*Cryptologia*, 33:283–291, 2009

ISSN: 0161-1194 print
DOI: 10.1080/01611190902894946

Taylor & Francis
Taylor & Francis Group

# Accessible Voter-Verifiability

DAVID CHAUM, BEN HOSP, STEFAN POPOVENIUC, AND POORVI L. VORA

**Abstract** All voter-verifiable voting schemes in the literature require that the voter be able to see and to mark. This paper describes modifications to the Prêt à Voter and PunchScan schemes so that a voter who can either see or hear, or both, independent of marking ability, may avail of voter-verifiability without revealing her vote. The modified systems would provide privacy and integrity guarantees that are currently available only to voters who can both see and mark.

**Keywords** Prêt à Voter, PunchScan, voter-verifiable, voters with disabilities, voting



## 1. Introduction

Newly-proposed voter-verifiable voting systems provide strong tally-correctness guarantees without requiring a trusted voting machine or a strict chain of custody for votes. A key contribution of these systems is the ballot encryption step, where voters encrypt their own ballots, without accessing computational power, by marking specially-designed paper ballots. This step, crucial to the integrity properties of the systems, requires that the voter be able to see *and* to mark. This paper describes slight modifications to two of the most popular voter-verifiable systems—Prêt à Voter [4] and PunchScan [12]—that would allow voters who can either hear *or* see (independent of marking ability) to independently encrypt their ballots and thus avail of privacy and integrity guarantees available to other voters. Additionally, these modifications would also retain the privacy of voters who choose human assistance to mark their votes. This is not possible with any other voting system, and is particularly useful, as assistive devices for marking votes can be somewhat intimidating to use.

The importance of the modifications we propose cannot be overstated. The choices available today to voters with disabilities are severely limited, consisting mainly of specialized user interfaces for voting on direct-recording electronic (DRE) voting machines or paper ballots. DREs are known to have several security vulnerabilities [11], and simple paper ballots require a very strict chain of custody. Further, if a voter requires human assistance on using the specialized interfaces, it often comes at the cost of vote privacy. In contrast, voters who can see and mark can use the voter-verifiable systems that have been implemented [4, 12, 7, 6]; of these, PunchScan has been used for binding elections [2], and Scantegrity II [6] is being

Address correspondence to Poorvi L. Vora, Department of Computer Science, Academic Center, 801 22nd Street NW, Washington, D.C. 20052, USA. E-mail: poorvi@gwu.edu

**Table 1.** No visual disability

| | Hearing disability | No hearing disability |
|---|---|---|
| Inability to mark | ✓ | ✓ |
| No inability to mark | ✓ | ✓ |

**Table 2.** Visual disability

| | Hearing disability | No hearing disability |
|---|---|---|
| Inability to mark | × | ✓ |
| No inability to mark | If able to use Braille | ✓ |



considered for use in governmental elections in the US. To rectify the inequity, the modifications we propose will make available the security and privacy guarantees of the voter-verifiable systems to voters with disabilities; additionally, if voters seek human assistance on the use of these modified systems, they may do so without compromising privacy. Note that our modifications ensure that, once cast, a vote would not be identified as coming from voters with a particular ability (to see, hear or mark).

Tables 1 and 2 indicate the accessibility of the systems after the proposed modifications. A tick mark indicates that the systems can be used (without taking recourse to the use of Braille, which is not commonly understood), a cross that they cannot. At this time, the only way to provide accessibility to voters who can neither see nor hear involves the use of Braille. Note that the issue of system usability is outside the scope of this paper, which focuses only on demonstrating that the sense of sight and the ability to mark are not both necessary for voter-verifiability.

Table 3 describes the properties of various types of voting systems that can be used with specialized user interfaces. The properties are for those groups of voters with tick marks in Tables 1 and 2.

The rest of this paper is organized as follows. Section 2 describes related work. Section 3 describes the Prêt à Voter [4] and PunchScan [12] systems. Section 4 describes the modifications to the original systems that increase system accessibility, and Section 5 provides conclusions.

**Table 3.** Voting system properties

| | DREs | DREs with paper trails | Paper ballots | Modified PaV/ PunchScan |
|---|---|---|---|---|
| Tally verifiability | × | Some, using manual recounts requiring strict chain of custody | Some, using manual recounts requiring strict chain of custody | ✓ |
| Privacy if voter chooses human assistance | × | × | × | ✓ |

## 2. Related Work

Several voter-verifiable systems provide vote privacy and tally verifiability guarantees to voters who can see and mark, without requiring that the voting machine be trusted [5, 15, 8, 14, 4, 12, 3, 7, 6]. These systems do not require a chain of custody on the votes or voting machines, and enable the voter to verify the tally without trusting any entity involved in the vote tallying process. The Voting-on-Paper Assistive Device (Vote-PAD) [1] enables voters with visual or dexterity impairments to complete paper ballots. The device consists of a plastic ballot-sleeve, tactile indicators and an audio tape recording, customized for each election and ballot design. Similar devices, called Tactile Ballots, have been used in elections in Rhode Island [10]. Prime III [9] provides a multimodal interface to a voting machine with a voter-verifiable video audit trail (VVVAT) that is a video record of all interactions with the voting machine. The multimodal interface enables independent voting by voters with varying abilities, and the video audit trail, if assumed to be independent of the untrusted voting machine, provides a check on the voting machine. However, the tally correctness of voting using paper ballots, or DREs with manual audits, or Prime III, is completely dependent on the chain of custody (of the ballots or the audit trail), and is hence not voter-verifiable.



## 3. Overview of Voter-Verifiable Voting Systems

The voter-verifiable voting systems we consider—Prêt à Voter [14, 4] and Punch-Scan [12]—may be generalized to one type of system as follows (see [13]). A voter's ballot consists of two parts: the key and the encrypted ballot. The voter uses the ability to mark to fill up her ballot. Ballot design ensures that, in the process of filling up the ballot, the voter encrypts her vote without access to automated computational power. The voter uses sight to verify that the encryption is correct, this too does not require access to trusted computational power. The encrypted ballot is used by the voter as a receipt, and forms the input to the virtual ballot box which is publicly accessible. All encrypted ballots in the ballot box are decrypted and tallied in a privacy preserving and verifiable manner, using standard cryptographic primitives. Interested voters and observers may convince themselves, using software written by any entity they trust, that the decryption, and the resulting tally, is correct.

We will focus on the design of the two ballot parts and on vote encryption, which form the user interface for the ballot casting process. Because the process of marking encrypts the ballot, and sight is required to verify correct encryption, it is not immediately obvious that voters who cannot see or voters who cannot mark can use the systems without revealing their votes. We propose modifications so that voters who can either see or hear (independent of marking ability) may also generate a correctly encrypted receipt, using specialized user interfaces or human assistance, without losing privacy. The verifiable decryption and tally processes, on the other hand, are typically verified by all voters using software, and these would be verified by those who cannot see, or those who cannot mark, in the usual way they would access computational power, such as for email or web browsing, using specialized user interfaces. We will hence not discuss the decryption and tally processes.

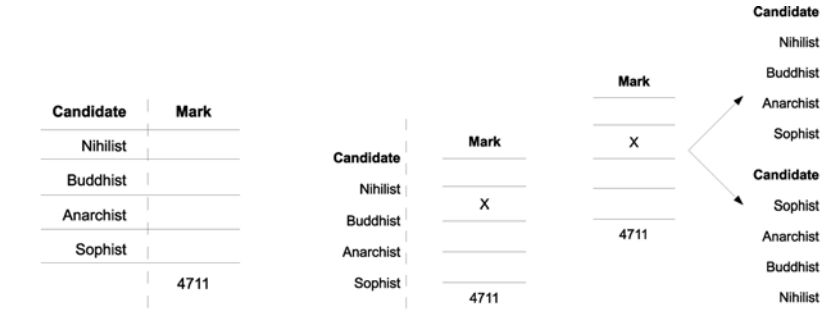
### 3.1. Prêt à Voter

The Prêt à Voter ballot consists of two ballot halves placed side by side; the left half contains the candidate names in pseudo-random order, and the right half contains the mark a voter places next to the chosen candidate(s). After marking the ballot, the voter separates the two halves along a perforation, destroys the left half in the presence of a polling official, and makes a copy of the right half before casting it as her encrypted ballot (see Figure 1). She also takes a copy of the right half as her receipt. The right half also bears a string of symbols which form the *onion*; it contains encrypted information on the pseudo-random order of the candidates, and is used by a mixnet to decrypt the vote. If the encryption function used for the onion and the pseudo-random function used for candidate order are both assumed secure, and at least one entity in the mixnet is assumed honest (does not reveal the keys and performs a secret shuffle), the privacy of the vote is ensured. The voter who wishes to verify that her vote is indeed in the virtual ballot box as encrypted may check her receipt against the public virtual ballot box, or entrust this task to any entity of her choice.



### 3.2. PunchScan

The PunchScan ballot consists of two ballot layers placed one underneath the other. The lower layer contains dummy variables (such as letters of the alphabet) placed pseudo-randomly from left to right. The upper layer contains a map between the candidates and the dummy variables; the upper layer also has holes in it that expose the dummy variables on the lower layer. The voter marks the hole(s) that contains the dummy variable associated with her choice of candidate(s); the mark made by the voter is visible on both layers (see Figure 2). The upper layer hence bears a mark for the position of the chosen dummy variable, and the lower layer bears a mark for the dummy variable as well as the position. Notice, however, that no single layer by itself can be used to determine the vote; in particular, each layer bears an encryption of the vote. The voter chooses which layer to cast (before seeing the layers), and the other layer is destroyed after the ballot is filled in. The voter also obtains a copy of the cast layer as her receipt. The encrypted ballot is decrypted by a shared authority. As with

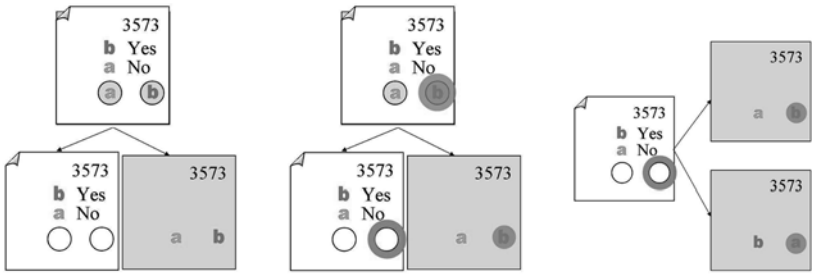



(a) A sample Prêt à Voter ballot. A permuted list of candidates is on the left

(b) A voted Prêt à Voter ballot. When the right side is separated from the left side the mark is not a clear vote anymore

(c) Given only the right side, the mark is equally likely to represent a vote for any candidate.

**Figure 1.** Prêt à Voter ballot.




(a) A sample PunchScan ballot. When the two pages are overlayed, the symbols on the bottom page are visible through the holes.

(b) A voted ballot. Looking at each layer individually, one cannot say that the mark is for "Yes" or for "No".

(c) Given only one layer of the ballot, the marks on that layer are equally likely to represent a vote for any candidate.

**Figure 2.** PunchScan's ballot.



Prêt à Voter, the encrypted ballots are stored in a virtual ballot box, and voters may check that their encrypted receipt is in the box.

## 4. Modifications for Accessibility

In this section we present modifications to the ballot casting ceremony, and to the manner of ballot presentation, to improve the accessibility properties of both systems. The sense of hearing is not required for the regular voting process proposed by PunchScan and Prêt à Voter, hence voters who cannot hear, but can see and mark, are not limited by the regular versions of these systems. Because these systems, however, do assume voters can see and mark, we describe how they may be modified for those voters who can see or mark but not both, and for those who can neither see nor mark. Note that the ability to distinguish among colors is not currently required for the use of either Prêt à Voter or PunchScan. Note also that, for those with low vision who would be able to see well with larger font sizes on a screen, both Prêt à Voter and PunchScan may easily be used with a good magnifying glass. Hence, our modifications for those who cannot see may not be required by those whose visual disability is restricted to color blindness, and/or can be addressed through the use of a magnifying glass.

### *4.1. General Approach*

The two parts of the ballot form the plaintext vote when placed in a certain manner; for example, placed side by side as in Prêt à Voter, or one on top of the other as in PunchScan. It is this required arrangement that generates a barrier for the blind voter; a sighted voter simply arranges the ballot parts to view her plaintext votes. In our modifications, the ability to hear is used as a substitute for the ability to see, and we do not assume that voters know Braille, as knowledge of Braille is not very common. In Section 4.3 we describe how the ballots may be presented to the blind voter using the ability to hear. There is no direct substitute for the ability to mark; however, if the voter unable to mark can see, she can be aided by a helper. Because, in both systems, the voter may communicate the encrypted vote to a helper (we describe how in more detail in Section 4.2) her vote is private with respect to the helper. A voter who can neither see nor hear would need a helper to mark the

ballot; the vote would not be private with respect to this helper unless the voter can use Braille. Finally, the encrypted receipts essentially contain information about the mark placed by the voter, and auxiliary information, such as serial number and onion. This information can be stored and displayed in a manner that does not retain the manner of casting of the vote.

It is worth noting that the clear text ballots produced after the decryption are indistinguishable regardless of the way they were cast (using an accessible interface or not), since no link between any clear text ballot and any encrypted ballot is revealed. Thus, even if information was retained on how a ballot was cast, this information would not reduce the privacy of the voter.

### *4.2. Voters Who Can See but Not Mark, Regardless of Hearing Ability*

In this case, the voter must mark the ballot through a helper, or by using a computer through an interface operable through devices such as sip-and-puff devices. In either case, vote privacy is retained. Note that, in existing systems, voters who cannot mark are forced to use sip-and-puff devices in order to obtain privacy. Additionally, all existing systems that can be used by voters who cannot mark depend on a strict chain of custody for tally integrity and do not provide voter verifiability.

If the voter will use a helper, prior to her entering the polling booth, a photocopy is made of that half of the ballot which will be marked and retained as a receipt. In PunchScan, it is a half chosen by the voter, in Prêt à Voter, it is the right half. A helper accompanies the voter into the booth. The voter examines her ballot and decides how she would mark it, then signals (or tells) the helper which spaces to mark. The helper only has one half of the ballot, so this does not tell him anything about the voter's vote; the vote is already encrypted before being communicated to the helper. The voter then destroys both her ballot halves, and the helper's page is scanned and given to the voter as a receipt. It is not strictly necessary for the voter to have an extra copy of her chosen page inside the voting booth. If no photocopier is available, the helper can take the chosen page into the booth and the voter can bring the unchosen page. However, this may increase the chances of the voter making an error.

The voter may also use a sip-and-puff device to interface with a computer. The part of the ballot that will become the receipt, instead of being provided to a helper, is scanned into a computer, and the voter uses a sip-and-puff device to mark her choice. The marked half of the ballot is then printed, and this forms the receipt. In either case, the computer now contains the encoded choice of the voter, which is simply the position of the mark.

### *4.3. Voters Who Can Hear but Not See, Regardless of Marking Ability*

These voters will use an audio system to vote; that is, the sense of sight will be replaced by the sense of hearing. No helper will be required. The blank ballot (both halves) is scanned, and two computer-generated vocal tracks are created (one for each half). The voter listens to these vocal halves over a set of headphones. In the case of Punchscan, the top half will be played first, telling the voter the symbol for each option (for example, "Yes is *b*, No is *a*"). The voter will listen and make a mental note of the symbol for her choice. Next, the bottom half will be played, telling the voter the order in which the symbols appear (for example, "The first symbol

is *a*, the second is *b*''). The voter will be listening for the symbol she remembers as associated with her choice. When she hears the correct symbol, she says aloud the location of the symbol (for example, ''second''). In the case of Prêt à Voter, the left half will be played, with option order (for example, ''the first option is Nihilist, the second is Buddhist, . . .''). When the voter hears her choice, she says aloud the location of the choice (for example, to vote for *Buddhist* in this case, she says ''second''). What the voter says out loud is recorded as her cast ballot, along with the onion or serial number. She may choose to make two such recordings and cast only one vote, while auditing the other one to determine that the onion is correctly recorded. The voter will also be provided a signed audio receipt by the polling place, which she can take home as her receipt.

On the surface, this seems to create a situation where blind voters' ballots will be distinguishable from other ballots on the bulletin board because they are in a different format (i.e., audio rather than image). However, recall that the raw scanned ballot images are not actually posted on the bulletin board, because that would allow voters to make extraneous marks or smudges on their ballots, facilitating coercion attacks. Instead, a computer-generated ''idealized'' ballot image is generated on demand. Similarly, a computer-generated ''idealized'' audio ballot can be generated on demand for any ballot on the bulletin board. Because all ballots can be both viewed as an image and heard as audio, blind voters' ballots are not identifiable. While decrypting the ballots to produce the clear text votes, the information about how the ballot was cast in the first place is lost; the clear text ballots produced are indistinguishable regardless of the way they were cast (using an accessible interface or not). Thus, the encryption of the vote itself provides protection against privacy loss, regardless of whether it is possible to distinguish the manner of vote casting from the encrypted vote.

As a further refinement, the audio tracks for PunchScan can be interlaced and played together for the voter as follows. The first symbol on the bottom page is read (''The first symbol is *a*.''), followed by the choice associated with that symbol on the top page (''The symbol for ''No'' is *a*.''). This will remove the need for the voter to remember the symbol they heard from the top page until she hears it again on the bottom page. Unfortunately, this involves listing the candidates in random order, which may run afoul of laws in some jurisdictions requiring candidates to be listed on the ballot in some specific order.

### *4.4. Voters Who Cannot See or Hear, but Can Mark*

Voters who cannot see or hear must have a way to have information communicated to them. For example, if the voter knows Braille, she can receive Braille ballot pages. She can then choose to mark the ballot herself or only communicate her encrypted vote to her helper, thus availing privacy.

### *4.5. Voters Who Cannot See, Hear, or Mark*

Voters who cannot see, hear or mark have a difficult time having both information communicated to them as well as having them communicating information to others. This community of voters would require a human helper that would mark and cast the ballot. It is likely that a helper will also be needed to help such a voter verify her receipt. We are not able to modify the systems for this community of voters.

## 5. Conclusions

We have described minor modifications to PunchScan and Prêt à Voter to enable their use by those can either hear or see. We hope that it will soon become standard practice to present voter-verifiable voting schemes in a manner that does not present barriers to particular communities, such as the community of blind voters, and the community of voters with mobility-related impairments that make it difficult to mark votes.

## About the Authors

David Chaum, widely recognized as the inventor of electronic cash and techniques that more generally let individuals protect their privacy in interactions with organizations, has also made fundamental contributions related to the theory of cryptography. He has taught, led a crypto research group, launched several conferences as well as international projects, and founded DigiCash and the International Association for Cryptologic Research (IACR). Chaum has a PhD in computer science from the University of California, Berkeley.

Ben Hosp is pursuing a doctoral degree in Computer Science at GWU. His field of research is electronic voting, and he has developed a model for evaluating and comparing voting systems using Shannon information theory. In 2003, he graduated magna cum laude with a BS in Computer Science from Roanoke College, where he was a member of the Alpha Chi national honors society and the Pi Mu Epsilon mathematics honors society. In 2003 and 2004, he wrote most of ''Citizen-Verified Voting,'' the first non-commercial voter-verifiable election system. From 2005–2007, he was an ARCS (Achievement Rewards for College Scientists) scholar.

Stefan Popoveniuc has successfully defended his doctoral dissertation at The George Washington University. His areas of interest are computer security and privacy in general, and electronic voting in particular. He has designed and built four complete voting systems, and is a member of the Punchscan team, which won first place at the 2007 intercollegiate voting systems competition, VoComp. Popoveniuc has a BS in computer science from Politechnical University, Bucharest, Romania.

Poorvi L. Vora is Assistant Professor in the Department of Computer Science at The George Washington University. She received the B. Tech degree in electrical and electronics engineering from the Indian Institute of Technology, Bombay, India, in 1986, the MS and PhD degrees in electrical engineering from North Carolina State University, Raleigh, NC, USA, in 1988, and 1993, respectively, and the MS degree in mathematics from Cornell University in 1990. Her areas of interest are electronic voting and cryptology.

## References

1. Accessible voting without computers. http://www.vote-pad.us/. (Accessed May 19, 2009)
2. Punchscan. 2006. http://www.punchscan.org/. (Accessed May 19, 2009)
3. Adida, B. and R. L. Rivest. 2006. Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting. In *WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society*, New York, NY: ACM Press, pp. 29–40.
4. Chaum, D., P. Y. A. Ryan, and S. A. Schneider. 2004. A Practical, Voter-verifiable Election Scheme. Technical Report CS-TR: 880, School of Computing Science, Newcastle University.

5. Chaum, D. 2004. Secret-Ballot Receipts: True Voter-Verifiable Elections, *IEEE Security and Privacy*, 2(1):38–47.
6. Chaum, D., R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, and A. T. Sherman. July 2008. Scantegrity ii: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *USENIX/ACCURATE Electronic Voting Technology Workshop*.
7. Chaum, D., A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora. May/June 2008. "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting," *IEEE Security and Privacy, Special Issue on Electronic Voting*, 6(3):40–46.
8. Chaum, D., J. van de Graf, P. Y. A. Ryan, and P. L. Vora. Secret ballot elections with unconditional integrity. IACR Cryptology eprint archive report, 2007/270.
9. Cross, II E. V., Y. McMillian, P. Gupta, P. Williams, K. Nobles, and J. E. Gilbert. 2007. Prime iii: A User centered voting system. In *CHI '07: CHI '07 Extended Abstracts on Human Factors in Computing Systems*, pp. 2351–2356.
10. Fresolone, M. Tactile ballots alternative voting method for the blind. http://www.votersunite.org/info/tactileballots.asp. (Accessed May 19, 2009)
11. Kohno, T., A. Stubblefield, A. D. Rubin, and D. S. Wallach. 2004. Analysis of Electronic Voting System. In *Security and Privacy*, 2004. Proceedings 2004 IEEE Symposium on 9–12 May 2004, pp. 27–40.
12. Popoveniuc, S. and B. Hosp. 2006. An Introduction to PunchScan. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2006)*. Cambridge, United Kingdom: Robinson College, pp. 28–30.
13. Popoveniuc, S. and P. L. Vora. 2008. A framework for secure electronic voting. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2008)*. Belgium.
14. Ryan, P. Y. A. 2004. A Variant of the Chaum Voter-verifiable Scheme. Technical Report CS-TR: 864, School of Computing Science, Newcastle University.
15. Vora, P. 2003. David Chaums's voter verification using encrypted paper receipts. Newcastle Upon Tyne, United Kingdom: Newcastle University, http://www.seas.gwu.edu/poorvi/Chaum/Chaum.pdf