

A Secure Paper-Based Electronic Voting With No Encryption

Asghar Tavakoly, Reza Ebrahimi Atani

Department of Computer Engineering,
Faculty of engineering, University of Guilan, P.O. Box 3756, Rasht, Iran.
atavakoly@msc.guilan.ac.ir, rebrahimi@guilan.ac.ir

Abstract: *We present a paper-based voting method that attempts to achieve the privacy of voters and election universal verifiability and integrity with only paper ballots and without using any cryptography method. The voting procedure is easy and it needs only selecting the intention of voter over screen of an electronic device. The rest of the voting procedure will be carried out by the device. Voter gets a receipt that can be used to verify that his vote has been counted in final tally as he intended. However the receipt cannot help voter to reveal who he voted for. Also vote selling or coercion is not possible even with the voter's cooperation. The ballot in our voting method has two side, one positive and one negative. Ballots have been prepared for voting in prepackaged form (i.e. 5 ballots per package). Some bubbles of each ballot are prefilled in random way. Numbers of positive and negative filled bubbles are equal with each other and also for each candidate in a package. For example if every package has 30 filled bubbles and if there are three candidates, there would be 10 filled bubbles for each candidate in a package. As it is clear half of those are positive and the other half are negative. The procedure of OneBallot voting is as follows: Voter puts the ballot inside of an electronic device and then he chooses his candidate on the device screen. Then device print another ballot exact same as the original one by one difference; the device fills one positive bubble or unfills one negative bubbles for the selected candidate. First action can be done on the original ballot but the second one needs to print new ballot inevitably. Then device makes a copy from new ballot as voter's receipt and transfers original ballot to the ballot box. After election, there will be a copy from all of ballots in a public board (i.e. a website).*

1 Introduction

In recent decades some electronic voting schemes have been proposed to make election systems more robust and accurate. The two most important properties in all of these schemes are privacy and universal verifiability. First means that it must not be possible track down the relation between ballots and voters (anonymity) and also voter must not be able to prove who he voted for (anti-coercion). The second property means the correctness of election procedure must be clear for everyone. In other words it must be guaranteed that voters' votes have been tallied in the same way that they have intended.

In this paper we introduce a simple paper based voting system. It tries to preserve both properties without using any encryption method. First try in this area was the ThreeBallot voting system that has been

represented by R. L. Rivest. It was remarkable in preserving integrity and privacy of voters and many details in our method have been inspired from it.

Our method is easy to vote for voters by only choosing the favorite candidate on the screen of an electronic device. In next section we explain how the device does rest of the work. Voter gets a receipt and he can use it to check that his vote is included in the final tally or not. We need a public board to put copy of ballots in sight of voters to give them ability of checking their receipts and investigating final result of election.

The paper constitutes following parts: in next part, we explain details of our voting system that consists of structure of ballot, structure of electronic device and also the voting procedure in details. Third part contains security considerations and we explain how our voting system preserves privacy and integrity properties. In fourth part we describe other considerations and finally conclusion and references are in parts 5th and 6th.

2 Details of Voting System

In this part we explain our voting system. It consists of structure of ballot, structure and usages of electronic device and explanation of all steps of voting procedure.

2.1 Ballot Structure

As we illustrated before, each ballot consists of two sides. One of them with white background is positive and the other with gray background is negative. There is three bubbles in each of the sides for each candidate and some of them are prefilled randomly. Number of positive and negative prefilled bubbles for each candidate in a package must be a fixed number. There is also a long number on bottom of each side of the ballot as its ID. It helps voter to recognize his ballot from his receipt after election. Figure 1 shows an example of a ballot for our voting system.

2.2 Electronic Device Structure

The electronic device must have some abilities to precede the voting procedure. It must have a screen to let voters choose their favorite candidate. It must be able to print new ballots

<i>Alice</i>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>
<i>Bob</i>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
<i>Carol</i>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
	2277763907620553	8710945560326719

Figure 1: A ballot sample for OneBallot voting system

with the correct arrangement of filled bubbles in case of unfilling negative bubbles. It also must sign new ballots in a way to make them recognizable from raw ballots. It can do this by putting a particular stamp on the ballot. Refer to figure 2 to see a voted ballot.

2.3 How To Vote

The procedure of voting is as follows:

- 1- First voter gets a ballot and puts it in the electronic device.
- 2- Then the voter chooses his favorite candidate on the screen.
- 3- Device decides to fill a bubble in positive part or unfill a bubble from negative part. If it took second action it must print a new ballot with new arrangement of filled bubbles that has one fewer from original ballot in negative side.
- 4- Next and final step is printing a copy from the ballot as voter's receipt. Then device transfers the original ballot to the ballot box.

3 Security

3.1 Preserving Privacy of Voters

The two most important properties of an election are privacy and integrity. We preserve first one by making voter's intention unrecognizable from his receipt. Coercer cannot find out which mark is voter's intention. Since any combination of prefilled ballots are possible and also the procedure of choosing bubble by device is done randomly. Thus it is not possible to find out who voter voted for from his receipt and it preserves voter's privacy.

There is only one arrangement that making it must be forbidden for device. With a little attention it can be understand that three filled negative bubbles with three empty positive bubbles for a candidate means the voter did not vote for that candidate. Thus the device must not make this arrangement on a ballot.

3.2 Integrity and Universal Verifiability

Preserving integrity is as follows: after election there will be a copy of all the ballots in a public board (i.e. a web site) and also a list consists of name of persons who were present in the election. Number of ballots must be as same as number of voters plus a few more that depends on the last package. For example if we used just one ballot from the last package, number of unsigned ballots is number of ballots in a package minus one.

By revealing ballots anyone can check his receipt with his original ballot to make sure that his vote is present in final tally and it has been tallied as intended. Also anyone can do tallying procedure from scratch by himself for checking correctness of the final result.

Adding or diminishing ballots is not possible because for that to happen list and number of voters must change. Changing the signed ballots is also impossible because it can be notified by voters and it rise the risk of losing the integrity of election. If someone cannot find his copy in the public board exactly as it was, he can fill a protest and deliver it to election official.

<i>Alice</i>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/>
<i>Bob</i>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<i>Carol</i>	<input checked="" type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
	2277763907620553	8710945560326719

Figure 1: A sample for a voted ballot

4 Discussions

There is some important cases that worth to note that we list them here:

- About our voting method it must be mentioned that our method is easy to vote by just selecting the voter's favorite candidate on a screen. So it does not need any necessary education or training for voters.
- Trying not using any encryption method, helps everybody understand what is going on during the election procedure. Unlike to using encryption methods that is not so clear and comprehensible. In this method everyone can scrutinize the ballots by himself to be sure about the correctness of final result.
- There must be a question about number of bubbles. However, our method works with two or even with one bubble per positive and negative sides of a ballot, but it makes creating random patterns a little bit difficult. So any number more than two works fine.
- Sometimes we may need letting voters to vote for more than one candidate, for example in range voting. For this to happen we may need new design for the ballot. For example if in an election five candidate are competing, we need at least five bubbles in each side for both negative and positive sections. Device can make random patterns by choosing aggregate random number of negative or positive bubbles with the same size as selected number by the voter for each candidate.
- Next problem is difficulty in counting or tallying the votes because of plurality of filled bubbles. However if it even may help in some cases when positive and negative filled bubbles are equal for a candidate. This way it does not need to record anything at all.
- The election procedure depends highly on accurate working of electronic device. Without device it is not possible to precede voting procedure.

5 Conclusion

We presented a paper based voting method in easy template for voting and also understanding the security properties for everyone. It is highly verifiable and assures voters that their vote tallied as intended. Everyone can do the process of scrutiny by himself to make sure that final result is correct. It is because tampering ballots is not possible in our method. Besides integrity it is worth to note that privacy of voters is in high degree too. From voter's receipt, no one can find out who the voter voted for and it means there cannot be vote coercion.

It must be mentioned that main idea of this paper inspired from the ThreeBallot voting system that belongs to R. L. Rivest. Thus thank him and anyone who helped and participated in ThreeBallot voting system and examined its security aspects that helped us to review them and consider them in our work.

6 References

- [1] R. L. Rivest, *The ThreeBallot Voting System*, 2006.
- [2] R. A. Fink, *Applying Trustworthy Computing to End-To-End Electronic Voting*, PHD thesis, 2010.
- [3] D. Balzarotti, G. Banks, M. Cova, V. Felmetzger, R. Kemmerer, W. Robertson, F. Valeur and G. Vigna, *An Experience in Testing the Security of Real-World Electronic Voting Systems*, *IEEE Transactions on Software Engineering*, 2010
- [4] F. Yumeng, T. Liye, L. Fanbao and G. Chong, *Electronic Voting: A Review and Taxonomy*, *International Conference on Industrial Control and Elections Engineering (ICICEE)*, 2012.
- [5] R. Kusters, T. Truderung and A. Vogt, *Clash Attacks on the Verifiability of E-Voting*, *IEEE Symposium on Security and Privacy*, 2012.
- [6] R. Kusters, T. Truderung and A. Vogt, *Verifiability Privacy and Coercion-Resistance: New insights from a Case Study*, *IEEE Symposium on Security and Privacy*, 2011.
- [7] A. O. Santin, R. G. Costa and C. A. Maziero, *Three-Ballot-Based Secure Electronic Voting System*, *IEEE Security and Privacy*, 2008.
- [8] B. Adida, *Advances in cryptography voting system*, PHD thesis, MIT department of EECS, 2006.
- [9] F. N. Al-Shammari, A. Villafiorita, K. Weldemariam, *Understanding the Development Trends of Electronic Voting Systems*, *ARES*, 2012
- [10] S. P. Everett, K. Greene, M. D. Byrne, D. S. Wallach, K. Derr, D. Sandler and T. Torous, *Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance*, *CHI*, 2008.
- [11] R. Ara'ujo, R. Cust'odio, A. Wiesmaier, and T. Takagi, *An electronic scheme for the Farnel paperbased voting protocol*, *ACNS'06*, 2006.
- [12] J. Kelsey, A. Regenscheid, T. Moran and D. Chaum, *Attacking Paper-Based E2E Voting Systems*, 2008.
- [13] R. L. Rivest and J. P. Wack, *On the notion of "software independence" in voting systems*, 2006.
- [14] B. Randell and P. Y. A. Ryan, *Voting technologies and trust*, *IEEE Security and Privacy*, 2006.
- [15] P. Y. A. Ryan and T. Peacock, *Pr'et `a Voter: A system perspective*, *University of Newcastle*, 2005.