

41506 - Seminar Cryptography and Data Security

Punchscan: Digital voting scheme with paper-based receipts

Michael Senn michael.senn@students.unibe.ch — 16-126-880

2022-12-07

Lorem ipsum dolor si amet, et conijunctur.

1 Introduction

This report provides an overview of the Punchscan voting system. It aims to explain the utilized concepts, point out shortcomings, and highlight some of the attacks which have been published since.

2 Ballot design and voting

This chapter will describe both the ballot design as well as the voting process from the perspective of the voter.

2.1 Ballot design

A punchscan ballot consists of two pages stacked atop each other, shown in figure 2.1. It is uniquely identified by a numerical ID, printed on both pages. The top page contains the question asked as well as all possible answers, with each answer being mapped to a symbol — in this case the letters ‘a’, ‘b’ and ‘c’. The bottom page contains the same symbols, which can be seen through cutouts in the top page when stacked atop each other. Both the mapping of answers to symbols on the top page, as well as the order of symbols on the bottom page, are independent random permutations per ballot.

| | |
|--|---|
| <div>ID: 007</div> <div>What is your favourite prime?</div> <div>b) 2 a) 3 c) 65535</div> <div><input type="radio"/> <input type="radio"/> <input type="radio"/></div> | <div>ID: 007</div> <div></div> <div><input type="radio"/> c <input type="radio"/> b <input type="radio"/> a</div> |
|--|---|

Figure 2.1: Punchscan ballot consisting of top (left) and bottom (right) page

2.2 Voting process

After having identified themselves at the polling place, a voter will have to commit to getting to keep either the top or the bottom page of the ballot as a receipt. They will then receive a random ballot, consisting of a top and bottom page stuck together. The voter will read the question and decide on their answer, and then look for the symbol corresponding to their answer through the holes in the top page. They will mark their answer using a dauber — a huge highlighter as used in Bingo — thereby leaving a stain on both the top as well as the bottom page of the ballot. The effect of having marked their choice is shown in figure 2.2.

The voter will then destroy the page they did not intend to keep by feeding it through a shredder. The remaining page is scanned by a poll worker. The voter gets to see and confirm that the scanned page, including an automatic evaluation of which field was selected, matches their choice. If they agree with the shown choice, they get to leave, keeping the scanned half of their ballot as a receipt.

| | |
|--|----------------|
| <p>What is your favourite prime?</p> <p>b) 2 a) 3 c) 65535</p> <p><input type="radio"/> <input type="radio"/> <input checked="" type="radio"/></p> | <p>ID: 007</p> |
| <p><input type="radio"/> c <input type="radio"/> b <input checked="" type="radio"/> a</p> | <p>ID: 007</p> |

Figure 2.2: Top (left) and bottom (right) pages of ballot after voter marked their choice