41506 - Seminar Cryptography and Data Security

Punchscan: Digital voting scheme with paper-based receipts

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

2022-12-11

Lorem ipsum dolor si amet, et coniunctur.

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.

Chapter 2 will start by introducing the layout of the ballot as well as the process of voting from the voter's point of view.

1.1 Notation

1.1.1 Permutations

Permutations will be denoted by the letter π, with an index describing their purpose. As an example, π_{top} will be used to refer to the permutation of the ballot's top page. We will use the standard one-line notation where, for a permutation over elements $\{a, b, c\}$ with the canonical ordering, $\pi = cba$ refers to a permutation π such that $\pi(a) = c$, $\pi(b) = b$, and $\pi(c) = a$. For a permutation over two elements we also use the notation as in the paper, where $\rightarrow$ is the identity permutation and $\circlearrowright$ is the permutation flipping the two elements. Composition of permutations is denoted as $\pi_1 \circ \pi_2$, evaluated right-to-left.

2 Ballot design and voting

This chapter will 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.

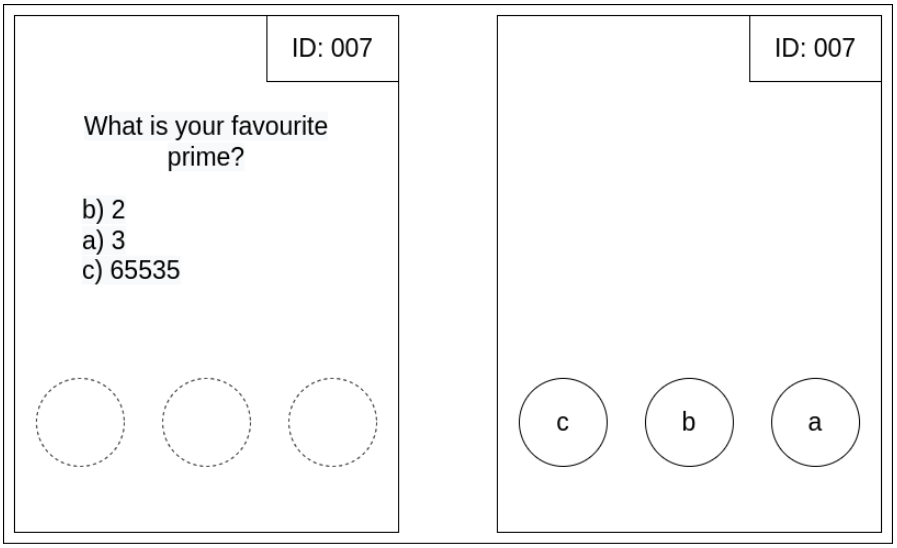

Figure 2.1: Punchscan ballot consisting of top (left) and bottom (right) page

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 leave, keeping the scanned half of their ballot as a receipt.

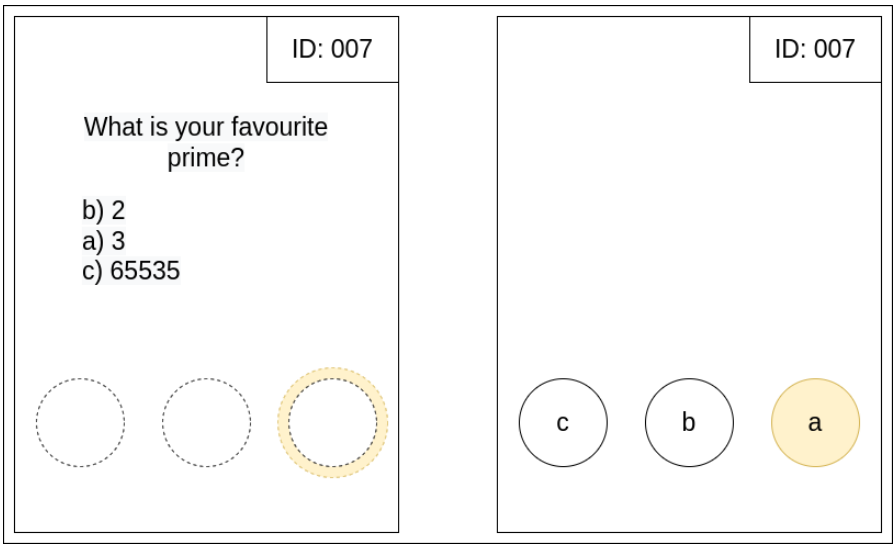

Figure 2.2: Top (left) and bottom (right) pages of ballot after voter marked their choice

3 Setup

During the setup phase, the election authority will initialize the contents of three tables. This will be followed by an audit, to ensure honesty of the election authority. The three tables which are initialized are referred to as the **P**, **D** and **R** tables:

***P*rint table** Contains all information which is required to print the ballots, along with information for auditing purposes.

***D*ecryption table** Contains all information required to decrypt the voter's encrypted vote in the tally phase, along with information for auditing purposes.

***R*esults table** Contains outcome of election.

For the following, we will assume an election with one question, answer possibilities a and b, voted on by n voters.

3.1 Election authority in a threshold setting

For the purpose of this chapter we assume the election authority to be a single entity, in full possession of their private keys. In a real-life deployment it would be prudent to utilize some form of threshold cryptography to spread the trust across multiple parties.

3.2 Initializing the P table

The election authority first populates $2n$ rows of the P table as shown in table . This table is indexed by a primary key ID_P, corresponding to the ballot ID which will be printed on both pages of the ballot. It then picks two random permutations π_{top} and π_{bottom} over 2 elements, corresponding to the permutations of the top and bottom pages respectively. Permutations are chosen as described in , but will be shown explicitly here.

For each row it then calculates two cryptographic commitments, $Com(\pi_{\text{top}})$ and $Com(\pi_{\text{bottom}})$, to π_{top} and π_{bottom} respectively.