Improving the *Farnel* Voting Scheme

Roberto Araújo
TU-Darmstadt

Peter Ryan
Newcastle University

Electronic Voting - 2008

Outline

- Introduction
- Review
  - The Original Farnel Scheme
  - The Farnel Variant
- Farnel box – Preliminaries
- A New Ballot Design
- A Single Box Farnel Scheme
- Conclusions

Introduction

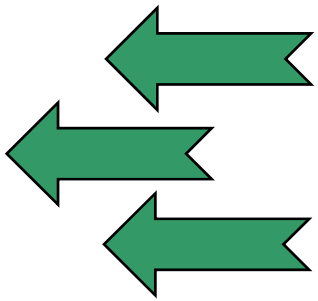
- Polling Station Elections
  - Voter-verifiability

- **Based on cryptography**
- Electronic OR Paper-based + Electronic (e.g. Pret-a-Voter)
- **Drawback**: cryptography not easily grasped by average voter

- **Without cryptography**
- Paper-based

  e.g. Randell-Ryan, Threeballot
- **Drawback**: ***less security assurances***

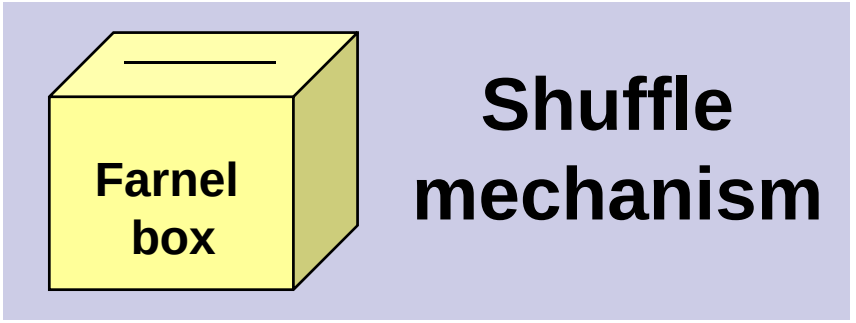
Improved with (minimal) cryptography



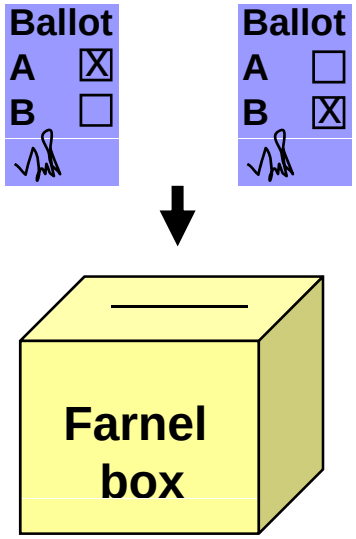
Farnel variant

The Original Farnel (Custódio - 2001)

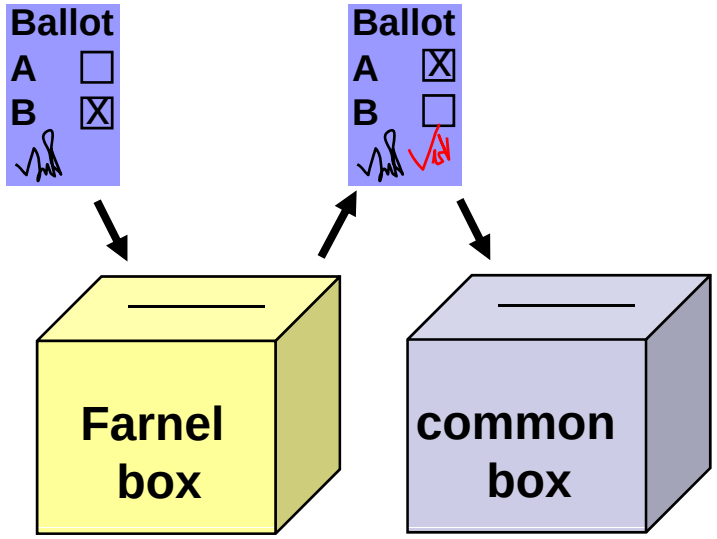
- Paper-based
- Two ballot boxes



Initialization (pre-voting)



Voting



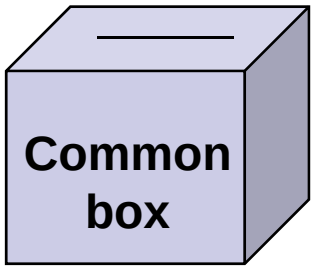
The original Farnel is **NOT** voter-verifiable

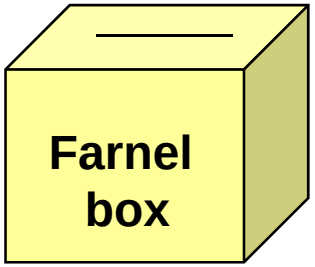
A Variant of Farnel (Araújo et al. - 2007)

- Paper-based
- Does not use cryptography
- Employs an improved Farnel ballot box
- **New kind of voter-verifiability**
  - Voters verify a subset of the votes cast into the ballot box.

A Variant of Farnel (Araújo et al. - 2007)

- The Ballot Boxes



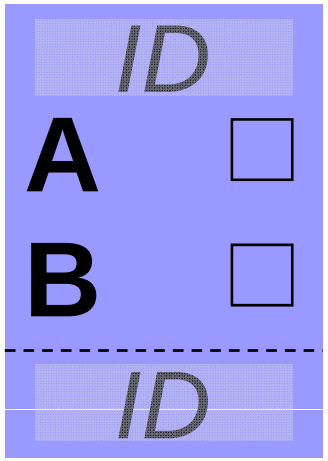


Shuffle and *copy* info

+

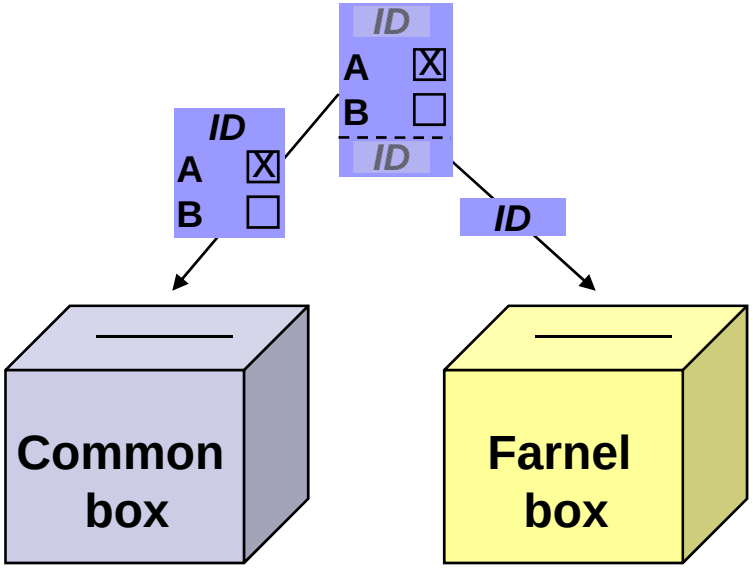
Remove scratch surfaces (optional)

- The Ballot Form

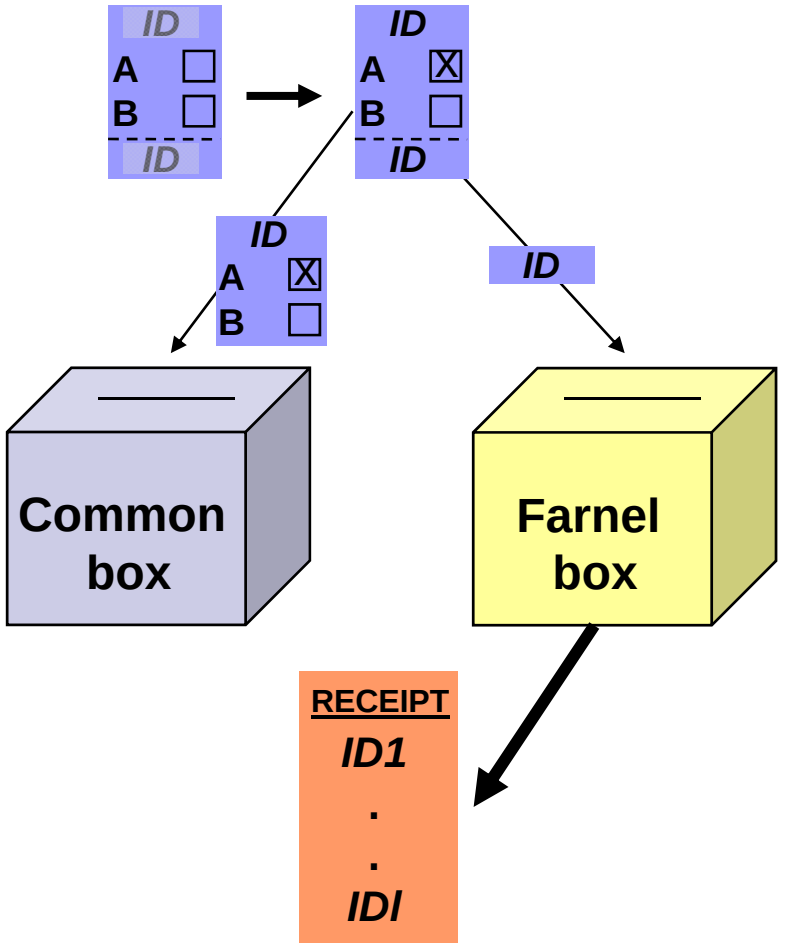


A Variant of Farnel (Araújo et al. - 2007)

- Initialization

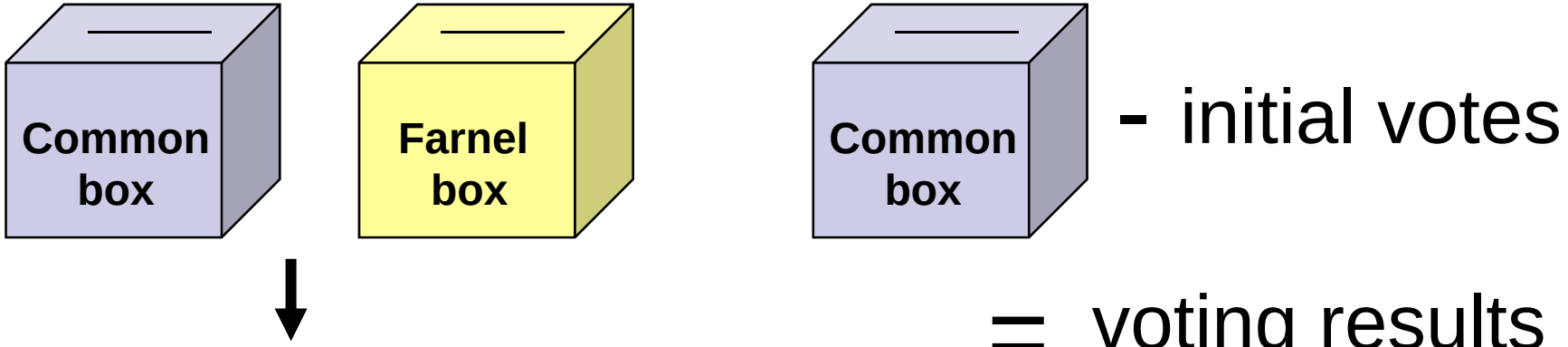


- Voting



A Variant of Farnel (Araújo et al. - 2007)

- Tally



Drawback: ☹
Honest authorities

Farnel Box - Preliminaries

- Initialization Process
  - Preserves the voter's anonymity
  - Votes or receipts (encrypted or not)
  - Initialization:

    Votes marked at random;

    A predetermined number of votes per option;

Encrypted Receipts → **votes for void**

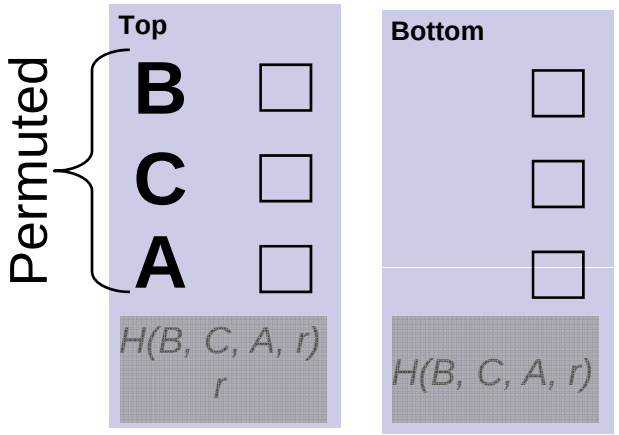
Totals carefully recorded

Farnel Box - Preliminaries

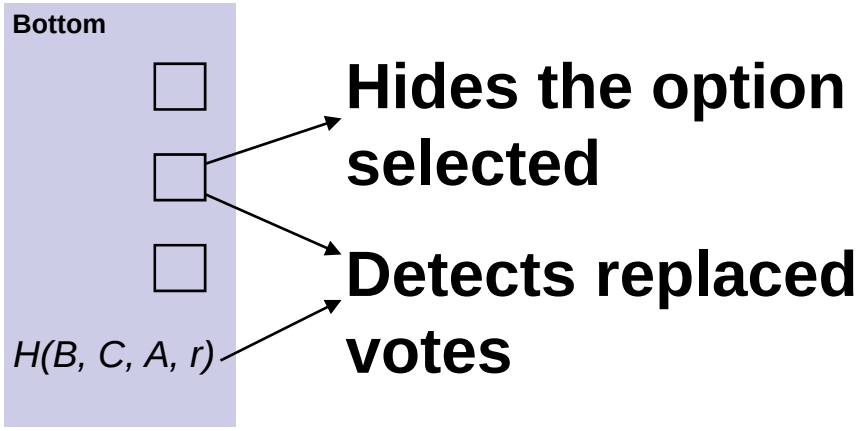
- Box Parameters
  - Number of initial elements (votes or receipts)
  - Number of receipts
  - Defined such that:
    - The voters' anonymity is preserved
    - Elements cannot be distinguished through the receipts
    - Receipts detect accuracy problems with acceptable probability

New Ballot Design – Farnel variant

- The receipt should:
  - **NOT** reveal the option selected before voting closes.
  - **DETECT** replacement of votes



- New Ballot form:
  - Pret-a-Voter style form
  - Top page = vote
  - Bottom page (without scratch) = receipt

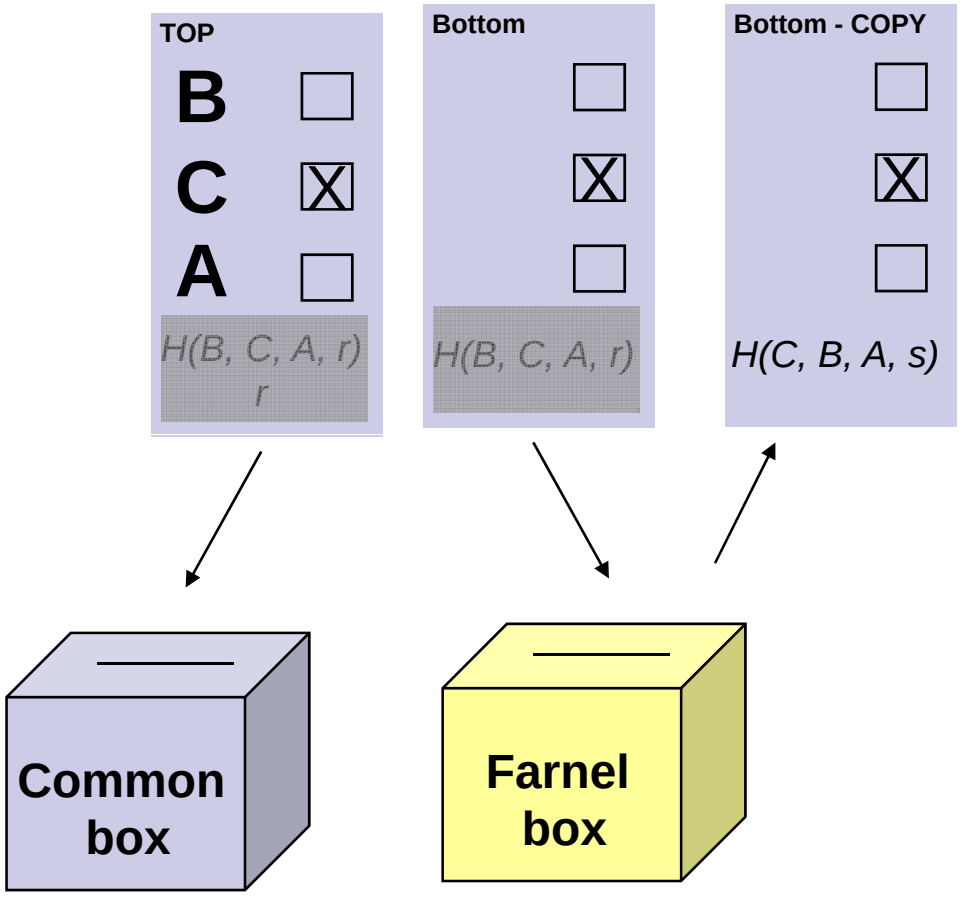


- Requisite: commitment scheme
  - Hash function

- Auditing Ballots

New Steps – Farnel variant

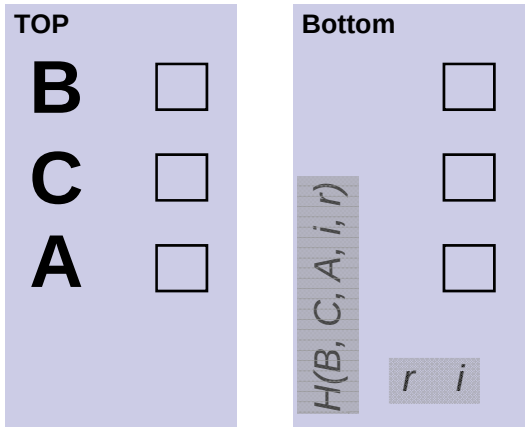
- Voting



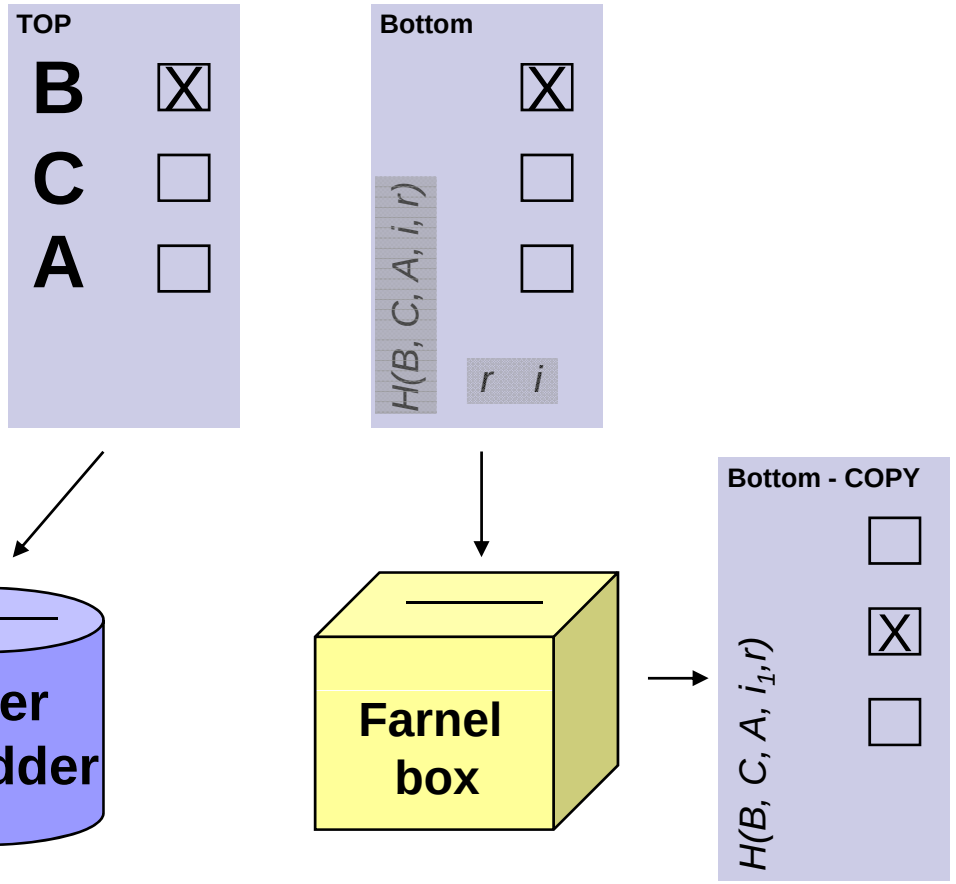
- Tallying Votes
- Verifying Votes

A Single Box Farnel Scheme

- Ballot form



- Voting



BBoard

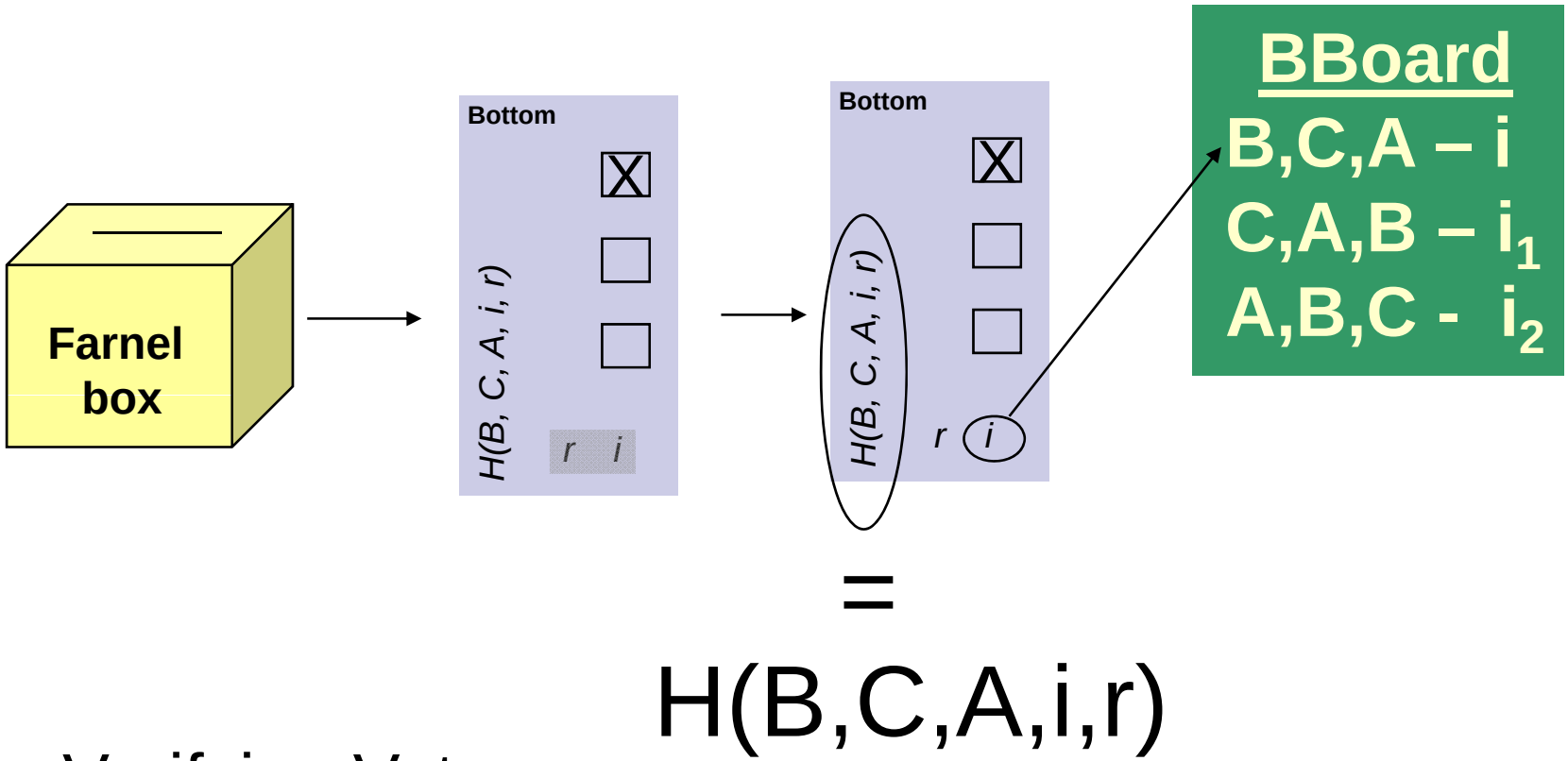
B,C,A – i

C,A,B – i_1

A,B,C - i_2

A Single Box Farnel Scheme

- Tallying



- Verifying Votes

Conclusions

- Farnel mechanism
  - Not only allows a new way of voter-verifiability, but …
  - May help counter certain psychological style attacks
  - Mitigates randomization attacks
- New ballot form for Farnel variant
  - Solves previous drawback
  - Requires only a commitment scheme
- Single Farnel Scheme – more simple ballot cast procedure
- Implementing the Farnel concept is challenging
- Future work – A more practical electronic version

Thank you