Secure voting for children

Stefan Popoveniuc
KT Consulting, and
The George Washington University
poste@gwu.edu

***Abstract*—It has been stated that the new class of end-to-end verifiable voting systems is too difficult to understand by the average voter. Even though end-to-end voting systems provide excellent integrity guarantees, they are based on rather complex designs. It is paramount that the general public understands how these systems work, since their design is at the root of the security and privacy properties that they offer.**

We present a physical analogy of an end-to-end verifiable voting system based on a mixnet. Our design should be accessible to elementary school pupils and can be physically built by children.

Keywords: secure voting, end-to-end verifiability, voting with hoses and water.

I. Introduction

End-to-end voting systems such as Prêt à Voter [3], Punch-Scan [6], Scratch&Vote [1] or Scantegrity II [2] provide a set of properties that is unachieved by any of the voting systems which are currently used in public elections. They allow each voter to check that her ballot was cast as intended and recorded as cast, and allow anyone to check that all the ballots have been tallied as recorded. Altogether, they provide a mathematical proof that the tally is produced from all the cast votes. At the same time, the confidentiality of the cast ballot is protected.

We present a physical model for a mixnet-based [4] voting system that is end-to-end verifiable. The system can be built by children and has the same fundamental properties as the electronic end-to-end voting systems. The scope of this paper is to provide a simple explanation and analogy for the concepts which stand at the roots of what can become a new generation of voting systems.

A. Current model for voting systems

To exemplify the potential problems with the current approach in voting systems, we present a simplified model which closely resembles both electronic voting systems, as well as hand counted paper ballots. Having such a model in mind, it can be easily explained why patching this model will not work, and new designs should be used, such as the class of end-to-end verifiable voting systems.

Let's consider the following voting system (described by David Dill [5]): a voter arrives at a polling place, and after proper identification, is given a ballot, and proceeds to the voting booth. In the voting booth there is a human with a paper notebook and a pencil, siting behind a thick black curtain – call him *The Recorder*. Through the curtain, the voter tells *The Recorder* her favorite candidates and gets back a verbal assurance that her vote was cast.

Aside from the privacy problems (because the voice of the voter can be familiar to *The Recorder*), let's consider the problems that can arise with regards to integrity:

- *The Recorder* can write down a totally different vote than that communicated by the voter. This can happen because *The Recorder*:
  - did not hear the choice properly
  - heard the choice properly, but did not like it
  - is a supporter of a particular party
  - made a mistake (e.g. "misspelled" a name)
- *The Recorder* did not write anything at all;
- *The Recorder* wrote down some extra votes for the contests the voter did not vote.

At the end of the day, each *Recorder* counts the votes he recorded and gives totals to the poll workers. The notes of all the recorders along with their declared tally are then transported to the election headquarters and tallied. Results are declared. At this stage problems that can affect the integrity can arise:

- the count done by each *Recorder* is simply wrong
- once *The Recorder* sees the count, it decides to change all the ballots to favor a losing candidate
- the entity that transports the votes from the polling place to the central place
  - changes the ballots in transit;
  - loses some ballots;
  - alters some ballots;
  - injects some ballots;
  - disappears altogether;
- the counting at the election headquarters is wrong;

If the human *Recorder* is replaced by an electronic recorder, i.e. a computer, a Direct Recording Electronic voting system is obtained, a DRE for short. All the attacks described above are still possible. The DRE can capture the vote incorrectly from the voter because of a miscalibrated touch screen or a poorly designed interface, can internally decide to flip votes from one candidate to another or an electrical surge can cause it to simply record the vote with errors or not record it at all.

DREs are black boxes; what happens inside them is extremely difficult to check. Claims can be made on what DREs are supposed to do, but independently checking that they worked properly is difficult. Proper testing before the election, federal and state certification, code inspection and extensive mock elections can detect many of its flaws, but not all of them, and not during an election. While it is possible to

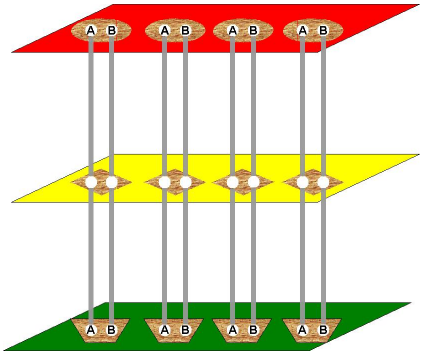

Fig. 1. Three tables on top of each other, four ballots, two candidates.

prove the presence of a bug, the absence of a bug is virtually impossible to prove.

In the case of hand counted paper ballots, *The Recorder* is made of the physical box in which the voters deposit the ballots, along with the poll workers that count the paper ballots at the end of the day. The same attacks are still possible.

The end-to-end model of voting systems departs from the current model and provides mathematical proofs for each step that it performs. Some proofs can be checked by anyone, regardless if they participate in the electoral process or not, and other proofs can be checked by the voters that cast ballots.

B. Organization

There are three basic steps in the voting process: preparing for the election, voting and tallying, and finally, auditing the tally. We describe the physical model of an end-to-end voting system: section II describes the preparations, section III describes the voting and tallying, and section IV describes how the tally is audited.

II. Preparing for the election

As a simple example, we use a ballot with a single contest and two candidates, Alice and Bob. The number of voters in this election is four, thus the number of ballots is also four. The physical model does not scale well to a longer ballot or to more voters, but it is sufficient to introduce all the necessary notions for the computerized model, which does scale to an election that uses a normal size ballot and millions of voters.

The system uses three tables (boards, stands): one red, one yellow and one green. The red table is the highest, at 7 feet above the ground, the yellow is in the middle, at 4 feet above the ground and the green table is the lowest, at 1 foot above ground. The red and the green table are connected with plastic hoses and the hoses go through the yellow table. Figure 1 portraits the setting.

We assume that the hoses are long enough, i.e. longer then the distances between the tables. They may not run straight down and may have multiple folds.

The red table has oval regions cut into it, and in each oval region there is an oval piece of wood. The green table has trapezoid shapes cut into it, and in each hole there is a trapezoid piece of wood. The yellow table has holes cut into it, in the shape of a diamond (rhombus), and in each hole there is a rhombus piece of wood.

There is only one way a trapezoid piece of wood can fit into a trapezoid hole. An oval piece of wood or a rhombus can be put into their respective hole in two ways: at 0 degrees or rotated at 180 degrees. The diamond is not a square, so it is not possible to rotate it at 90 degrees.

There are four holes and four pieces of wood for each table. An oval is connected to a rhombus with two hoses. The rhombus is further connected to the trapezoid with two other hoses. The hoses run in pairs, and in any pair, the hoses are initial parallel (they do not cross). As seen in Figure 1, when all this setup is installed, it looks like three tables one on top of each other, with pairs of hoses coming from the top table, through the middle table and continuing to the bottom table. All the hoses are initially parallel: the left most hose on the top table is the left most hose on the middle table and the left most hose on the bottom table. Same goes for the second left and for all the hoses.

The ovals on the top table represent the ballots. The holes in the ovals where the hoses are connected represent the candidates, and are labeled with Alice and respectively Bob, in this order. The names are written down on paper labels that are affixed to the holes. When all the hoses are parallel, the left label has Alice written on it and the right label has Bob written on it. Every oval has similar labels.

Initially, anybody can check that the order is first Alice and then Bob on all ovals, and that all the hoses are parallel.

A. Possible operations

There are two operations that are possible for the wood shapes: rotations by 180 degrees and switches. On the red table, the ovals are only allowed to be rotated. Switching ovals around doesn't hurt, but doesn't help either. A hole that corresponds to Alice is going to correspond to Bob after the the oval is rotated, and vice-versa[1]. When an oval is rotated twice, the initial state is restored.

On the yellow table, the rhombuses are allowed to be both rotated and switched. By doing a rotation of a rhombus, the order of the holes is flipped, and thus the correspondence with the holes of the ovals and trapezoids is scrambled. The left hole of an oval is not going to correspond to the left hole of a rhombus anymore. Same for the the left holes of an oval and the left hole of a trapezoid.

By switching two random rhombuses between them, the correspondence between a rhombus and an oval, and the correspondence between a rhombus and a trapezoid are also scrambled. The left most rhombus is not going to correspond to the left most oval, or trapezoid.

On the blue table, the trapezoids are only allowed to be switched. It is not possible to rotate a trapezoid, since it would not fit its hole anymore. By switching two trapezoids, the

[1]We ignore the fact that the writing is going to be upside-down when the oval is rotated at 180 degrees

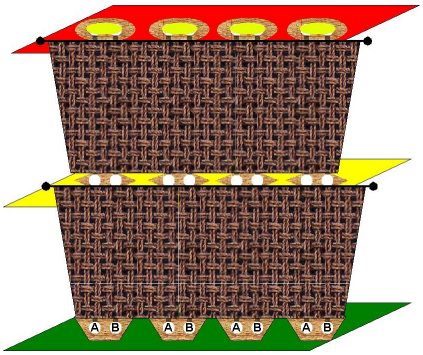

Fig. 2. Hoses are covered with curtains. Ballots are covered with silly putty.

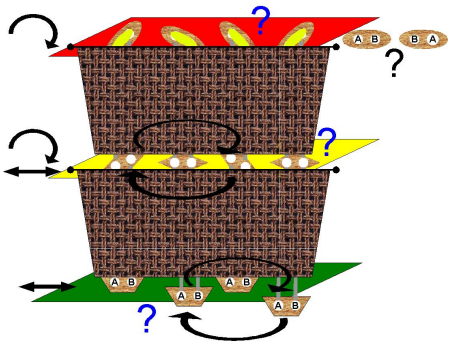

Fig. 3. The ovals are rotated. The diamonds are rotated and switched. The trapezoids are switched.

correspondence between a trapezoid and an oval (on the red table) is scrambled. Remember that ovals are not switched among them, thus switching the trapezoid is necessary to randomize the connection between ovals and trapezoids.

Since trapezoids cannot be rotated, Alice will always correspond to the left hole of a trapezoid and Bob will always correspond to the right hole, regardless of how many rotations and switches are done to all three types of shapes.

B. Setting up the system

In the initial setup, when no wood shapes have been rotated or switched, the left oval corresponds to the left rhombus and to the left trapezoid. Same for the right one, and for the ones in between. Moreover, the left hole of an oval corresponds to Alice. The left hole of a trapezoid always corresponds to Alice. Anybody can check that on all ovals and trapezoids Alice is to the left and Bob is to the right. Moreover, all the connecting hoses run parallel.

After the initial check is done, the following operations are performed:

- The labels on the ovals, which contain the names or the candidates, are covered with silly putty, such that the names are not visible anymore.
- A impressed seal is applied at the top of each silly putty (using e.g. a signed ring or a rubber stamp). This ensures that anybody that would try to uncover the names would have to break the seal.
- The space between the top table and the middle table is covered with a curtain, such that the body of the hoses is covered, but their ends remain visible. Same for the space between the middle and lower table. Figure 2 portraits the setup.
- The people running the election (or, in fact, anyone) are invited one by one to do any number of the four possible operations: rotate an oval, rotate a rhombus, switch two rhombuses, or switch two trapezoids. The operations are done in private, i.e. no one except the person doing the operation is allowed to see what operations are done.

A person that approaches the voting system is not allowed to look behind the curtains, but is allowed to perform any number of operations to any number of shapes. A person may rotate and switch all of them; a second person may choose to only rotate or switch some of the shapes; a third person may choose not to perform any operation, but still pretend that she did.

The number and nature of the operations performed is not known to anyone. A person that approaches the voting system does not know what operations have been performed by the persons before her. Only the first person knows the state in which it finds the voting system, but as soon as the second person approach, the correlation among shapes and among holes may have been randomly scrambled by the first person.

We assume that not all the persons that contribute to the scramble collude, i.e. they do not all tell each other what operations they performed. At least one person keeps secret the random transformations that she performed. A coalition of all but one person cannot figure out the state in which the system is.

Because of the two curtains, no one can know after the switches and rotations which end of the hose connected to the red ovals corresponds to which end of the hose connected to the yellow rhombuses and further to the trapezoids. This is because the trapezoid and the rhombuses have been switched among them.

Because the ovals have been rotated a random number of times, no one knows if, for a particular oval, Alice is on the right or Bob is on the right. Moreover, since the rhombuses may also have been rotated a random number of times, the hose connected to the left hole may go up to a hole that is labeled for either Alice or Bob.

Figure 3 portraits the possible four operations and the inability to follow the correspondences after the operations have been performed.

The curtains are going to always cover the body of the hoses and are never to be removed before the election ends. Instead of curtains, a brick wall can be built around the body of the hoses. However, the ends of the hoses are always visible.

III. Voting and tallying

The voting ceremony consists of the following steps (as shown in Figure 4):

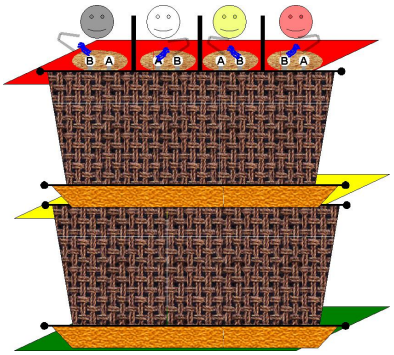

Fig. 4. Each voter is given a glass of water. In the privacy of the both, the voter removes the silly putty and sees the order of the candidates. The voters poor water on the favorite candidate.

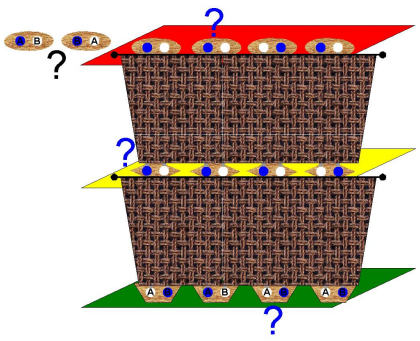

Fig. 5. Results are computable by anyone by looking at the trapezoids. Votes are not linked with voters because the hoses are helter skelter.

1) The yellow and green tables are covered with curtains.
2) Each voter is properly identified. If she has the right to vote and she did not already cast a vote, she is allowed to participate.
3) The voter is given a glass full of water. There is enough water in the glass to fully fill any one hose.
4) The voter approaches the red table and chooses one of the ovals to vote on.
5) The voter inspects the silly putty to see if the seal is unbroken. If the seal is broken, she notifies the election officials and chooses another oval with a valid seal.
6) The voter removes the silly putty and sees the names of the two candidates. There are two possibilities, either the voter sees Alice on the left and Bob on the right, or Bob on the left and Alice on the right. No one else except the voter knows this order.
7) The voter pours the water from the glass into the hole that corresponds to her favorite candidate. Everyone sees where the water is poured, but no one except the voter knows to which candidate the water gets poured into. This is because the ovals has been arbitrarily rotates by many people at the beginning. Also, anyone can see that the voter is only pouring water into a single hole (no over-voting or split votes).
8) The water flows through the hose, until the hose fills. However, the water is not visible at the yellow or green table, since the tables are covered with curtains.
9) The voter removes and shreds the labels that have the names of the candidates written on them.
10) The voter covers the entire oval with remodeled silly putty and, using a steel stylus, places her handwritten signature on the silly putty.

After all the voters have voted, the curtains that cover the yellow and green tables are removed. The role of these curtains is to hide how the water flows down when the voter pours it into a hole of an oval. If these curtains would not exist, an observer would be able see that the water ends up in a particular hole of of a trapezoid (e.g. the left one), and thus that the voter cast a vote in a certain way (e.g. for Alice).

By inspecting which holes in the green trapezoids contain water, anybody can tally the votes. The trapezoids cannot be rotated, because they would not fit their hole anymore. At the beginning, before the ovals were rotated, all the hoses were parallel. That means that, on each trapezoid, the water in the left hose indicates a vote for Alice and water in the right hose indicates a vote for Bob. Thus the vote count is easily done by anyone, by counting how many left holes of the trapezoids have water, and attributing that many votes to Alice. For Bob, the right holes are counted. In Figure 5 we can see that Bob got three votes and Alice one vote, thus Bob wins the election.

Nobody knows how many times each oval has been rotated. Additionally, the labels with the names of the candidates have been removed by the voters. Even if someone sees that there is water in one of the holes of the oval, she does not know to which of the two candidates the water corresponds to. Water in the left hole would correspond to Alice if the oval has been rotated an even number of times, or to Bob if the oval has been rotated an odd number of times.

Also, because the trapezoids were switched among them, no one can know in which particular trapezoid the water from any particular oval ended up (see Figure 5). One cannot say that the left most trapezoid corresponds to the left most oval, since what was initially the third trapezoid is now in an unknown position.

IV. Checking

To make sure that everything went smoothly, an audit procedure is performed. At any time after the election, each voter can make sure that the water that she poured is still there, by simply inspecting the hole she remembers she filled, and seeing if there is water in it or not. If she see that there is no water in there, she can check the signature he made on the silly putty with the steel stylus. If the signature is not there anymore, she has proof that someone tampered with her vote.

No one could have extracted the water from a hose, or injected water into another hose, since any of these two operations would result in the destruction of the signature that the voter did on the silly putty.

The final step is to again audit the physical setup (the first audit of the physical setup was the initial one in which the

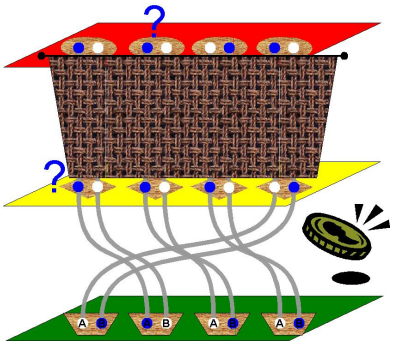

Fig. 6. Auditing the hoses.

order of the candidates and the parallelism of the hoses was verified). Using a stretch of the imagination, an attacker could have caused the water to still be in the holes on the top tables, but the bottom part of the hose to have no water. In other words, there would be a hose for which, one end has water, but the other end does not (e.g. one end is on the red tables and the second one at the yellow table, or one end is at the yellow table and the second one at the green table). While such a scenario does not make a lot of sense in the physical metaphor, it is more than possible in the electronic counterpart.

To make sure that both ends of each hose contain water, an unbiased coin is flipped. If the coin comes up heads, the bottom curtain is removed. If it comes out tails, the top curtain is removed.

Everyone can check that both end of each hose have water and that the hoses run in pairs. If anyone was able to fiddle with the setting, this audit would catch any cheating with a probability of 50%. The audit does not reveal how anyone voted, since there is still a curtain which covers the connections between two of the tables. As seen in Figure 6, even after the audit, any oval could be connected with any rhombus, and the order of the holes could differ (the hoses in a pair may cross).

A. Performing a better audit

If the 50% probability of not detecting a cheater is too low, a different kind of audit can be performed: when looking at the yellow table, an unbiased coin is flipped for each rhombus:

- if the coin comes up heads, then a red fluorescent gas that is lighter then water is injected into the hose with a syringe. The gas travels up the hose and must end up in one of the holes that contains water.
- if the coin comes up tails, then a green fluorescent liquid that is heavier then water is injected into the hose with a syringe. The liquid travels down the hose and must end up in one of the trapezoid's hole which contains water.

In this case, both curtains that cover the space between the tables are left untouched, i.e. they still cover the hoses.

An attacker that managed to fiddle with a single ballot would have to guess which way the coin is going to land for that particular rhombus. He can guess that with probability $50\% = \frac{1}{2}$. To fiddle with two ballots and not get caught, the cheater would have to guess the result of two independent coin tosses; the probability of doing that is $\frac{1}{2} \times \frac{1}{2} = 25\%$. The probability of fiddling with all four ballots and not get caught implies a correct guess for all coin flips, and would thus be $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = 6.25\%$. Thus the probability of this not happening is $1 - 6.25\% = 93.75\%$. In general, the probability that an attacker cheats on k ballots and is not detected is $\frac{1}{2^k}$. For example, for $k = 20$, the probability is lower than one in a million.

This audit still preserves the unlinkability between ovals and trapezoids, since either the top or the bottom part of a hose is checked, but never both parts.

If the audit needs to be repeated, the red gas and the blue liquid is let out, the ovals are left untouched, the rhombuses rotated and scrambled, and the trapezoids are scrambled. The audit is then repeated by flipping the coin again. The trust level can be increased to whatever desired level.

V. Conclusions

We have presented a physical setup that allows voters to cast anonymous ballots and to check that their ballots are not modified after they are cast. The model allows any outside observer to check that the tally has truly been produced from all the recorded ballots.

Our model has all the properties of end-to-end voting systems, except scalability. The advantage of a physical setup is that the process can be intuitively understood by a large number of voters. Our proposed voting system can be physically built by elementary school children.

The physical metaphor closely follows the design of electronic voting systems that use mixnets[4] as a way to anonymize the clear text votes that the voters cast. It offers the same levels of privacy and high integrity assurance.

Scantegrity II is the first end-to-end verifiable voting system which has been used in binding public sector elections, to elect the mayor and city counsel in the city of Takoma Park, Maryland, U.S.A. It is important to explain in simple terms how such systems work to the average voter.

References

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

[2] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity ii: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop*. USENIX Association, 2008.

[3] David Chaum, Peter Y. A. Ryan, and Steve Schneider. A practical voter-verifiable election scheme. In *In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, ESORICS, volume 3679 of Lecture Notes in Computer Science*, pages 118–139. Springer, 2005.

[4] David L. Chaum. Untraceable electronic mail, return address, and digital pseudonym. *Communication of ACM*, February 1981.

[5] HBO. Hacking democracy - movie, 2006.

[6] Stefan Popoveniuc and Ben Hosp. An introduction to PunchScan. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2006)*, Robinson College, Cambridge UK, June 2006.