

Two more Approaches towards Receipt-Free Voting ...

**and why they fail in
the standard model**

Martin Hirt

ETH Zurich

Standard Model

What it is ...

- bilateral (synchronous) unreliable channels,
- PKI,
- bad guys can see all channels at all time,
- no physically secret channels,
- no physically secure modules.

Why *Standard-Model*

- sufficient for [Cha81], [CF85], [Ive91], [PIK91], [FOO92], [Sak94], [CFSY96], [CGS97], ...

Approach I - Last Ballot

Overview

- voter may cast **many ballots**, and
- only the **last one is considered** for tallying.

How to Construct a Receipt?

- vote-buyer sees all channels at *all time*,
- voter is to prove last vote,
- money (and proof) only after the vote deadline.

But:

- Nice new assumption: “sometimes untappable channels”.

Approach II - Valuable Secret-Key

Overview

- voter **does not want to reveal his secret-key**,
- otherwise scheme would **not be receipt-free**.

Coercibility?

- trivially coercible (force voter to reveal secret key, and receive and verify receipt).

Vote-Buying?

- voter **proves in ZK** knowledge of a SK matching his PK, such that the above verification predicate is satisfied.

Remark: In credential systems: recipient wants to **use** the secret key.

Receipt-Freeness in the Standard Model

Assumptions

- standard model,
- tally must be exact.

How to Construct a Receipt

- commit to randomness: $r = \text{SHA}(\text{"hello world"})$,
- run protocol fully deterministically for vote v with randomness r .

Why is “hello world” a Receipt

- outgoing communication of voter is simulatable given v , r , any secrets, and all incoming communication.
- in- and outgoing communication of voter determines v .

Conclusions

Receipt-freeness is a subtle property.