Because they are in the boardroom, they can also peer over other people's shoulders and look at what voters write and do.

To some limited extent, the adversary is capable of executing certain sleight-of-hand activities. For example, the adversary might drop two ballots into a ballot box instead of one without detection, or make a ballot vanish (e.g., into their sleeve). Such manoeuvres can affect the distribution or collection of physical materials, unless additional protections are enforced.

We assume that the adversary wishes not to be detected. Thus, the adversary does not wish to reveal their malicious intentions, and a failed attack might lead to serious consequences (e.g., lost reputation, lingering doubts, loss of job, investigation). Unlike electronic attacks, which might be carried out at a distance and be hard to trace, boardroom attacks by an adversary in the room might carry high risks. Consequently, deterrence may play an important role.

4 Previous Work

The papal election is the most famous example of a boardroom election. We briefly comment on this long-standing procedure and modern proposals. Unfortunately, the papal protocol neither safeguards ballot privacy nor outcome integrity, and all modern proposals depend on complex technology and hence are unlikely to be widely used.

Small-scale elections in a single room have been organised and studied for centuries, a prime example being the papal election. Its rules are still mostly based on the papal decree *Ubi Periculum* [29], written in 1274, and made into canon law in 1298 [14]. Although it describes in great detail the way the electors should interact with the outside world, and requires the winner to be elected by at least a two-thirds supermajority, it makes no mention of how the vote is to happen. More recent rulings forbid the presence of any audio-visual recording equipment [30]. They also establish some formal requirements, including ballot chain of custody and ballot format (secret ballots, with explicit constraints on their size and design). These rules, however, do not address the issues of privacy and verifiability in the presence of a skilled adversary.

There are some images and speculations about how ancient Greeks may have voted by dropping a pebble, a pottery bit, or a small bronze disk—to which was attached a peg corresponding to the vote—into a tall urn or urns, possibly creating an audible sound [6,7]. Although much remains unclear about how the ancient Greeks actually voted, we can imagine very attractive methods involving dropping pebbles into urns behind the protection of a privacy screen.

Today, boardroom voting commonly occurs in classrooms, company management meeting or faculty meetings as well as at shareholder meetings where intimidation and fraud are frequent [2,17]. Within the past fifteen years, researchers have proposed several solutions, always based on electronic means, including smartphones [4], blockchains [24], authenticated communication channels [15], or insecure devices [1]. Such cryptographic solutions have attempted to improve efficiency [21] or add features such as decentralisation [24], robustness [18], or the possibility of vote delegation [22]. Kahan and Rock [17] examined corporate voting in the United states from a legal perspective.

Kiayias and Yung [20] explored self-tallying cryptographic voting methods that may be useful in the boardroom because they offer strong ballot secrecy and simplified post-casting procedures.

Kulyk [21] surveyed and compared cryptographic boardroom voting, assuming a common network, the deployment of a public-key infrastructure, and that each voter has an electronic device. Kulyk also compiled a list of useful cryptographic primitives and protocols and compared their computational complexity.

Hao [16] studied “classroom voting,” where the most important requirements are minimising the cost of election materials and using open-source software and readily available low-cost hardware.

5 Building Blocks

This section presents primitives used as building blocks in the physical protocols of the following section. Here we describe the primitives succinctly; the Appendix provides more details, as well as other building blocks that could serve to develop alternative protocols.

5.1 Pre-Existing Building Blocks

Privacy Enhancers In a boardroom election, all voters vote in the same room and can observe each other to gather information on voting decisions. Privacy enhancers, such as booths, opaque panels, or pieces of cloth under which voters can manipulate objects, can allow voters to make certain decisions and mark ballots in secret.

Locked Boxes Small items, such as ballots, tokens, pens, or stamps, often change hands in our context, creating opportunities for an adversary to steal or alter them. Identical small boxes, each with a lock, can be an effective way to ensure the integrity of items as they are changing hands or for a certain duration, or to solve *commitment problems.*

Random-Draw Methods Many secure voting schemes require the generation of random permutations. This process can be carried out physically quite easily; examples abound, such as drawing random items from a bag, common in board-games (as in Scrabble where one draws letters).

Cut-and-Choose Cut-and-choose is a mainstay auditing procedure. It refers to making duplicates of required items, drawing some (either at random or chosen by an auditor), and examining them thoroughly in public to ensure that they have not been maliciously altered. By taking a few items at random, one can ensure with high confidence that, if a large proportion of all items were deficient, this fact would be detected and the election would be stopped. It can also be used to reveal part of a secret that is split into multiple sections, as David Chaum's protocol for electronic cash does [10]. The main drawback of such methods is that they add complexity and time, and require more materials (more ballots or tools so that some can be removed and publicly examined).

Invisible Ink Invisible ink can be used to strengthen ballot confidentiality in multiple ways and has been used in the Scantegrity voting system [11,13]. We define invisible ink as any ink that is not visible to the human eye without the use of special tools or chemical reactions. We also consider time-sensitive invisible ink that automatically becomes visible after a specified period of time, or that disappears after a certain time. Invisible ink limits the risk of onlookers trying to determine what a voter is writing while they are writing. It also allows the resulting secret to be kept in plain sight during the rest of the voting protocol, including during shuffles, reducing opportunities to alter the ballot. In terms of usability, using invisible ink has little cost to the voters, but requires more advanced manufacturing and increases costs.

5.2 New Building Blocks

The following building blocks are either entirely new (such as foldable paper ballots and visual secrets), or present novel uses of existing mechanisms.

Scales and Transparent Ballot Boxes Putting the ballot box on a scale to measure its weight over time can prevent certain attacks by detecting if a voter places more than one ballot into the box. Transparent ballot boxes are already used to address the same problem, though they mostly prevent someone from not voting at all. Inattentive voters could be fooled by two envelopes being cast at the same time. They have the small inconvenience of making it potentially feasible to follow each envelope during the shuffling process, especially when there are few ballots.

Polarising Filters Another way to reinforce confidentiality is to use polarised light filters, either on ballots, or on a screen used to distribute some common secret. The main advantage of this method is that it makes filming the boardroom with hidden cameras harder, as polarised cameras tend to be bulkier or more expensive [31], and applying a filter before-hand can fail because the adversary needs to know the direction of the polarisation. This method has fewer applications, as it is mostly useful when using a common screen, or small devices that react to polarised light. From a usability standpoint, it requires only polarised glasses, which can easily be found for less than 10€, does not significantly increase the time taken to vote, and slightly raises the complexity.

Foldable Paper Ballots To protect ballot confidentiality, we propose foldable paper ballots. The simplest example is a paper ballot consisting of two labelled columns, where each column corresponds to a particular choice, which is labelled at both the top and bottom of the ballot, as in Figure 1.

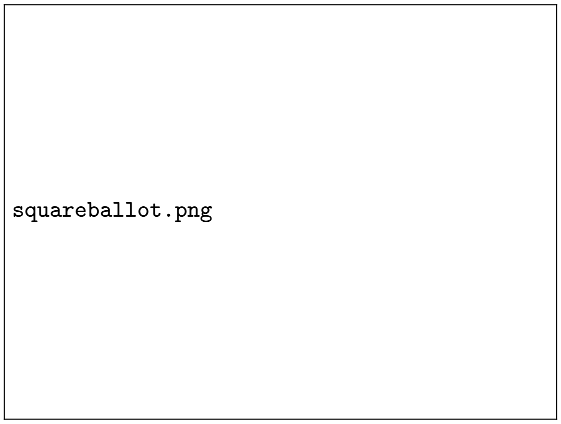

Fig. 1. A foldable paper ballot for a binary choice between two candidates. The voter makes a mental note of where each label is, folds the edge of the ballot on top of the label, rotates it, and puts a mark on the zone corresponding to the candidate of their choice—all in plain sight of other voters.

A voter wishing to mark a ballot makes a mental note of the labels for each column and folds both the top and bottom portions of the ballot down over the labels to hide them. The voter then randomly rotates the ballot several times before applying their mark. When rotating their ballot, a voter should prevent adversaries from observing the number of rotations, e.g., by rotating the ballot beneath a cloth. An adversary who does not know the number of times a voter rotated a ballot cannot easily discern their choice by observation alone, as the ballot is symmetrical. The folding can either be temporary or designed to resist some attacks by making part of the paper adhesive, preventing an adversary from unfolding the ballot and glancing at it discreetly. To make temporary folding more secure (and resistant against quickly unfolding and flashing the label at someone), the top and bottom parts can be folded twice.

A foldable paper ballot consisting of two columns supports two choices. To support additional choices, we suggest using a polygonal paper ballot. An alternative is a candidate wheel, which is a continuous band of paper with candidates on the side (see Appendix for figures and more details).

Parallel Vote Tallying If voters suspect that someone could maliciously handle the ballots during the opening of the ballot box and the tallying phase, they might not want to trust the process to a single person. To address this issue, one solution is to hold multiple parallel tallies for the same election by duplicating ballots, with different guarantors for each ballot box. The problem is then to ensure that the ballots cast into each ballot box are identical, or discreditation attacks might be possible. One solution is based on the binary foldable ballot.

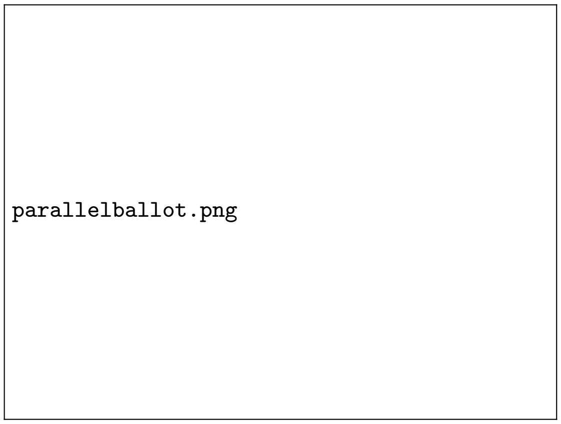

Fig. 2. A ballot design for parallel elections that forces voters to vote for the same candidate in both elections. Each voter makes two marks on the same side, then cuts the ballot in two along the dashed horizontal line, and casts each half in a different ballot box.

In this ballot, the space where the voter is supposed to make a mark is split into two, vertically, as in Figure 2. Once the paper is folded, the voter makes two marks on the same side, which can be checked by other people in the room, before cutting the ballot in half and casting each half in a different ballot box.

The Appendix shows a generalisation to more candidates based on the candidate wheel.

Visual Secrets To obtain verifiability in a boardroom, one possibility is to have a secret that is present on the ballot given to the voter, such as a secret string under a scratch-off protection, and all ballots are revealed publicly after the votes are all cast. As long as a coerced voter cannot communicate the secret to the adversary before the ballots are all revealed, they are safe, as they can tell the adversary that they voted according to any other revealed ballot, without the possibility to prove anything (unless a candidate obtains zero votes). There is one caveat: when the adversary coerces multiple voters who all happen to say they have the secret corresponding to the same ballot. In such case, the adversary knows that at least some of them are lying[1]. However, if they can communicate their secret to an adversary before the public reveal, they can be held accountable to their votes, negating their privacy.

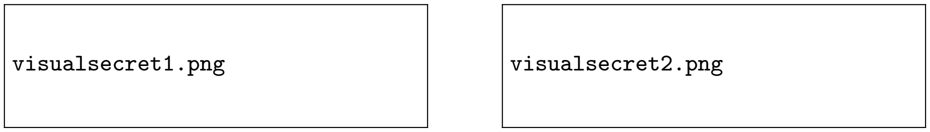

Fig. 3. Two examples of visual secrets, which are easy to distinguish and remember but hard to describe orally. The patterns shown here are relatively simple; more complex ones could be used.

One solution is to focus on secrets that are easily recognisable but hard to communicate. There is one simple way to do this, thanks to our visual pattern recognition. The idea is to use a set of images built with similar patterns although visually different. For example, 30 different images of lions could be taken among a set of 1000, making it hard to describe any image with high precision succinctly. Alternatively, abstract patterns could also be used, as in Figure 3. One simple way of doing this is to give a sheet of stickers to each user, with many variations on a given design. This way they can select the design of their choice, remove it from the sheet under the table and apply it to their ballot[2].

One drawback of visual secrets is that some people might forget the pattern (or confuse it for another), but this fact is true for any pattern that needs to be

[1] There is one potential fix for such situations that drastically reduces the probability of coerced voters saying they have the same secret, but it has a high usability cost and could potentially induce other security weaknesses. It works by agreeing to add a certain number of votes in favour of each candidate to the total, casting the corresponding ballots, and removing the corresponding number from the tally.

[2] This method has two problems: first, the sheet with the remaining stickers can be kept, which creates a vulnerability. Second, the chosen sticker itself could be seen by an adversary during the operation, especially if the voter is coerced into cooperating.

remembered, and humans have excellent abilities for visual recognition—going above recognition for strings—especially with short-term memory [25].

Stamps The visual secrets mentioned previously can be used in multiple ways, but the obvious way is to imprint a mark on a ballot that only the voter can remember, allowing them to track their ballot when it becomes public. The question is then how to distribute visual secrets securely, and how to apply them on a ballot in a way that is not immediately traceable by an adversary, as the solution shown above with stickers is vulnerable.

One solution is to use customised stamps. The stamps can be put in a bag, using a random draw method. To mitigate the risk of an adversary seeing the pattern, two additional precautions should be taken. First, the stamp should use invisible ink, such that the visual secret is not visible to the voter's neighbours as they apply the stamp. Second, it should be a stamp that rotates when pushed down—called a self-inking stamp—making the pattern visible only when one presses on the stamp. Consequently, the voter can look at the pattern by pressing it in their hands before their eyes, but prevents neighbours from seeing the pattern due to the limited angle at which the pattern is visible. Moreover, it makes showing the pattern to an adversary much more conspicuous. Care should be taken that the stamps are used only on the ballots and put back on the table afterwards, to prevent voters from keeping a proof of how they voted. Another possibility is to make the stamps freely available at the center of the table once they are used, so that coerced voters can fabricate fake evidence that they voted one way[3].

This method requires custom-made stamps, which is moderately costly. However, they can be re-used a few times, even more so if only a subset of the stamps is taken each time. Using visual secrets adds some complexity as it requires two actions by the voter (checking the pattern and stamping the ballot).

6 Voting Protocol

We propose a new paper-based boardroom voting protocol, BVP1, that offers ballot privacy and voter privacy when voters are seated around a table. The protocol combines the building blocks of foldable ballots, randomised stamps, random draws, invisible ink, and a ballot box on a scale. We assume there is a single ballot question with k choices, where k is small enough that a k-ary foldable ballot works (say, $k < 7$). We also discuss variations of this protocol.

[3] As long as they manage to stamp a few sheets of paper with different stamps, they have a high chance of getting one with the result they are supposed to have, and it would be hard for the adversary to confront them in the boardroom before the vote corresponding to each pattern is made public.

6.1 Boardroom Voting Protocol 1 (BVP1)

We describe *Boardroom Voting Protocol 1 (BVP1)* in terms of its setup, ballot marking, casting, counting, and verification steps. Let n denote the number of voters.

Setup. The election authority prepares n or more k-ary foldable ballots and an opaque bag of n externally indistinguishable visual-secret stamps, each inked with invisible ink. Each stamp imprints a random abstract pattern. The protocol also requires a ballot box, scale, and one or more opaque black cloths. The n voters are seated at a table on which there are one or more black cloths. To deal with spoiled ballots and stamp malfunctions, the election authority should also prepare some number of extra ballots and stamps.

Ballot Marking and Casting

1. Each voter receives a k-ary foldable ballot, where each side corresponds to a ballot choice.
2. The election authority places n visual-secret stamps in the middle of the table, where the voters can observe that the stamps do not have any externally identifying features.
3. The election authority places the stamps in an opaque bag one by one under scrutiny of the voters, after which the bag is slightly shaken and passed around the table. Each voter takes one stamp out of the bag.
4. Each voter visually inspects the pattern on their stamp and remembers it.
5. Each voter folds the edges of their ballot and rotates the ballot under the cloth until they are confident that only they know which side corresponds to which candidate.
6. In plain sight, each voter stamps their ballot in a location on the ballot of their choice.
7. One by one, each voter casts their ballot into a ballot box on a scale in a clearly visible place in the room.

Counting and Verification

1. The election authority shakes the ballot box, takes out the ballots, unfolds them, and places them on the table for all to observe (but not touch). The election authority sprays revealing ink on the ballots.
2. The election authority counts the number of ballots, tallies the result, and writes down these numbers for all to see.
3. Each voter verifies the counts and looks for their visual secret.
4. If any voter does not see their visual secret or disputes any count, or has any other concern, they may raise an objection stating their concern.
5. If the number of objections is less than half the margin of victory, the winner is elected. Otherwise, the election is annulled.

6.2 Variations

We discuss four optional variations: voting station, rotating ballots under the table, parallel ballot collection and tallying, and protection against discreditation attacks—which offer different tradeoffs among complexity, privacy, and outcome integrity.

Voting station. Instead of voting at the main table, each voter could vote, one-by-one, at a dedicated voting station in the room, with observers from different factions. The station might be a table with a stack of ballots, a bag of unused stamps, a ballot box, and an opaque cloth. This setup would provide slightly better privacy and would better accommodate larger sets of voters.

Rotating ballots under the table. Instead of using opaque cloth(s), voters could rotate their ballots under the table. This simpler method, however, might make it easier for malicious voters to exchange ballots in a chain-voting attack (see Section 7.4).

Parallel ballot collection and tallying. When the environment is highly contentious with high risk of attack, including discreditation attacks, it may be difficult for the voters to agree on an election authority, and there might be increased risks for discreditation attacks. In such situations, it may be helpful to conduct the ballot collection and tallying portion of the election in parallel, with each of two factions controlling one ballot box.

A crucial challenging task of conducting ballot collection and tallying in parallel is to ensure that each voter submits the same ballot choices to each ballot box. Section 5.2 describes a mechanism for doing so. Because BVP1 uses invisible ink, voters would carry out two rounds of stamping: first with a common stamp that simply imprints a visible black disk, then second with the unique stamp. Other people in the room can check that each voter stamps two black disks on the same region, and that people only stamp with invisible ink next to a black disk.

Protection against discreditation attacks using receipt ballots. BVP1 offers only weak voter verification: each voter knows whether or not their ballot was properly collected and counted, but they cannot convince others of this fact. For example, one or a few voters could falsely claim that their visual secret is not present or that their ballot is filled out incorrectly. BVP1 offers no way to adjudicate such claims, other than to ignore them if their numbers do not affect the election result. The following variation offers increased protection against discreditation attacks at the cost of diminished ballot privacy.

Using the procedure described above for creating two identically marked ballots, each voter keeps one of the ballots (which we shall call the "receipt ballot") on the table in front of them in plain sight. Observers cannot see the visual secret because it is imprinted with invisible ink. After the cast ballots are counted, let j be the number of voter raising an objection. If j is less than half the margin of victory, then the objections cannot affect the election outcome.

If j is at least half of the margin of victory, then the following process can be carried out to adjudicate the objections. The election authority collects all of the receipt ballots in front of voters raising an objection. After mixing these receipt ballots in an initially empty ballot box, the election authority places them in a central part of the table and sprays them with revealing ink. Then, everyone can compare the revealed receipt ballots with the set of cast ballots. An objection is deemed valid if and only if the associated revealed receipt ballot does not match any other of the cast ballots.

If the number of validated objections $j\prime$ is at least half the margin of victory, then the election is annulled.

At the end of the election all ballots should be mixed together and preferably also destroyed.

7 Analysis

We analyse our voting protocol, including its outcome integrity, ballot privacy, usability, and potential vulnerabilities and attacks.

7.1 Outcome Integrity

The integrity of the election outcome rests on the ballots being cast as intended, collected as cast, and counted as collected. All ballots are in plain sight from their distribution until they are shuffled in the ballot box, except for the moment when they are rotated under the cloth (or table). This fact makes it hard for an adversary to modify or replace another voter's ballot.

Assuming each voter can remember and identify their visual secret, each voter can verify if their ballot has been correctly collected and counted. Although each voter can notice if their ballot has been altered, they cannot prove it (unless using the receipt ballot variation). Because the ballot box sits on a scale, attempts to cast more than one ballot can be detected.

Threats to outcome integrity include voter mistakes in remembering their visual secret or keeping track of the ballot orientation. In addition, discreditation attacks might cause the election to be annulled.

7.2 Ballot Privacy

The inability of someone in the room to link a voter to a cast ballot depends on several assumptions, including: the ability of the voter to hide the orientation of the ballot, the inability of observers to read the invisible ink, and the absence of cameras in the room.

In addition, to protect against malicious or coerced users, it is important that the voter be unable to: describe their secret, show their ballot orientation or marks to anyone else, secretly imprint and exfiltrate their visual secret, or make any identifying marks on the ballot.

The receipt ballot variation reduces the anonymity set of those making an objection to the number of people making objections.

7.3 Usability

The user experience seems fairly simple for an alert sighted voter: the voter acquires a ballot, folds it, and rotates it a few times under the cloth keeping track of its orientation. They take a stamp from a bag, look at it to learn the pattern, stamp their ballot in the desired area, and cast the ballot into a ballot box.

During the counting and verification phase, the voter looks for their ballot by looking for their visual secret. After finding it, the voter verifies that it is marked correctly. The voter also verifies the tally and the number of ballots counted. Throughout the entire voting process, the voter observes activities in the room.

It remains to be determined through usability testing how well voters can carry out these tasks. Potential difficulties include keeping track of the orientation of the ballot, remembering the visual secret, and being able to notice possible malicious activities.

7.4 Potential Vulnerabilities and Attacks

We consider several potential attacks. Inspired by chain voting [34], an adversary could acquire a stamp, discreetly stamp their own ballot, and exchange their ballot with that of a coerced or bribed voter. With the ballots in plain sight, it would be difficult to do so without detection, especially involving many voters.

In an attempt to defeat the variation for imprinting two identical ballots, a malicious voter could feint imprinting one of the invisible ink marks without making an imprint. To mitigate this threat, part of the stamp (not part of the visual secret) could be inked with visible ink with a simple common mark.

A malicious or coerced voter could make a uniquely identifiable mark on their ballot—for example, by pricking a pin hole in a certain location, or intentionally smudging the stamp in a certain way. Similarly, a corrupt election authority could distribute uniquely identifiable ballots with discreetly placed pin holes, marks, or tears. This latter attack can be mitigated by putting the unmarked ballots in a bag and drawing them at random.

It would be difficult to ensure that there are no miniature hidden cameras in the room or on malicious voters. Privacy enhancers partially address this concern, as it is easier to ensure that the ballot is not in the field of those cameras while under a cloth.

A malicious or coerced voter could attempt to show the orientation of their ballot to a nearby adversary. Mandatory rotations under the cloth makes it harder to enforce, although it might still be possible to create a crease that makes it identifiable.

7.5 Dealing with Election Failure

All election systems are vulnerable to denial-of-service attacks, which can be easy to carry out (e.g., bomb the voting place). Similarly, for most election systems, the system cannot prevent attacks on the election outcome, but at best can detect such attacks. One advantage of boardroom elections is that, in comparison with large-scale elections, they are relatively easier to re-run if necessary. Also, in many boardroom contexts, the cost to an adversary of getting caught is especially very high. While re-running an election would be a highly undesirable outcome, this outcome exists as a final option. It then makes sense to have a secondary highly secure, although possibly less usable, system at hand. Voters could then use an easy, fast, and usable protocol that only guarantees detection of fraud (but not necessarily adjudication). The existence of a backup solution and deterrence allows voters to benefit from increased efficiency, while reducing the risk of election annulment.

8 Conclusion, Open Problems, and Future Work

This paper introduced the first practical protocol for boardroom elections with ballot privacy and voter verifiability using only low-tech cryptography. The protocol is significant because many important elections take place in boardrooms, and these elections typically are carried out without ballot privacy or voter verifiability. All modern proposals for boardroom elections depend on complex technology, but it is unlikely that many people and organisations will be willing to run boardroom elections using complex technology, especially in a context where people tend to be distrustful of electronic voting. Although our protocol is potentially vulnerable to some attacks, it offers greater election integrity and ballot privacy in comparison to the simple paper methods used in most boardrooms today.

As boardroom voting happens in a vast range of situations with varying financial, temporal, and usability constraints, there are benefits in having a range of protocols from which to choose. The low-tech primitives we introduce, and the BVP1 protocol and its variants, provide a useful first set of simple solutions that avoid certain drawbacks of existing E2E systems including their need for complex audits. We hope that others will be inspired to discover even better boardroom election solutions, for example, achieving stronger verifiability and greater resistance to discreditation attacks.

We plan to continue this work by conducting usability tests of the new primitives and voting protocol. Open problems include: (1) Devise additional solutions that provide stronger verifiability, better protection against discredidation attacks, or greater simplicity. (2) Find solutions that work for voters with visual impairments.

References

1. Arnaud, M., Cortier, V., Wiedling, C.: Analysis of an electronic boardroom voting system. In: Heather, J., Schneider, S., Teague, V. (eds.) E-Voting and Identify. pp. 109–126 (2013)

2. Barrett, R.W.: Elephant in the boardroom: Counting the vote in corporate elections. Valparaiso University Law Review **44**, 125 (2009)
3. Benaloh, J., Rivest, R.L., Ryan, P.Y.A., Stark, P.B., Teague, V., Vora, P.L.: End-to-end verifiability (2015), `http://arxiv.org/abs/1504.03778`
4. von Bergen, P.: A mobile application for boardroom voting. Master's thesis, Bern University of Applied Sciences, Biel, Switzerland (2014)
5. Blunch, N.J.: Position bias in multiple-choice questions. Journal of Marketing Research pp. 216–220 (1984)
6. Boegehold, A.L.: Toward a study of athenian voting procedure. Hesperia: The Journal of the American School of Classical Studies at Athens **32**(4) (1963)
7. Canevaro, M.: Majority Rule vs. Consensus: The Practice of Democratic Deliberation in the Greek Poleis, pp. 101–156. Edinburgh University Press (09 2018)
8. Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., et al.: Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy. In: Proceedings of USENIX Security 2010. USENIX Association (2010)
9. Carback, R.T., Chaum, D.A., Essex, A., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T., Vora, P.L., Wittrock, J., Zagorski, F.: The Scantegrity Voting System and its Use in the Takoma Park Elections (2016)
10. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology. pp. 199–203 (1983)
11. 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** (2008)
12. Chaum, D., Carback, R.T., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y.A., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes. IEEE transactions on information forensics and security **4**(4), 611–627 (2009)
13. 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)
14. Colomer, J.M., McLean, I.: Electing popes: approval balloting and qualified-majority rule. Journal of Interdisciplinary History **29**(1), 1–22 (1998)
15. Groth, J.: Efficient maximal privacy in boardroom voting and anonymous broadcast. In: Juels, A. (ed.) Financial Cryptography. pp. 90–104 (2004)
16. Hao, F., Clarke, D., Randell, B., Shahandashti, S.F.: Verifiable classroom voting in practice. IEEE Security Privacy **16**(1), 72–81 (January 2018)
17. Kahan, M., Rock, E.B.: The hanging chads of corporate voting. Georgetown Law Journal **96**, 1227–1281 (2007)
18. Khader, D., Smyth, B., Ryan, P., Hao, F.: A fair and robust voting system by broadcast. Proceedings of the Gesellschaft fur Informatik pp. 285–299 (2012)
19. Khader, D., Tang, Q., Ryan, P.Y.A.: Proving Prêt à Voter receipt free using computational security models. In: EVT/WOTE (2013)
20. Kiayias, A., Yung, M.: Self-tallying elections and perfect ballot secrecy. In: Naccache, D., Paillier, P. (eds.) Public Key Cryptography. pp. 141–158 (2002)
21. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M., Haenni, R., Koenig, R.E., von Bergen, P.: Efficiency evaluation of cryptographic protocols for boardroom voting. In: ARES 2015, August 24-27. pp. 224–229 (2015)
22. Kulyk, O., Neumann, S., Marky, K., Volkamer, M.: Enabling vote delegation for boardroom voting. In: Financial Cryptography and Data Security. Cham (2017)

23. Kutylowski, M., Zagórski, F.: Scratch, click & vote: E2E voting over the internet. In: Towards Trustworthy Elections, New Directions in Electronic Voting (2010)
24. McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security (2017)
25. N. Shepard, R.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior **6**, 156–163 (02 1967)
26. Nakajima, M., Yamaguchi, Y.: Extended visual cryptography for natural images. In: WSCG 2002, February 4-8. pp. 303–310 (2002)
27. Naor, M.: Bit commitment using pseudorandomness. Journal of Cryptology **4**(2), 151–158 (Jan 1991)
28. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) Advances in Cryptology — EUROCRYPT'94. pp. 1–12. Berlin, Heidelberg (1995)
29. Pope Gregory X: Ubi Periculum (1274)
30. Pope John Paul II: Universi dominici gregis on the vacancy of the apostolic see and the election of the roman pontiff. In: Apostolic Constitution (02 1996)
31. Prutchi, D.: Dolpi - two low-cost, raspi-based polarization cameras for humanitarian demining and other applications (2015), `https://web.archive.org/web/20190406042503/https://hackaday.io/project/6958-dolpi-raspi-polarization-camera/details`
32. Ryan, P.Y.A.: Prêt à Voter with confirmation codes. In: EVT/WOTE (2011)
33. Ryan, P.Y.A., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à Voter: a voter-verifiable voting system. IEEE TIFS **4**(4), 662–673 (2009)
34. Saltman, R.: The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence. Palgrave Mcmillan (01 2006)
35. Sled, S.M.: Vertical proximity effects in the California recall election. Tech. rep., Caltech/MIT Voting Technology Project (2003)
36. Zagórski, F., Carback, R., Chaum, D., Clark, J., Essex, A., Vora, P.L.: Remotegrity: Design and use of an end-to-end verifiable remote voting system. In: ACNS (2013)

A Appendix

We provide more details for some of the preexisting building blocks mentioned in Section 5, with their advantages and some issues they raise. We also include figures of selected additional foldable paper ballots.

A.1 Detailed Preexisting Building Blocks

Privacy Enhancers To protect voters from malicious observation, the voting area can include private spaces established through means such as opaque panels, curtains, booths, or other visually obfuscating elements, as is already used in many countries to guarantee the voter's privacy while they fill in their ballot. An adversary unable to observe voters casting their votes must rely on potentially more costly, risky, or conspicuous methods. Attempts to encroach on other voters' voting areas should be detected with a high probability, either by an honest voter or by a third party monitoring the election. Private voting areas complicate attacks relying on passive observation while providing voters with some assurance that nobody is watching them cast their vote. They can also facilitate more advanced attacks, however, by masking malicious activity, and they are potentially vulnerable to hidden cameras, especially if the adversary can be the one setting up the voting area. Private voting areas should carefully balance protecting voters' privacy from spying adversaries and shielding adversaries from the scrutiny of other voters.

In practice, private booths can be used in boardroom voting, although they have multiple issues: they take a significant amount of space, are vulnerable to cameras, but mostly cause delay, unless there are many booths present, and require people moving around, all of which degrades usability. An alternative is to use more portable voting areas, where voters are still partially observable while casting their ballots. In this case, the goal is to offer private manipulation of an item. The simplest case in our context is putting the ballot under the table and writing a name without being able to see the ballot before folding it (and, most importantly, without one's neighbours being able to see what is written). A slightly more involved but more secure means is to have a sheet of fabric on the table, under which the voter can manipulate, sign and fold their ballot. Similar systems are also used in conjunction with electronic voting in parliaments, where the hand of the voter is hidden in a box with three buttons inside.

One issue with private booths and voting stations is that the sequential access to them voting would be slower than for the parallel voting (as in BVP1). To speed up voting, one could have two or more stations, but this could potentially create vulnerabilities depending on how it is implemented.

Scales Although they do not seem to be used in this way today, counting the ballots as they are inserted in the ballot box is inspired from an ancient practice: in Ancient Athens, where pottery bits called *ostraka* with votes recorded on them were visibly—and potentially audibly—dropped in tall urns [7,6]. To implement this primitive correctly, the ballot box should ideally rest on a scale away from the group of voters—the weight display being visible to everyone—with people going to cast their votes one at a time. At least one attack is prevented by this method, which works as follows. An adversary coerces one voter into not voting, faking the insertion of the ballot into the ballot box—quite easy with sleight-of-hand, especially if there is more than one person next to the ballot box. The adversary then votes twice by inserting two ballots instead of one, through sleight-of-hand. This requires having a second ballot ready, although that is often possible. By obtaining the missing ballot, the adversary can make sure that the total number of ballots is constant while preventing someone from voting how they want to, all without direct contact between the adversary and their target. This type of attack is preventable by forcing the ballots to remain in plain sight until they are inserted into a ballot box that shows the additional weight. The main drawback of this method is that it requires more equipment, and reduces usability as people have to move around to cast their ballot into the fixed ballot box.

Locked Boxes Small items, such as ballots, tokens, pens, or stamps often change hands in our context, creating opportunities for an adversary to steal or alter them. Identical small boxes with a lock on them can be an effective way to ensure the integrity of items either as they are changing hands or for a certain duration, or to solve *commitment problems*. There is quite a bit of leeway on how to use them, depending on the type of lock. For example, they can easily solve *commitment problems*—and they are generally the baseline example used when designing electronic commitment schemes [27]. One way to use a box is for an agent to put their lock on the box and give it to the voter without giving the key. Once the ballot is put inside the box, the voter closes the lock, and no one can modify the ballot before it is returned to the agent, unless they manage to get the key. Multiple keys can also be used at the same time on a given box. Alternatively, different items (such as empty unique ballots) can be placed in a set of locked boxes, with a key for each box. Then, either the boxes or the keys can be shuffled, before one is assigned to each voter. Although they provide very useful security features, locked boxes add a non-negligible level of complexity as well as time.

Random Drawing Methods Many secure voting schemes require the generation of random permutations. This can be done quite easily physically, and examples abound, such as drawing random items from a bag, common in boardgames (as in Scrabble where one draws letters). This method can be profitably used in boardroom voting, to generate a random permutation between a set of voters and any set of items—such as ballots, papers with secret numbers written on them, coloured pens, or any other small tool. One must be careful to ensure that the items are all identical to the touch with no removable identifiers (such as a sticky piece of paper attached on one side that can be discreetly removed when the item is taken from the bag). To alleviate this problem, locked boxes can be used, and both can be easily combined. To obtain stronger guarantees on the random draw when one uses locked boxes, there can be a succession of shuffles performed by different agents, with all the boxes being visible between shuffles. Although drawing items from a bag has a negligible cost (in time, material and complexity), this latter more secure method is more time intensive.

Cut-and-Choose Cut-and-choose is a mainstay auditing procedure. It works by making duplicates of required items, drawing some (either at random or chosen by an auditor), and examining them thoroughly in public to ensure that they are not maliciously altered. By taking a few items at random, one can make sure that, if a large proportion of all items are deficient, this fact will be detected and the vote will be stopped. It can also be used to reveal part of a secret that is split into multiple sections, as David Chaum's protocol does for electronic cash [10]. The main drawback of this method is that it adds complexity, and requires more materials (more ballots or tools so that some can be removed and publicly examined). The auditing process also takes additional time.

Invisible Ink Invisible ink can be used to strengthen ballot confidentiality in multiple ways and has been used in the Scantegrity [11,13] voting system. We define invisible ink as any ink that is not visible to the human eye without the use of special tools or chemical reactions. The first interest of invisible ink is that it limits the risk of onlookers managing to figure out what a voter is writing while they are writing. A second feature is that it allows the resulting secret to be kept in plain sight during the rest of the voting protocol, including during shuffles, reducing opportunities to alter the ballot. In terms of usability invisible ink has little cost to the voters, but requires more advanced manufacturing and increases costs.

We can also consider time-sensitive invisible ink that automatically becomes visible after a specified period of time, or that disappears after a certain time. The main advantage of using time-sensitive ink is that it might complicate the difficulty of a malicious voter exfiltrating an imprint of their stamp. Time-sensitive inks, however, require the election to proceed along a strict schedule, and they might cause delays waiting for the ink to react.

Polygonal Foldable Ballots and Candidate Wheels As the number of choices in an election increase, the polygonal paper ballot must provide an equal number of edges which may prove impractical when there are many choices, as voters might struggle to remember which sector corresponds to their choice. If that happens—no matter the number of candidates—the voter can either unfold the different labels[4] or request a different ballot if the folding is permanent.

While foldable ballots defeat an adversary relying purely on observation, they do not protect ballots against other types of attacks. Any party able to gain access to ballots before or during distribution can mark or otherwise modify ballots

[4] Unfolding a single label could give away information to a watchful adversary, although it can also be used for misdirection.

to distinguish them later. Using marked ballots, an adversary can defeat both ballot confidentiality and ballot anonymity by correlating marked ballots to individual voters. To prevent correlation of a voter's mark to their ballot, all voters should make their marks using stamps, paper punches, or some other method that does not produce signature-like marks. Moreover, the initial distribution of ballots should be random, in case an adversary made a preliminary mark on the ballots (potentially with invisible ink), and voters should check that their ballot has no identifying marks.

Fig. 4. An example of a foldable paper ballot for a choice between six candidates. Voters fold the edges of the ballot, rotate it, and put a mark on.

An alternative to the polygonal design when there are many candidates is the paper wheel. Instead of having a sheet of paper with two possibilities side by side, voters get a continuous band, as in Figure 5. This design allows them to rotate the wheel such that the candidate of their choice is in the position of their choice. They can then fold the labels, rotate the wheel while keeping track of their choice, and put their mark on it, before casting the ballot. Voters can potentially fold the wheel in two places to obtain a flat double-sheet of paper, making it easier to write on it and cast it into a ballot box. This action should be performed after they fold the labels and rotate the wheel, to prevent an adversary from noticing where the creases are and where they made their mark to obtain how they voted from the order of the candidates. Putting the candidates in random order on the ballot can be useful in general[5], but is not sufficient by itself to prevent the attack.

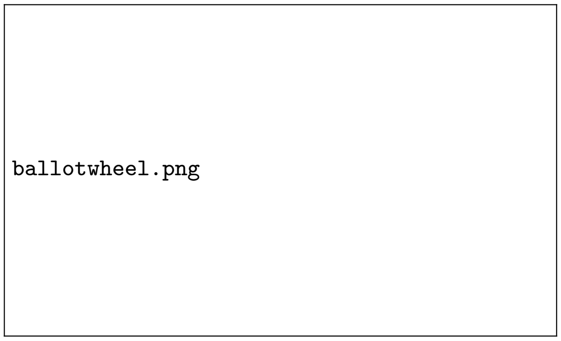

Fig. 5. The candidate wheel, where the voter folds all the labels, rotates the wheel and puts a mark on the cell of their choice before flattening the ballot and casting it into the ballot box.

A.2 Parallel Tallies for Many Candidates or Many Ballot Boxes

The parallel tally ballot can be generalised partially by taking inspiration from the candidate wheel. One possibility is to have two candidate wheels pasted together side by side, with the same ordering of candidates. That is, each row of the wheel has four sections: label, voting space, voting space and label, with a vertical line separating the voting spaces all along the wheel. Once the labels are folded, the voters rotate the wheels, make two marks side by side, and cut the wheels in half along the central vertical line, casting each half-wheel into a different ballot box. In this case, each half-wheel is essentially identical to the candidate wheel shown in Figure 5.

Another, less useful, possibility is to have a sheet of paper with four columns, in the same order as previously, except that the left side corresponds to a vote for the first candidate, and the right side to a vote for the other (with the labels indicating the left and right candidates on each row), as in Figure 6. Once they have folded the labels on the left and right parts and rotated the sheet, voters simply have to put their mark on all the spaces in the left column, or on all the spaces in the right, while being watched by others. They can then cut apart each row and cast each row into a different ballot box.

A.3 Building Blocks Not Used in the Protocol

The next building blocks are not used in our protocol but could serve to develop new protocols.

[5] A random order (and not just a cyclical shift) decreases both the effects of voter errors [35] and position bias [5].

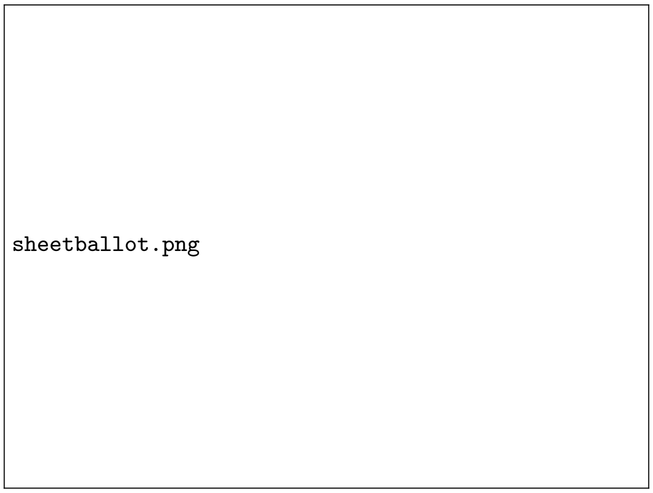

Fig. 6. A ballot that allows parallel elections with three different ballot boxes. Voters fold the labels on each side, rotate the ballot, put a mark on all cells in a column of their choice, cut the ballot in three, and cast each third in a different ballot box.

Removable Opaque Coverings A second way to implement low-tech *commitment* is to use removable opaque coverings. They can come in a few different formats, depending on the properties required. For example, one can use black photo tape, to prevent others from seeing what one wrote until after a certain time. A simple scheme based on this idea is for every voter iteratively to write who they vote for, cover the name with tape, and sign their name somewhere at the bottom of the sheet—not covered by tape—before giving it to the next voter. Once everyone is finished, there is a single sheet with everyone's vote, which an external auditor can then tally without knowing individual votes[6]. There are also alternatives to tape, such as scratch-off systems [23], which require more manufacturing but cannot be put back in their initial state once someone reveals the secret for the first time. Partially see-through envelopes—with a transparent window at a given location within an opaque body can also be used.

Such covering methods can work especially well when combined with random auditing systems such as cut-and-choose. For example, in certain methods, two scratch-off cards can be used, with the voter auditing one at random to check that it is correctly made, and using the second [36].

Visual Cryptography Visual cryptography is a way to distribute secrets and perform secret sharing, first introduced by Naor and Shamir in 1995 [28], and extended afterwards [26]. It works by creating two images on transparent sheets

[6] This simple example method has vulnerabilities, such as the possibility for collusion between the auditor and an adversary inside the room to compare information and obtain individual votes.

of paper, such that the overlap creates readable information. Setting one image to comprise random pixels—as in Figure 7—allows the separation of the initial secret in two physical parts, which only reveal information when together. This method can be used to separate initial secrets into halves to share with different voters or auditors, but it requires the printing of such secrets in advance.

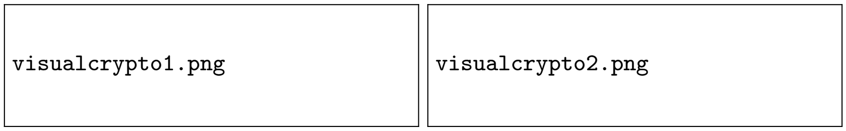

Fig. 7. An example of visual cryptography, where the superposition of both left strips creates the right strip. Public domain image, courtesy of Wikimedia Commons user Blokhead.

Prêt à Voter-style Tearing Off To obtain verifiability and preserve privacy, it can be useful to split in half the ballots used—or the information sheets distributed to voters. This method can, for example, be done as in the Prêt-à-Voter system, with the candidate order shown on the side and being torn off and discarded. The Prêt-à-Voter system requires some electronic components, so it cannot be used directly in our setting. Similar methods can also be used to split secrets in half, and can be used in many protocols. It has negligible costs, although it can lower usability depending on how much there is to tear off. It can also introduce new attacks if the tearing off process creates identifiable edges.

Blind Signatures Blind signatures support the aims of ballot confidentiality and ballot verifiability. David Chaum described a physical implementation of blind signatures through the use of envelopes with carbon-paper linings, allowing a trustee's signature to transfer to a contained document without opening the envelope [10]. Voters begin by marking their ballots and slipping them into carbon-paper-lined envelopes, turning them over to one or more trustees. The trustees verify the identity and the eligibility of the voters as well as the integrity of the envelopes, applying a certifying signature to the envelopes if all seems well. All certified envelopes go into a container which a trustee then shuffles such that an adversary cannot easily correlate any envelope to a voter. Once shuffled, a voter or trustee removes the envelopes from the hat and opens them, tallying the choices.

Opaque, carbon-paper-lined envelopes prevent honest-but-curious trustees from observing the ballots contained within envelopes. Since the envelopes are sealed, malicious trustees damaging the envelope seals will be detected with a high probability. However, they can potentially ruin certain ballots. The whole process also reduces usability as it requires multiple exchanges of envelopes, and requires carbon paper and envelopes.