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

Enka Blanchard, Ted Selker, Alan T Sherman

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

Nikola K. Blanchard[1], Ted Selker[2], and Alan T. Sherman[3]

[1] Digitrust,
Loria, Université de Lorraine Nikola.K.Blanchard@gmail.com, www.koliaza.com
[2] University
of California Berkeley and UMBC,ted.selker@gmail.com, http://ted.selker.com/
[3] Cyber Defense Lab, University of Maryland, Baltimore County (UMBC),sherman@umbc.edu,
https://www.csee.umbc.edu/people/faculty/alan-t-sherman/

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 an initial exploration of boardroom elections with ballot privacy and voter verifiability that use only "low-tech cryptography" without using computers to mark or collect ballots. Specifically, we define the problem, introduce several building blocks, and propose a new protocol that combines these blocks in novel ways. Our new building blocks include "foldable ballots" that can be rotated to hide the alignment of ballot choices with voting marks, and "visual secrets" that are easy to remember and use but hard to describe.

Although closely seated participants in a boardroom election have limited privacy, the protocol ensures that no one can determine how others 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.

Low-tech cryptography is useful in situations where constituents do not trust computer technology, and it avoids the complex auditing requirements of end-to-end cryptographic voting systems such as Prêt-à-Voter. This paper's building blocks and protocol are meant to be a proof of concept that might be tested for usability and improved.

Keywords: Applied cryptography, boardroom voting, foldable ballots, high-integrity election systems, usable security, visual secrets.

1 Introduction

Much 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. Edison's [17] first attempt at a private voting solution is inappropriate as it was for congress where the public needs to know how each participant voted. Many important elections, however, require anonymity but take place where it is easy to see others work, such as around a conference table in a 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.

Such "boardroom elections" typically use paper ballots with limited to no guarantees of ballot privacy, outcome integrity, or coercion resistance. Sitting around a table, for example, it is hard to hide your vote from your neighbour. With sleight-of-hand, anyone handling the ballots might replace a ballot with a fraudulent one without detection. 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.

For example, one of the authors recently participated in a tenure vote during which each of the 22 voters could easily see the ballot choices of nearby voters; anyone could see ballot marks through the folded paper ballots; and ballots were distributed and collected in a chaotic fashion during which anyone could handle the blank and marked ballots. One left-handed voter marked their ballot with distinctive backward checks in red ink. While simple paper ballot elections could be conducted more securely, usually they are not.

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). This paper focuses on low-tech solutions.

We present a 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 simplifies the trust model and does not require the sophisticated cryptographic audits integral to most *End-to-End (E2E)* systems, such as Scantegrity [8,9,13,14] or Prêt-à-Voter [23,32,33]. The independence from electronic tools also ensures limited cost and improved availability in a wide variety of settings, while assuaging widespread concerns about computer malfeasance.

Well-known examples of low-tech cryptography include the following: committing to a secret value by covering it with black photographic tape; encrypting a message by locking it in a safe box; and creating a unique unreproducible tamper-evident seal by randomly sprinkling many tiny sparkles in translucent epoxy glue [35].

The protocol focuses on the following properties: No one can determine how any individual voted, even when observing a voter marking their ballot from close proximity. 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 present a variation of BVP1 in which objecting voters can prove such malfeasance at the cost of some degradation of ballot privacy.

Contributions include: (1) A definition of the boardroom voting problem. (2) New building blocks for boardroom elections, including "foldable ballots" that can be manipulated to obfuscate the alignment of ballot choices with voting marks, and "visual secrets" that are easy to remember but hard to describe. (3) A new protocol for boardroom voting that offers ballot privacy and voter-verifiable outcome integrity.

We recognise that our proposals need to be tested for usability. We offer them, not as an ultimate solution, but with the hope that this initial exploratory work will inspire others to seek additional solutions to boardroom voting.

2 Low-Tech Boardroom Elections

A *boardroom election* is an election that takes place with all voters present in a single room, which shall called 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, a typical boardroom election might involve three 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.

Solutions should be simple, afford ballot privacy, resist undue influence, and provide outcome integrity verifiable by the voters present. In particular, solutions should 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, even with the cooperation of corrupt voters, no one should have the ability to link a marked ballot to the voter who cast it. 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

The assumptions and adversarial model, include characteristics of the room and the adversary's motivations, capabilities, access, resources, and risk tolerance.

3.1 Assumptions

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, or at least their use is prohibited while the election is in progress. Assume that no cameras are hidden or otherwise present in the room. Given that some of our building blocks provide some defence against cameras, this assumption can be revisited. Similarly, 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 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.

During the election, communications among people in the room are not allowed beyond those required for the election procedure. It would be impossible, however, to prevent all such communications completely, possibly including ones sent through covert channels (e.g., hand gestures). 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 is covert and might be a voter or member of the election authority. Multiple adversaries might act in concert, or each for a different — and potentially conflicting — 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. 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.

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

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 [16]. 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. For example, some fraternal organizations vote on each new membership application by "Blackballing" in which, behind a privacy screen, each voter drops either one white ball or one black ball into a collection box.

Today, boardroom voting commonly occurs in classrooms, faculty meetings, and company management or shareholder meetings. Intimidation and fraud are frequent [2,21]. Within the past fifteen years, researchers have proposed several solutions, based on electronic means, including smartphones [4], blockchains [27], authenticated communication channels [19], or insecure devices [1]. Such cryptographic solutions have attempted to improve efficiency [25] or add features such as decentralisation [27], robustness [22], or the possibility of vote delegation [26]. Kahan and Rock [21] examined corporate voting in the United States from a legal perspective. For these previous works, the main defining characteristic of boardroom voting is an election with a small number of voters.

Kiayias and Yung [24] 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 [25] 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.

Essex et al. [18] present the integrity-verification mechanism Aperio for use in minimally equipped secret paper-ballot elections.

Hao [20] 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.

Section 7.6 also discusses a paper ballot system corresponding to what is often done in practice.

5 New Building Blocks

We present three new building blocks for the physical protocol of Section 6: foldable paper ballots, visual secrets, and parallel vote tallying. For additional building blocks, see Section 8.

5.1 Foldable Paper Ballots

To protect ballot confidentiality during ballot marking, we propose *foldable paper ballots*. A paper ballot might consist of two labelled columns, where each column corresponds to a particular choice, which is labelled at both the top and bottom of the ballot (see Figure 1).

To mark a ballot, the voter makes a mental note of the labels for each column and folds the top and bottom portions of the ballot down over the labels to hide them. They might move or rotate it in any way that allows them to remember what is under the part of the ballot the will mark. When rotating their ballot, a voter should prevent adversaries from observing the number of manipulations, for example, by rotating

the ballot beneath a large cloth. The ballot's symmetry adds to the difficulty of an adversary trying to view manipulations the voter makes before marking the outside.

The folding can be temporary or permanent. To prevent an adversary from unfolding the ballot and glancing at a label, part of the paper could be adhesive to make a permanent fold. To make temporary folding more secure (against quickly unfolding the label), the top and bottom parts could be folded twice. A limitation of the foldable ballot is that it requires the voter to remember what is inside a part of ballot and might increase the rate of ballot-marking errors.

The foldable ballot can be generalised to support additional ballot choices by using a polygonal paper ballot or candidate wheel, which is continuous band of paper with candidates on the side.

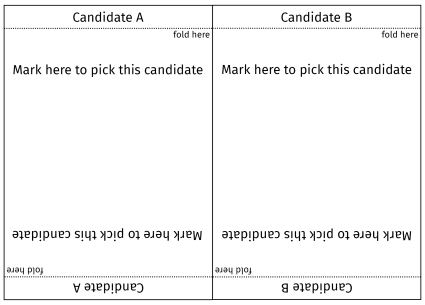

Fig. 1. A foldable paper ballot enables a voter to mark their ballot with privacy in a crowded boardroom. This ballot is for a binary choice between two candidates. The voter makes a mental note of where each label is, folds the edge of the ballot on top of the label, and puts a mark in the zone corresponding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

5.2 Visual Secrets

A voter may use *visual secrets* to enable voters to verify their votes without being able to prove how they voted, A visual secret is an image or pattern that is easy to recognise but hard to describe.

The idea is to use a set of images built with similar patterns though visually different. Each voter could mark their ballot choices with a visual secret. 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 (see Figure 2).

There are several possible ways of marking a ballot with visual secrets, including with stamps, peel-off stickers, or images under a scratch-off covering. Self-inking stamps reduce steps and are indelible (see Section 8.2). Providing each voter with a sheet of peel-off stickers has limitations: the sheet with the remaining stickers reveals which visual secrets were used, and a corrupt or coerced voter could expose the chosen sticker before applying it, The sticker could also potentially be moved or removed. Ballots with scratch-offs require somewhat complex advance planning.

During tallying, all ballots are revealed (e.g., placed on the center of a large table) and each voter can verify their ballot, identifying it by their visual secret. Provided a coerced voter cannot communicate their secret to the adversary before the ballots are all revealed, they are safe. After the ballots are revealed, the coerced voter could tell the adversary they voted according to any other revealed ballot with the desired ballot choice.

One drawback of visual secrets is that some people might forget the pattern or confuse it for another. Also, an adversary might view the visual secret being chosen. Humans have excellent abilities for visual recognition — better than their abilities to recognise strings — especially with short-term memory [28]. Another limitation is that it may be possible to describe the pattern uniquely by describing only a part of it, and doing so might be easier than describing the entire pattern.

Fig. 2. Two examples of visual secrets, which are easy to distinguish and remember but hard to describe orally in a few sentences. These patterns are relatively simple; more complex ones could be used.

5.3 Parallel Vote Tallying

We explain how to hold multiple parallel tallies for the same election by duplicating ballots, with different guarantors for each ballot box. Doing so can reduce the trust required in any single authority responsible for the tallying phase. Voters might suspect that someone could maliciously handle the ballots during this phase. The main challenge is to ensure that the ballots cast into each ballot box are identical; otherwise, parallel tallies could facilitate discreditation attacks.

One solution uses a variation of the binary foldable ballot. In this variation, the space where the voter is supposed to make a mark is split into two columns, vertically (see Figure 3). Once the paper is folded, the voter makes two marks on the same column, 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. This method can be generalised to more candidates using a variation of the candidate wheel [5].

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 (see Section 8). 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.

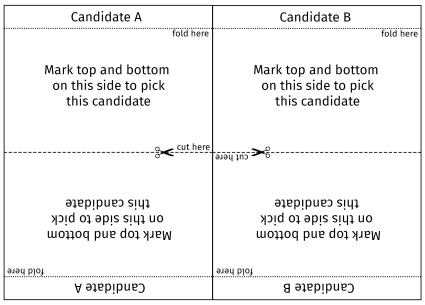

Fig. 3. A ballot design for parallel vote tallying that forces voters to vote for the same candidate in both elections. Each voter makes two marks on the same column, then cuts the ballot in two along the dashed horizontal line, and casts each half in a different ballot box.

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 edge 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 the cell of their choice on their ballot.
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 a 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, checks the vote on each (corresponding to which cell has been stamped), tallies the results, 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. A new election can be taken.

Section 6.2 includes a description of an optional procedure for adjudicating claims of missing visual secrets raised in counting and verification Step 4.

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, albeit slower, would provide slightly better privacy and would better accommodate larger sets of voters.

Rotating ballots under the table. Instead of using opaque cloths, 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, 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.

Section 5.3 describes a mechanism for ensuring that each voter submits the same ballot choices to each ballot box. 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 their unique stamp. Other people in the room can check that each voter stamps two black disks in the same column, 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 in Section 5.3 for parallel vote tallying, 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. They can be saved for election challenges or destroyed to eliminate manipulation before someone challenges it.

7 Discussion

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 in a way that uniquely identifies it, 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 for an alert sighted voter: the voter acquires a ballot, folds it, and manipulates it 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. Throughout the entire voting process, the voter observes activities in the room.

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

A study is needed to determine 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) should 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, or create a crease that makes the ballot 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 or threaten to 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 resolution). The existence of a backup solution and deterrence allows voters to benefit from increased efficiency, while reducing the risk of election annulment.

7.6 Comparison with Paper Ballots

We briefly compare BVP1 with a typical use of simple paper ballots, a protocol we shall call *SPB*. Details can matter greatly in voting protocols, yet SPB rarely is defined by rigorous rules nor carried out in compliance with such rules. We imagine SPB to work as follows: The EA distributes simple paper ballots. Voters mark the ballots, fold them, and toss them in the center of the conference table. With the help of the voters, the EA collects the ballots. Seated at the table, the EA tallies the ballots and announces the tentative tallies. Some voter verifies these tallies. If there are no objections, the EA declares the results official and maintains the marked paper ballots as evidence.

The main advantages of SPB are simplicity, speed, and low cost. Assuming everyone can watch everyone else, SPB also enjoys some outcome integrity. The disadvantages of SPB include very poor privacy (it is easy to see how nearby voters vote, and the collected ballots are not well mixed). Outcome integrity is threatened by sleight-of-hand by anyone touching the ballots (it would be possible for someone to replace cast ballots without detection). As with any system in which voters directly mark ballots, it is virtually impossible to prevent a corrupt or coerced voter from intentionally making a unique identifying mark, tear, or fold on the ballot.

It would significantly improve SPB to implement it using a private voting area and ballot box. For example, there could be a voting table, with a small privacy screen, in one area of the room where voters could mark their ballots one person at a time. A large ballot box in plain view of all could rest on the voting table. At the cost of decreased speed, the private voting area would give voters the option of greatly improved privacy. The ballot box would enhance outcome integrity by not allowing anyone to handle the ballots before counting.

Because the simpler SPB lacks a voter verification step, it is more susceptible than BVP1 is to attacks that replace ballots. When SPB is conducted without a private voting area, BVP1 has significantly stronger privacy properties than does SPB.

7.7 Open Problems

Open problems include (1) Conducting usability tests of the new building blocks and voting protocol. (2) Devising additional solutions to boardroom voting that provide stronger verifiability, better protection against discredidation attacks, or greater simplicity. (3) Finding solutions that work for voters with visual impairments.

8 Additional Building Blocks

We briefly describe selected additional building blocks, which we use in our protocol or which might be useful in designing other physical protocols. These building blocks include pre-existing ones (e.g., invisible ink) and novel uses of existing mechanisms (e.g., stamps).

8.1 Pre-Existing Building Blocks

Pre-existing building blocks include privacy enhancers, locked boxes, transparent ballot boxes, physical commitments, random-draw methods, cut-and-choose, and invisible ink.

Privacy Enhancers. 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. These devices are especially useful in boardroom elections, where all voters can observe each other.

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

Transparent Ballot Boxes. Transparent ballot boxes can be used to detect if a voter inserts more than one ballot or no ballot. Inattentive voters could be fooled by two envelopes being cast at the same time. Such ballot boxes have the small inconvenience of making it potentially feasible to follow each envelope during the shuffling process, especially when there are few ballots.

Physical Commitments. Commitments to character strings or images can be made by occluding them with removable black photographic tape or scratch-off coverings. Objects can be locked in boxes.

Random-Draw Methods. Many secure voting schemes require the generation of random permutations. This process can be easily carried out physically. For example, in some board games, players randomly draw items from a bag (e.g., Scrabble players draw letter tiles).

Cut-and-Choose. Cut-and-choose is a mainstay auditing procedure [10,11]. 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. It can also be used to reveal part of a secret that is split into multiple sections, as does Chaum's protocol for electronic cash [12]. 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 is used in the Scantegrity voting system [13,15]. 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. Invisible ink may have little negative impact on usability, but requires more advanced manufacturing and may slightly increase costs.

8.2 Novel Uses of Existing Mechanisms

We describe novel uses of three existing mechanisms: stamps, scales, and polarising filters.

Stamps. Stamps can be used to imprint special marks on ballots, as needed to implement visual secrets. When using stamps to imprint visual secrets, to mitigate the risk of an adversary seeing the pattern, we recommend two additional precautions.

First, use invisible ink, so that the visual secret is not visible as the voter applies the stamp. Second, use a self-inking stamp that rotates when pushed down (see Figure 4), making the pattern visible only when the stamp is pressed. With this type of stamp, the voter can look at the pattern by pressing it in their hands before their eyes, but neighbours cannot see the pattern. Also, this type of stamp makes showing the pattern to an adversary much more conspicuous.

Customised stamps can be put in a bag and distributed using a random-draw method. Care should be taken that the stamps are used only on the ballots and put on the table afterwards, to prevent voters from keeping proof of how they voted.

Stamping visual secrets requires custom-made stamps, which are inexpensive. The stamps 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).

Fig. 4. An easily available inexpensive self-inking stamping device.

Scales. Putting the ballot box on a mail scale to measure its weight over time can prevent certain attacks by detecting if a voter places more than one ballot into the box.

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 recording the boardroom with hidden cameras harder, as polarised cameras tend to be bulkier or more expensive [31], and the adversary would need to know the orientation of the polarisation. This method has fewer applications, because 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.

9 Conclusion

This paper introduces the study of secure paper based boardroom elections with ballot privacy and voter verifiability using only low-tech cryptography. We propose two new building blocks — foldable ballots and visual secrets — and protocol BVP1 that uses them. This line of research is significant because many important elections take place in boardrooms, and these elections typically are carried out without ballot privacy or voter verifiability. Other modern proposals for boardroom elections depend on complex technology. It is likely that some people and organisations will not be willing to run boardroom elections using complex technology. Despite the imperfections of our initial proposals and the need to test their usability, the proposals offer promise that there may be low-tech methods that provide greater election integrity and ballot privacy than do the simple paper-ballot systems as used in most boardrooms today.

When comparing voting systems, one must consider a variety of factors, including efficiency, simplicity, cost, usability, outcome integrity, ballot privacy, receipt freeness, coercion resistance, voter verifiability, and resistance to discredidation attacks. Whether BVP1 is better overall than the SPB simple paper ballot system (see Section 7.6), depends in part on the context and implementation details. BVP1 is more complex, depends on the unproven security of visual secrets, and is likely more error prone. SPB has serious privacy limitations and offers no voter verification other than the ability of voters to watch each other. The foldable ballot offers a practical way to mark ballots privately while seated nearby peering eyes.

For most boardroom voting systems and settings, hidden miniature cameras pose a significant threat to ballot privacy. Our foldable ballot prevents hidden cameras from discerning ballot choices by honest voters.

Because boardroom voting happens in a wide range of situations with varying financial, timing, and usability constraints, there are benefits in having a variety 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 solutions that avoid certain drawbacks of existing E2E systems including their need for complex audits. We hope that our work will inspire others to discover even better boardroom election solutions, for example, achieving stronger verifiability, improved usability, and greater resistance to discreditation attacks.

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. Blanchard, N.K.: Usability: low tech, high security. Ph.D. thesis (2019)
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. In: Hao, F., Ryan, P.Y.A. (eds.) Real-World Electronic Voting: Design, Analysis and Deployment, (2016)
10. Chaum, D.: Computer systems established, maintained, and trusted by mutually suspicious groups. Tech. rep., Electronics Research Laboratory, University of California, Berkeley, UCB/ERL M79/10 (February 22 1979)
11. Chaum, D.: Computer systems established, maintained and trusted by mutually suspicious groups. Ph.D. thesis, University of California, Berkeley (April 1982)
12. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology. pp. 199–203 (1983)

13. 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)
14. 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)
15. 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)
16. Colomer, J.M., McLean, I.: Electing popes: approval balloting and qualified-majority rule. Journal of Interdisciplinary History **29**(1), 1–22 (1998)
17. Edison, T.A.: Electric vote-recorder. US Patent 90,646 (June 1869)
18. Essex, A., Clark, J., Adams, C.: Aperio: High integrity elections for developing countries. In: et al., D.C. (ed.) Towards Trustworthy Elections, p. 388–401. IAVOSS/Springer-Verlag (2010)
19. Groth, J.: Efficient maximal privacy in boardroom voting and anonymous broadcast. In: Juels, A. (ed.) Financial Cryptography. pp. 90–104 (2004)
20. Hao, F., Clarke, D., Randell, B., Shahandashti, S.F.: Verifiable classroom voting in practice. IEEE Security Privacy **16**(1), 72–81 (January 2018)
21. Kahan, M., Rock, E.B.: The hanging chads of corporate voting. Georgetown Law Journal **96**, 1227–1281 (2007)
22. 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)
23. Khader, D., Tang, Q., Ryan, P.Y.A.: Proving Prêt à Voter receipt free using computational security models. In: EVT/WOTE (2013)
24. Kiayias, A., Yung, M.: Self-tallying elections and perfect ballot secrecy. In: Naccache, D., Paillier, P. (eds.) Public Key Cryptography. pp. 141–158 (2002)
25. 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)
26. Kulyk, O., Neumann, S., Marky, K., Volkamer, M.: Enabling vote delegation for boardroom voting. In: Financial Cryptography and Data Security. Cham (2017)
27. McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security (2017)
28. N. Shepard, R.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior **6**, 156–163 (02 1967)
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. Simmons, G.J.: Contemporary Cryptology: The Science of Information Integrity. Wiley-IEEE Press, Piscataway, NJ (1992)