Using Prêt à Voter in Victorian State Elections

EVT August 2012

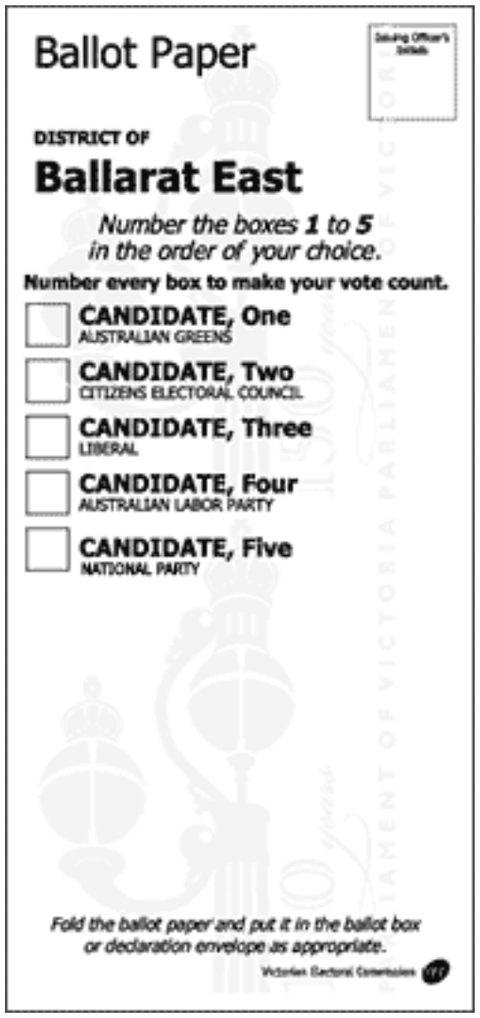
Craig Burton[1] Chris Culnane[2] James Heather[2]
Thea Peacock[3] Peter Y. A. Ryan[3] Steve Schneider[2]
Sriram Srinivasan[2] Vanessa Teague[4] Roland Wen[5] Zhe Xia[2]

Structure of talk

- Voting in the State of Victoria, Australia
- VEC's motivation for e-voting
- Introducing the Prêt a Voter voter-verifiable system
- Adapting to the VEC requirements: practical challenges
- Conclusion

Legislative Assembly (Lower House)

- Full preferential voting: number the candidates in order of preference.


Ballot Paper

Issuing Officer's Initials

DISTRICT OF

Ballarat East

*Number the boxes **1** to **5** in the order of your choice.*

Number every box to make your vote count.

CANDIDATE, One
AUSTRALIAN GREENS

CANDIDATE, Two
CITIZENS ELECTORAL COUNCIL

CANDIDATE, Three
LIBERAL

CANDIDATE, Four
AUSTRALIAN LABOR PARTY

CANDIDATE, Five
NATIONAL PARTY

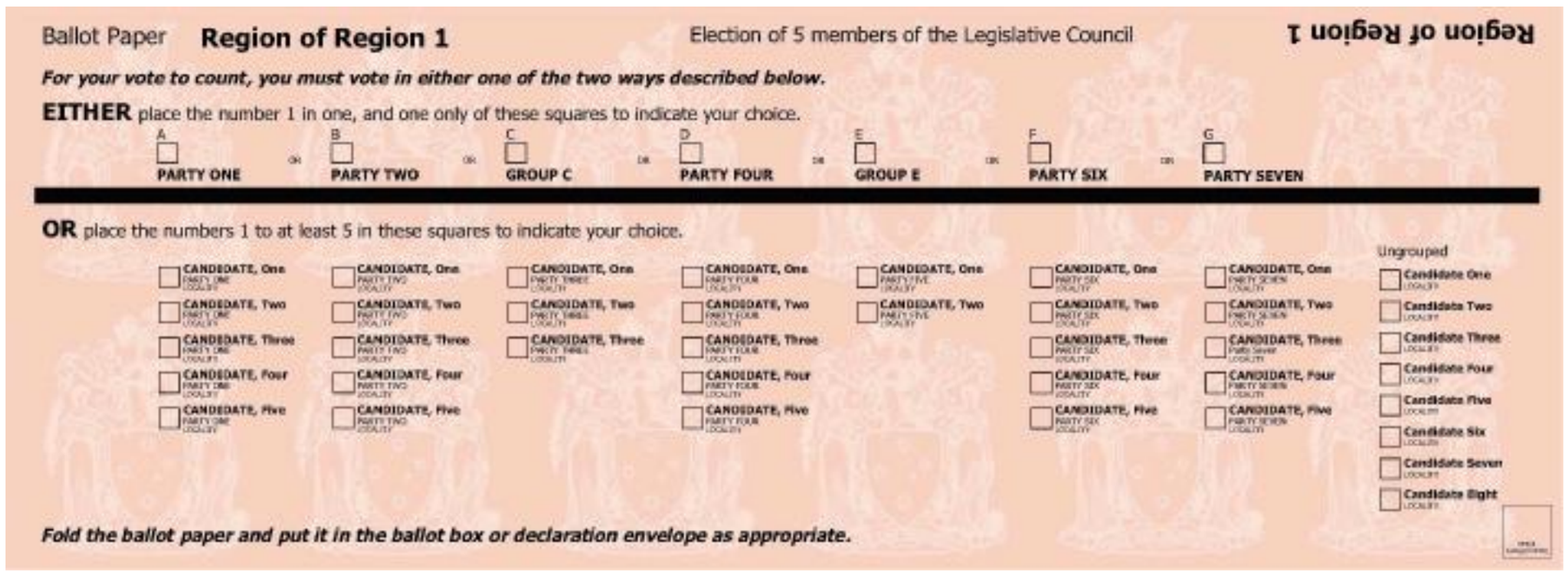
Fold the ballot paper and put it in the ballot box or declaration envelope as appropriate.

Victorian Electoral Commission

http://www.vec.vic.gov.au/vote/vote-howto-state.html

Legislative Council (Upper House)

- ATL: select exactly one choice; **or**
- BTL: number the candidates in order of preference


Ballot Paper **Region of Region 1** Election of 5 members of the Legislative Council Region of Region 1

For your vote to count, you must vote in either one of the two ways described below.

EITHER place the number 1 in one, and one only of these squares to indicate your choice.

A PARTY ONE OR B PARTY TWO OR C GROUP C OR D PARTY FOUR OR E GROUP E OR F PARTY SIX OR G PARTY SEVEN

OR place the numbers 1 to at least 5 in these squares to indicate your choice.

CANDIDATE, One / CANDIDATE, Two / CANDIDATE, Three / CANDIDATE, Four / CANDIDATE, Five

Ungrouped: Candidate One, Candidate Two, Candidate Three, Candidate Four, Candidate Five, Candidate Six, Candidate Seven, Candidate Eight

Fold the ballot paper and put it in the ballot box or declaration envelope as appropriate.

http://www.vec.vic.gov.au/vote/vote-howto-state.html

VEC's motivation for electronic voting

- VEC was an early adopter of e-voting (2006)
- **flexibility:** for remote (but supervised) voting including overseas, out of state, out of district
- **accessibility:** supports voters with disabilities. Electronic voting machines also handle foreign languages. Complexity of ballots means need for help to avoid malformed ballots – but human help loses privacy
- **usability:** to reduce (accidental) informal ballots
- **BUT:** proprietary system not open to inspection; lack of verifiability; issues with integration with VEC processes
- **WANT** e-voting but recognise the need for verifiability

Context of this project

- **Australian elections**: solution needs to be able to handle STV and preferential voting. Prêt à Voter judged to be the most appropriate voter-verifiable system able to support this.

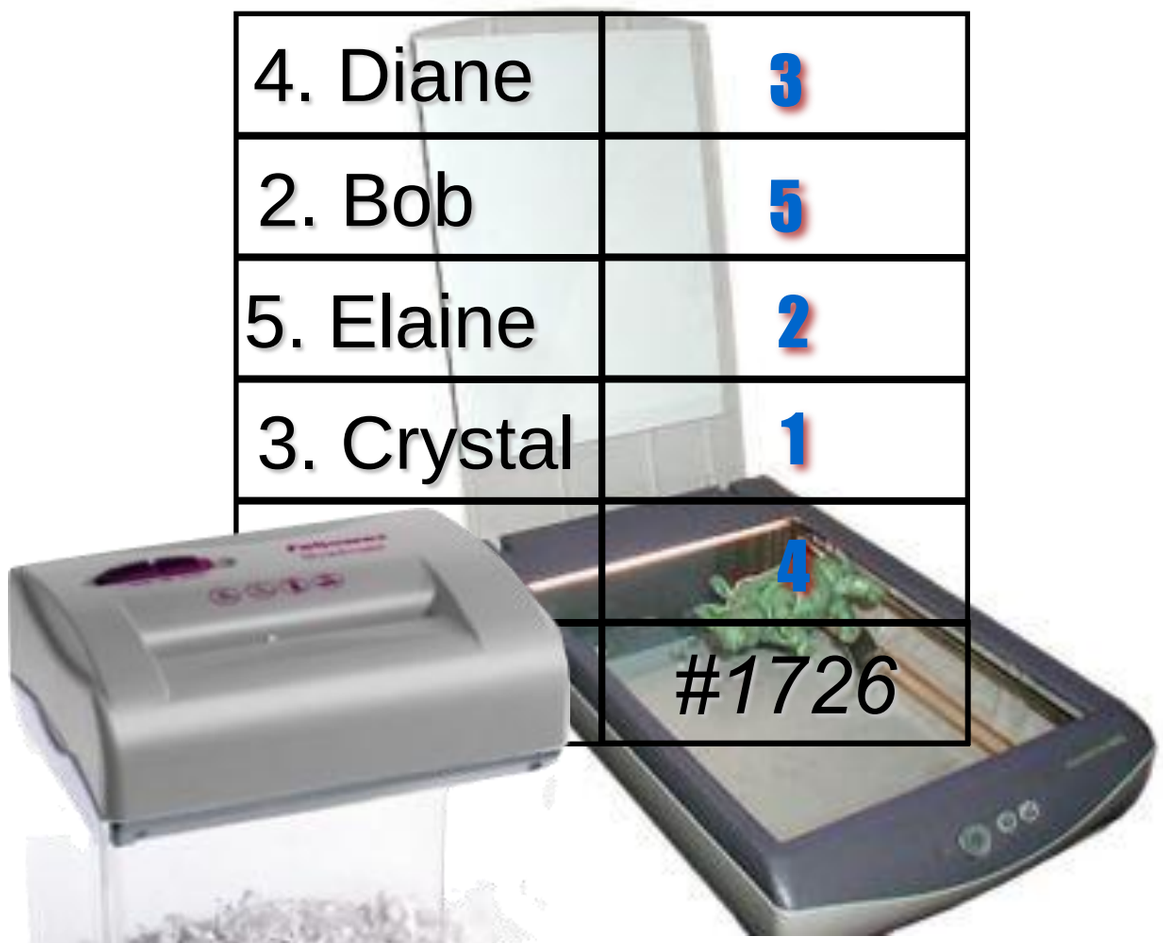
- **usability vs security:** what can you ask and expect voters to do?
- **scalability:** issues to be resolved for us to scale up to a state election.
- **pragmatics:** scanning (including OCR) and printing.
- **integrity and trust:** the electorate must have confidence in the solution.

Prêt à Voter

- A voter-verifiable voting system
- Verifiability: voters, independent checkers can verify stages of the election
- Integrity: evidence provided that the result is correct
- Privacy: have to trust some elements of the system, but aim to minimize this

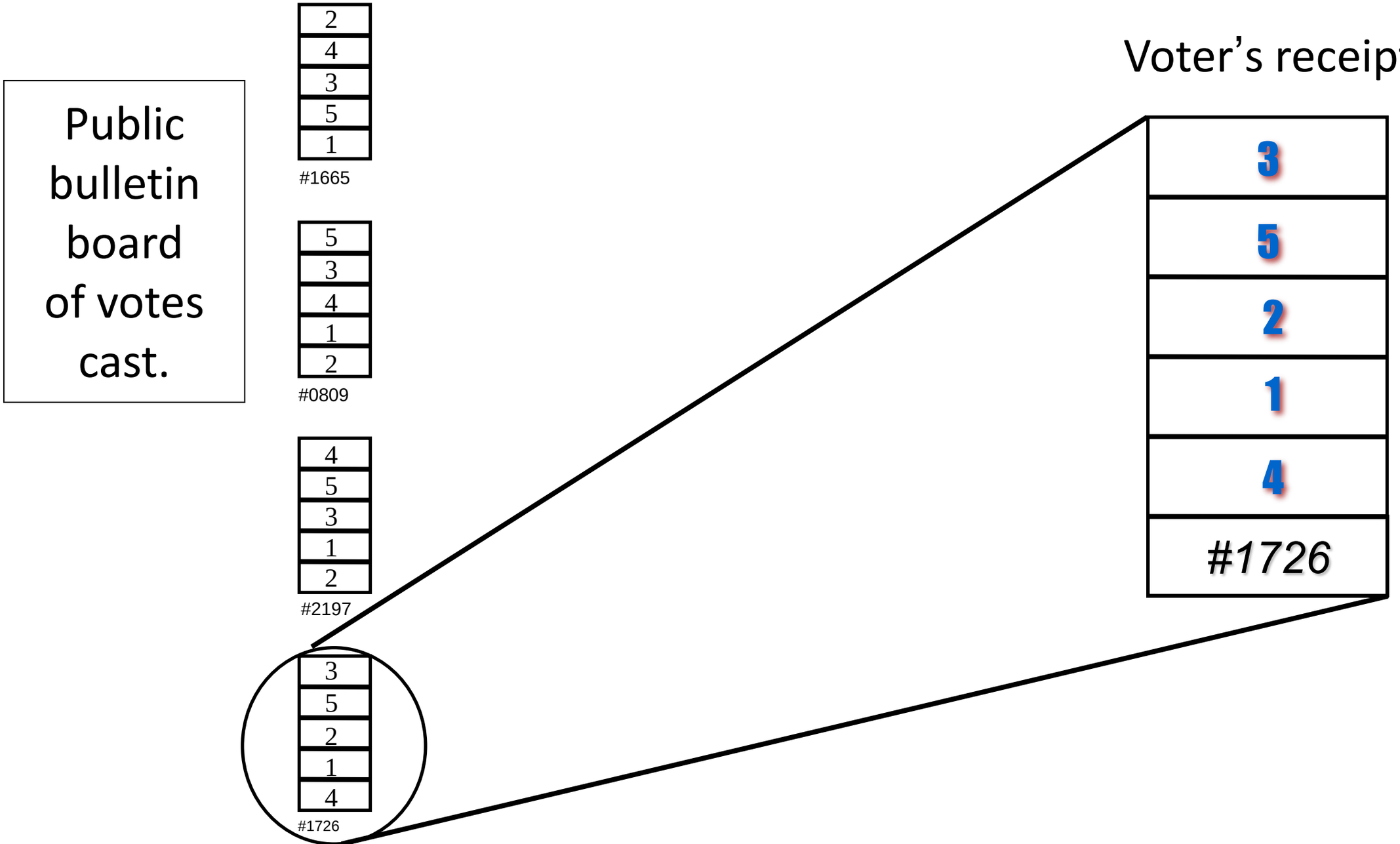
Voting with Prêt à Voter

- Place X or preferences against desired candidate. (*candidates in random order*)
- Separate left hand side.
- Destroy left hand side.
- Cast (scan) vote.
- Take receipt home.



Publish the ballots cast

- Voter receipts prevent election officials from altering or removing votes.
- Voters confirm inclusion of their vote



Tallying the votes

Public bulletin board of votes cast.

2
4
3
5
1

#1665

5
3
4
1
2

#0809

4
5
3
1
2

#2197

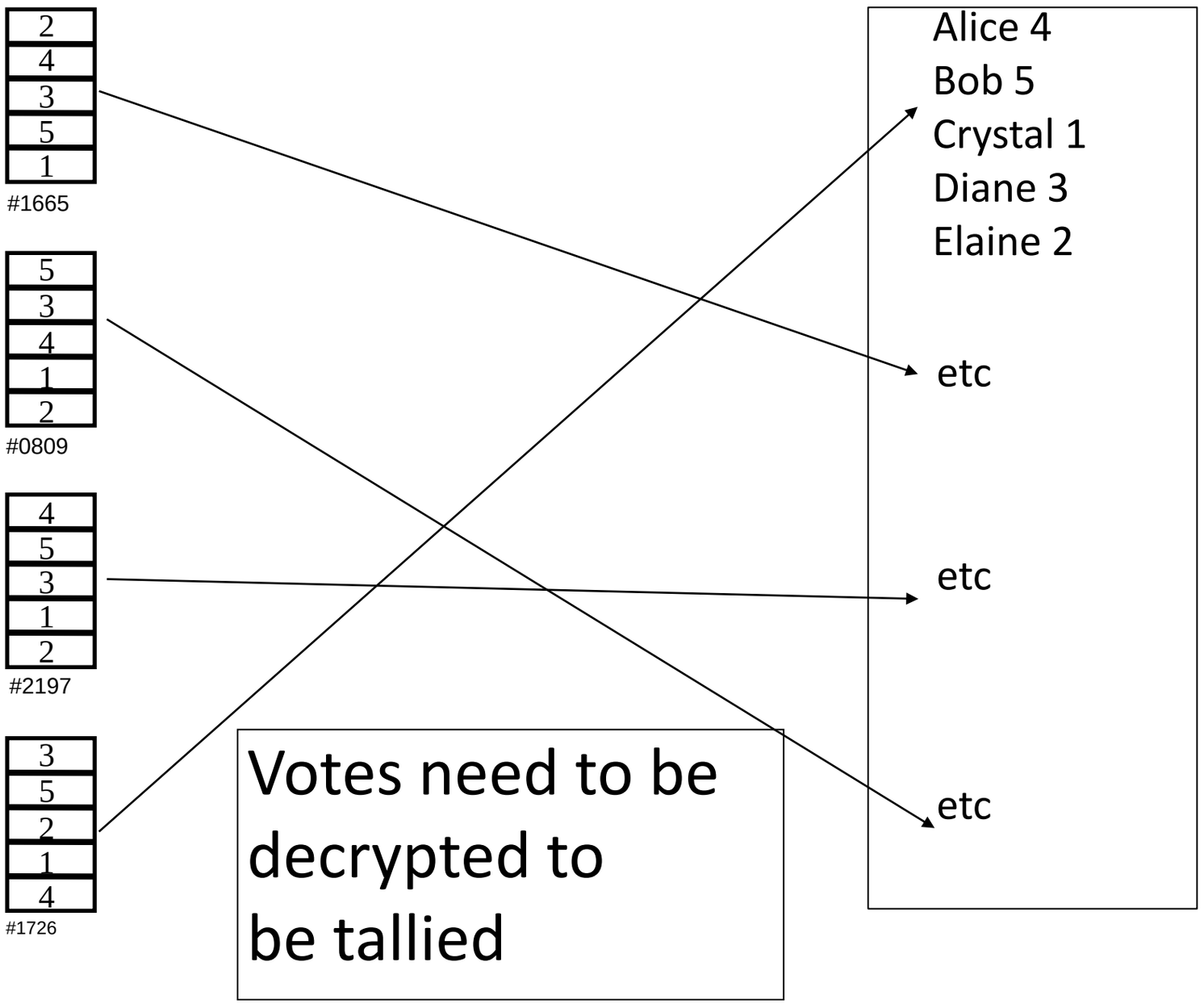
3
5
2
1
4

#1726

Tallying the votes

Public bulletin board of votes cast.

Public list of votes, shuffled and decrypted.



Votes need to be decrypted to be tallied

Tallying the votes

Public bulletin board of votes cast.

2
4
3
5
1

#1665

5
3
4
1
2

#0809

4
5
3
1
2

#2197

3
5
2
1
4

#1726

Public list of votes, shuffled and decrypted.

Alice 4
Bob 5
Crystal 1
Diane 3
Elaine 2

etc

etc

etc

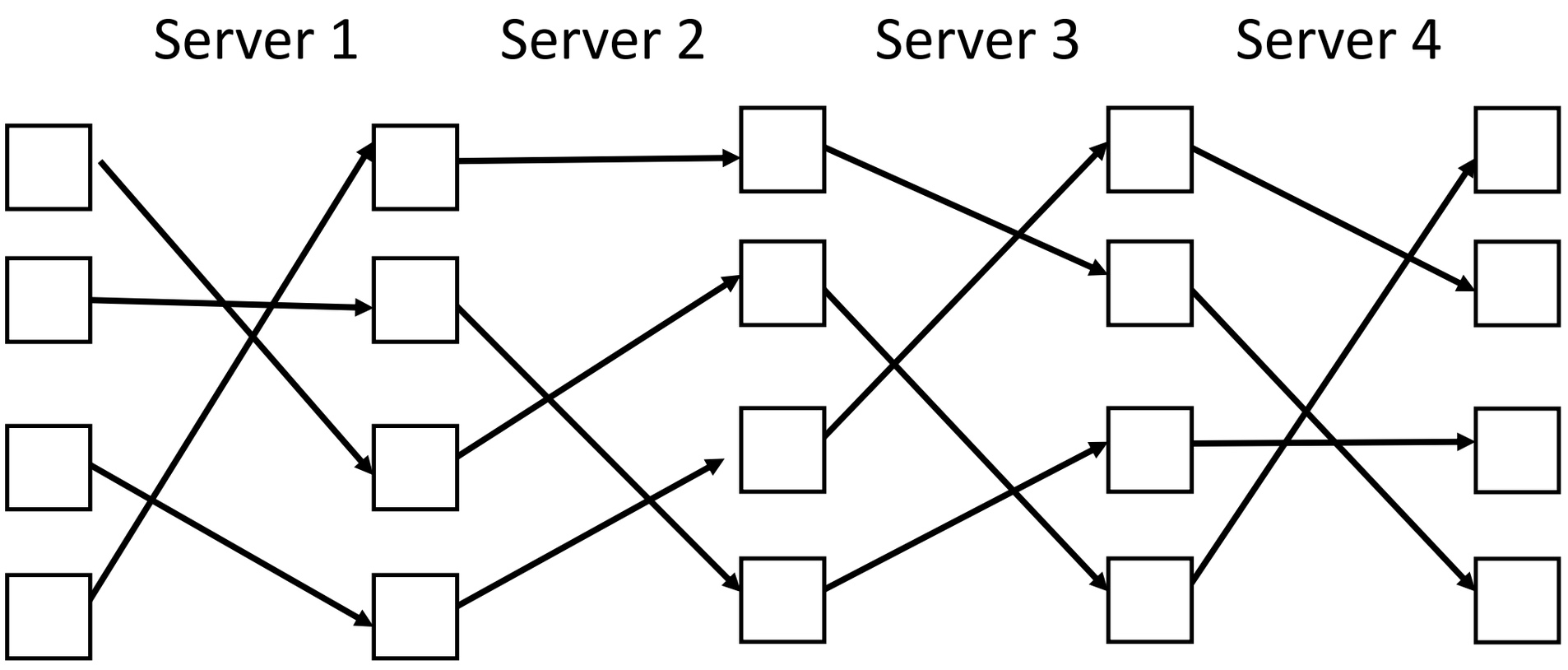
The links are not published (receipts are not linked to votes)

Tallying

When the votes are cast:

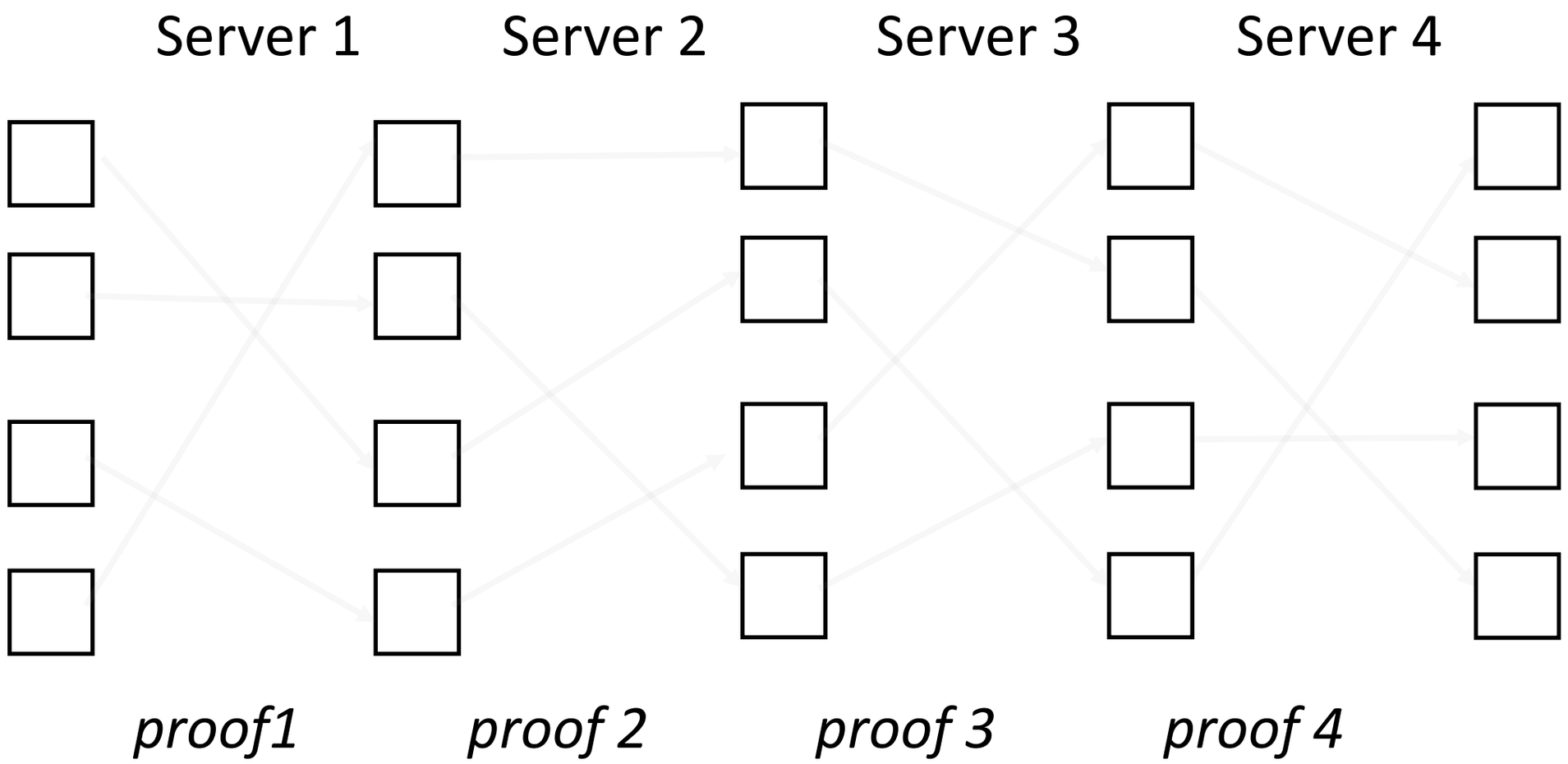
- Publish the votes cast (newspaper, or web bulletin board)
  – these should match the receipts, and voters can check.
- Mix up the votes (see next slide), so resulting votes are not linked to input votes (which correspond to receipts):
- Decrypt the mixed votes
- Publish the resulting votes.
- Count the votes.

Re-encryption mixnets with proofs (Chaum; Park et al.; Sako and Kilian)



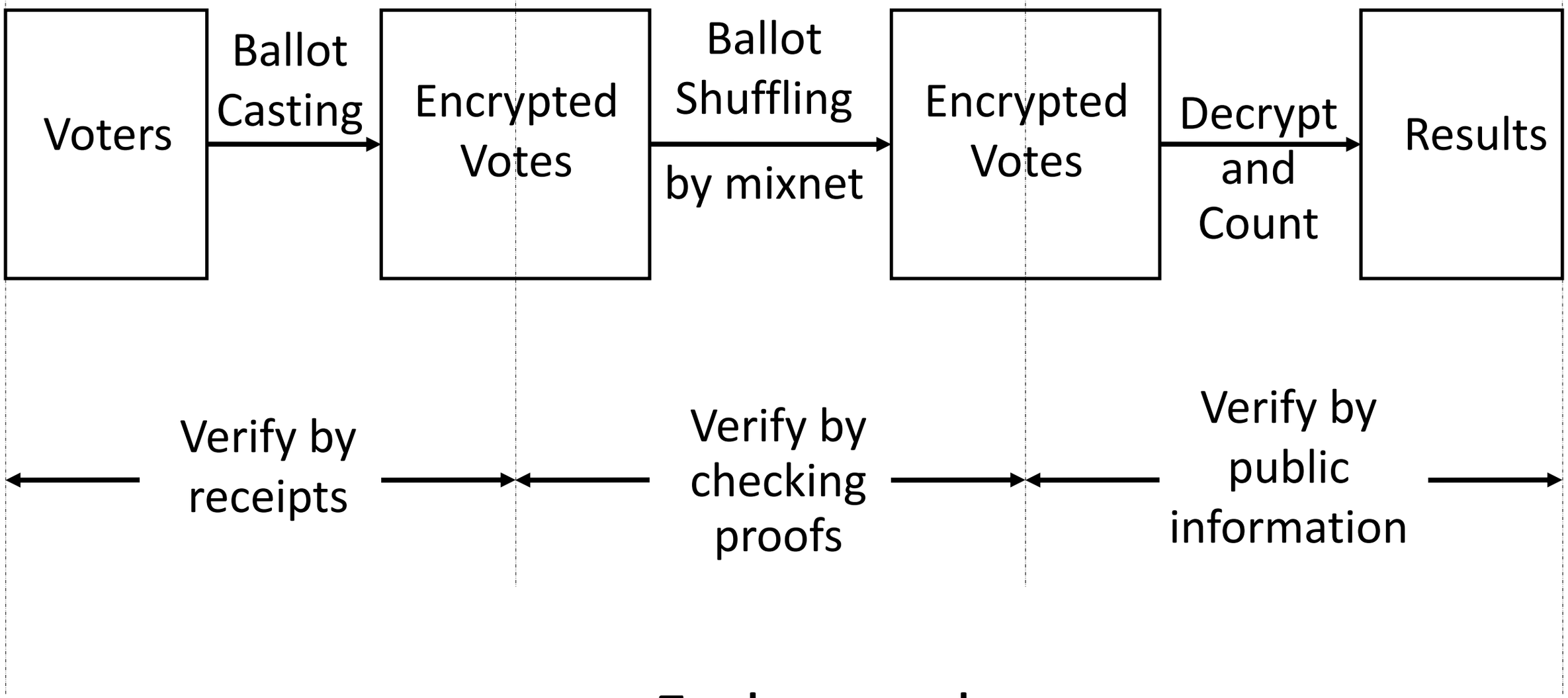
- Re-encryption mixing: $\{c,r_1\} \rightarrow \{c,r_2\}$ are different encryptions of c

Re-encryption mixnets with proofs (Chaum; Park et al.; Sako and Kilian)



- Tellers provide `proofs of shuffles': that the set of encrypted values is not changed from one stage to the next.
- These proofs can be independently checked.

End-to-end Verifiability for Prêt à Voter



Practical Challenges

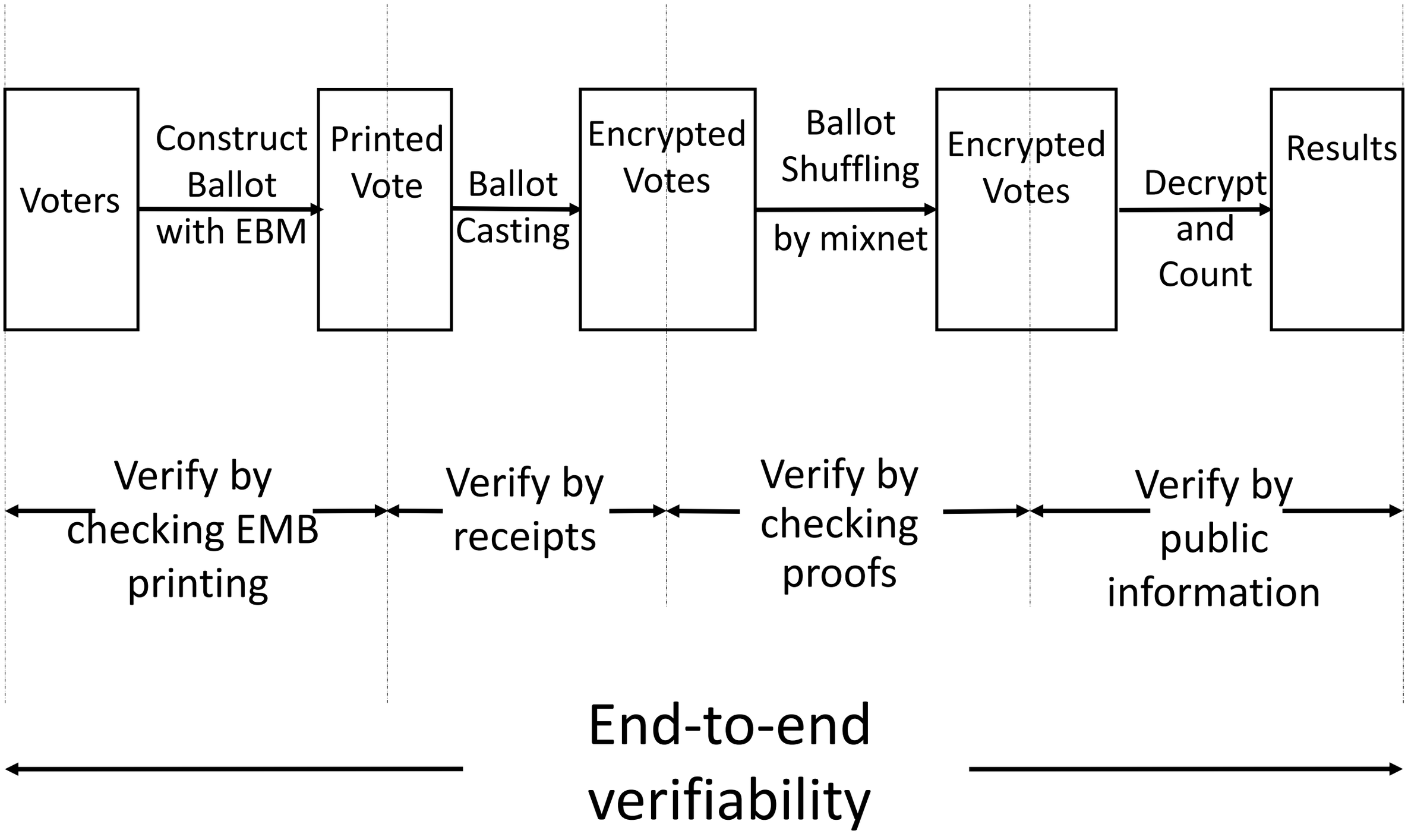
Practical challenges

- In practice in Victorian State elections there are typically around 35+ BTL candidates
- Prêt à Voter requires those candidates to be in a random order on each ballot
- Significant cryptography required to create the ballot forms
- Presenting 35+ spaces for voters to write preferences in a single column will require a long ballot form.
- Difficult for voters to find their choices by hand; issues around the order candidates are presented to voters
- Accessibility issues are compounded

Adapting Prêt à Voter: Front end

- **Solution**: Use an offline Electronic Ballot Marker to assist the voter to complete the ballot.
- It will capture the voter's preferences in a user-friendly way, and will print the preferences on the ballot form.
- Presents the candidates in the given fixed order
- Captures the voters preferences via touch screen
- Prints the preferences onto the ballot form in the appropriate permutation
- Voter confirms selection before scanning.
- Alerts voter if ballot not well formed
- Can have accessibility plug-ins (vision/mobility impaired) and offer different languages.
- **NB:** does lose the attractive feature of Prêt à Voter that no device learns the vote. Seems unavoidable.

End-to-end Verifiability for Prêt à Voter with EBM



VEC Ballot Form

Ballot form gives the permutation

Ballot Form – front side

Serial number: 1

No. 1	**Legislative Assembly**
( )	Donna
( )	Alice
( )	Charlie
( )	Bob
	Legislative Council **Above the Line (ATL)**
[ ]	Lib Dem
[ ]	Labour
[ ]	Green
	

Onion QR code

Candidate QR code

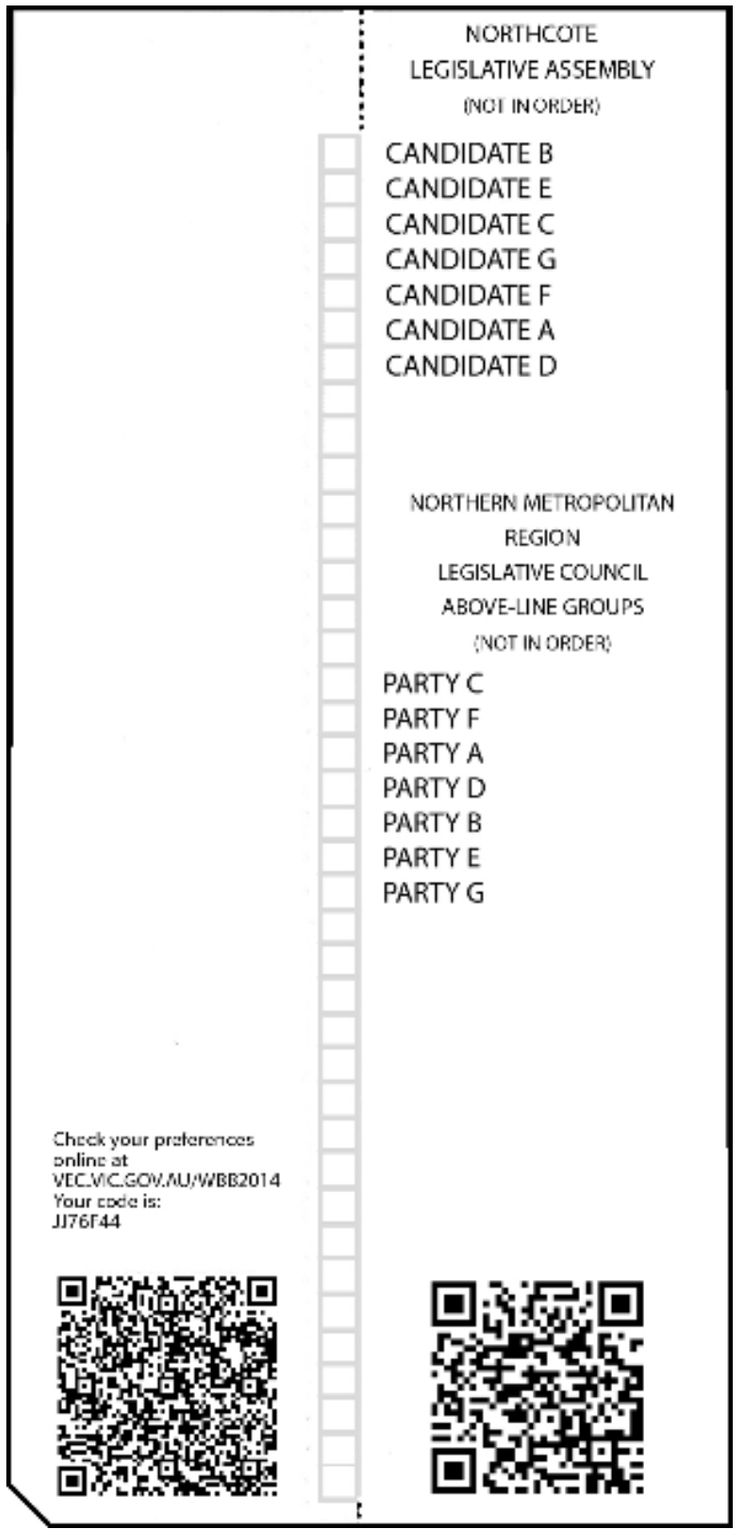
Serial No. 1
(Donna, Alice, Charlie, Bob),
(Lib Dem, Labour, Green),
(Steve, Vanessa, Craig, Peter
Chris, Thea, James)

Ballot form gives the permutation

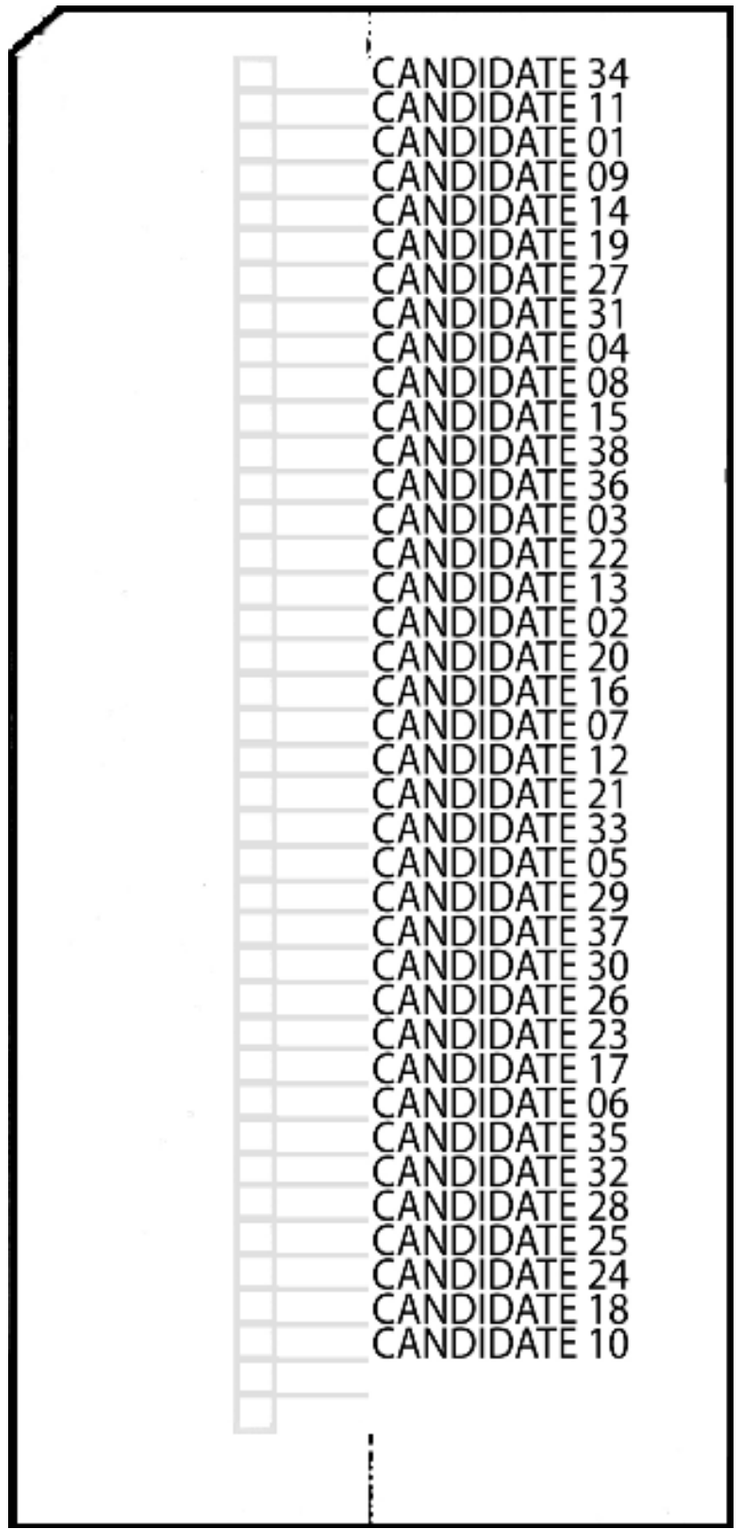
Ballot Form – Back side Serial number: 1

No. 1	**Legislative Council** **Below the Line (BTL)**
( )	Steve
( )	Vanessa
( )	Craig
( )	Peter
( )	Chris
( )	Thea
( )	James

A VEC ballot example



The front side



The back side

Victorian Voter Experience

1. Language selection and training

2. Scan candidate QR code (device obtains permutation)

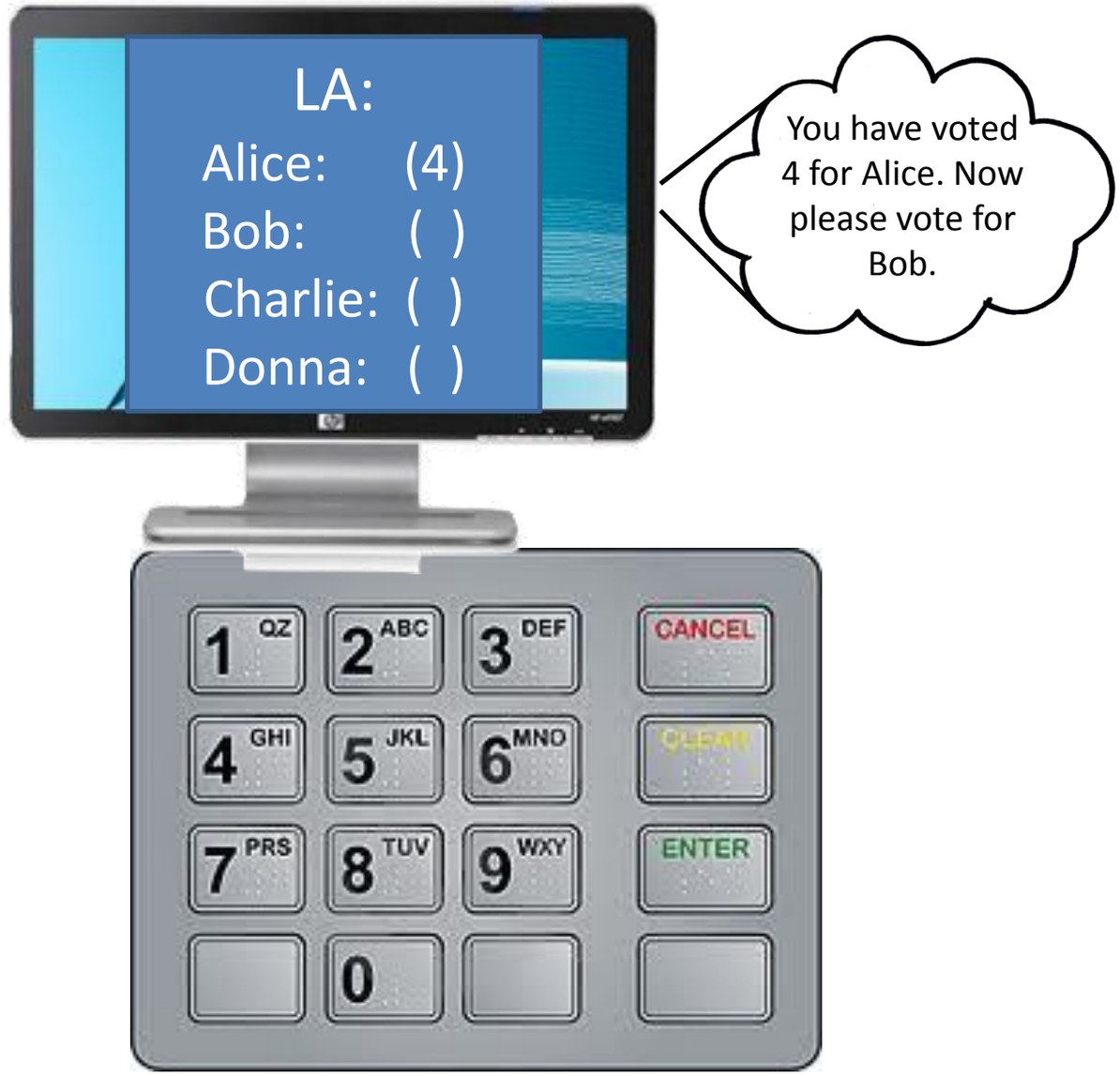
Candidate
QR code

3a. Construct vote via voting device (LA + LC-ATL)

3b. Construct vote via voting device (LA + LC-BTL)

3c. Vote casting for blind voters

No. 1	**Legislative Assembly**
( )	Donna
( )	Alice
( )	Charlie
( )	Bob
	Legislative Council **Above the Line (ATL)**
[ ]	Lib Dem
[ ]	Labour
[ ]	Green



Clipped corner

4a. Overprint on ballot form (LA + LC-ATL)

Ballot form

Serial number: 1

No. 1	**Legislative Assembly**
(2)	Donna
(4)	Alice
(3)	Charlie
(1)	Bob
	Legislative Council Above the Line (ATL)
[ ]	Lib Dem
[X]	Labour
[ ]	Green

Front Side

No. 1	**Legislative Council Below the Line (BTL)**
( )	Steve
( )	Vanessa
( )	Craig
( )	Peter
( )	Chris
( )	Thea
( )	James

Back Side (empty)

4b. Overprint on ballot form (LA + LC-BTL)

Ballot form

Serial number: 1

No. 1	**Legislative Assembly**
(2)	Donna
(4)	Alice
(3)	Charlie
(1)	Bob
	Legislative Council Above the Line (ATL)
[ ]	Lib Dem
[ ]	Labour
[ ]	Green

Front Side (ATL empty)

No. 1	**Legislative Council Below the Line (BTL)**
(3)	Steve
(5)	Vanessa
(1)	Craig
(2)	Peter
(6)	Chris
(4)	Thea
(7)	James

Back Side

5. Shred the names

Legislative Assembly
Alice
Bob
Charlie
Donna
Legislative Council Above the Line (ATL)
Lib Dem
Labour
Green

Front side: LA + LC-ATL candidates
Back side: LC-BTL candidates

6a. Submit vote (LA + LC-ATL)

No. 1
(2)
(4)
(3)
(1)
[ ]
[X]
[ ]

Front

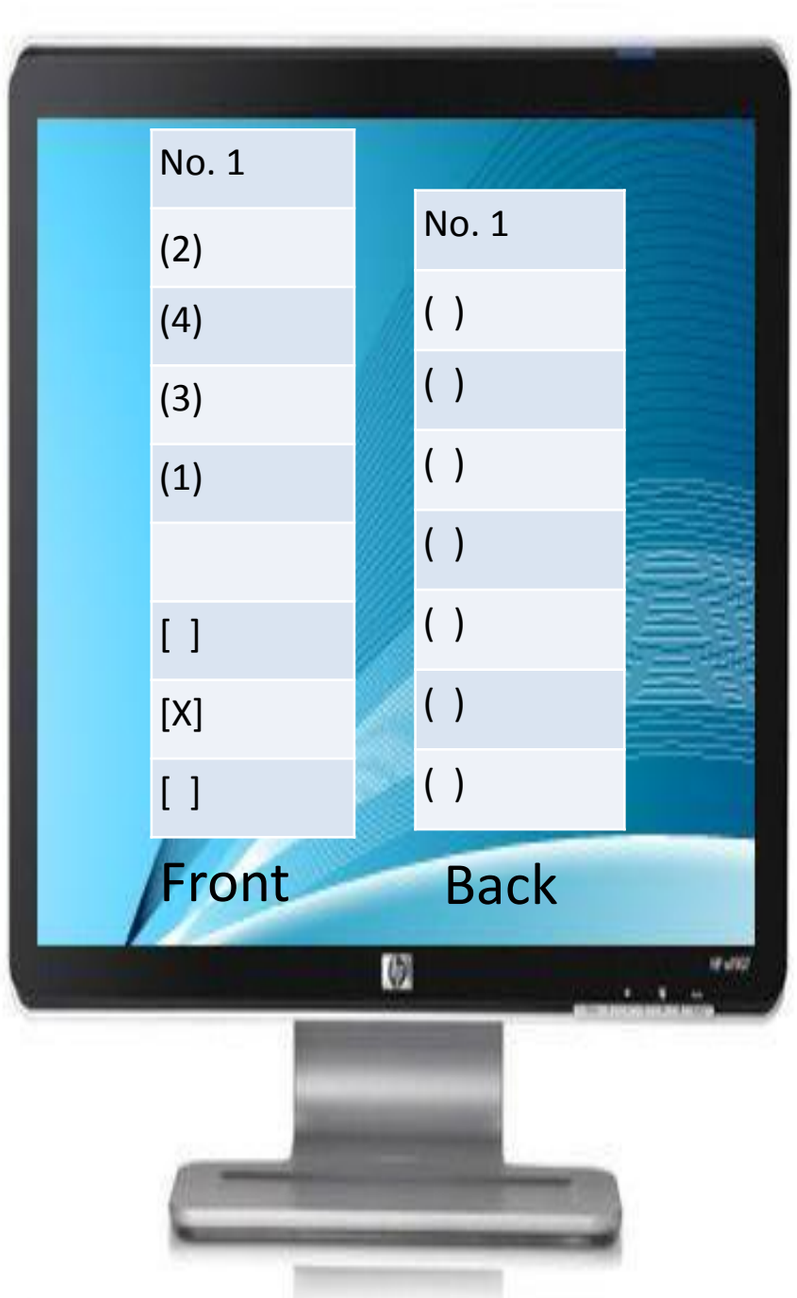
No. 1
( )
( )
( )
( )
( )
( )

Back

① Scan

② Display to the voter

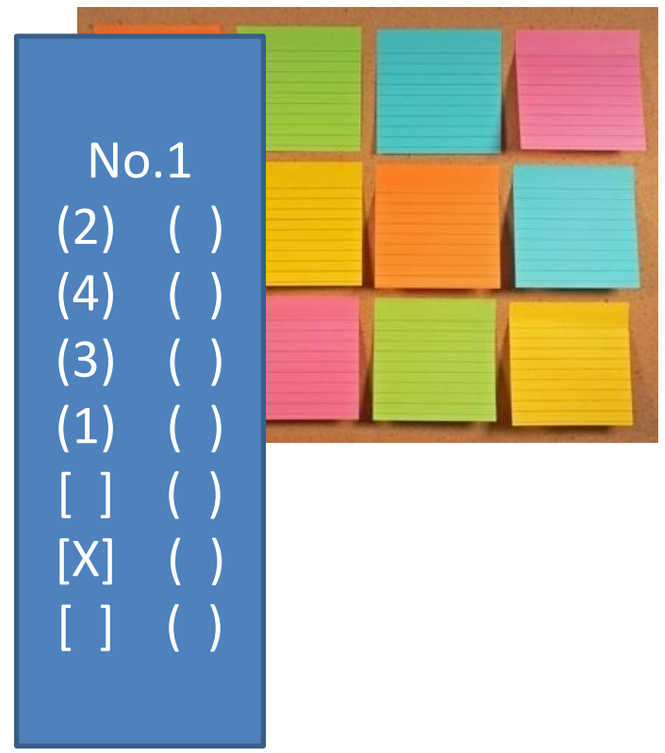
satisfy/modify



③ No.1: {2,4,3,1}, [2], {}

Submit to WBB

Bulletin Board



6b. Submit vote (LA + LC-BTL)

No. 1
(2)
(4)
(3)
(1)
[ ]
[ ]

Front

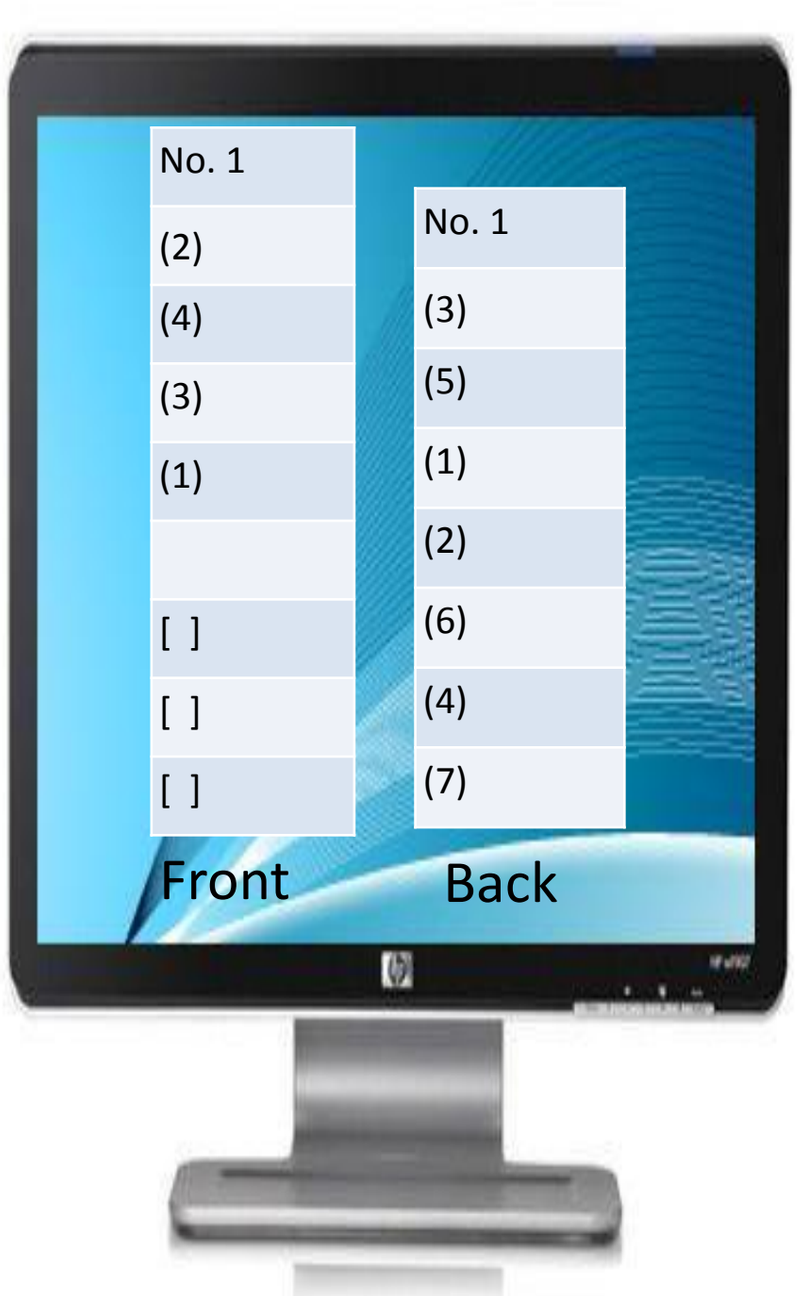
No. 1
(3)
(5)
(1)
(2)
(6)
(4)
(7)

Back

① Scan

② Display to the voter

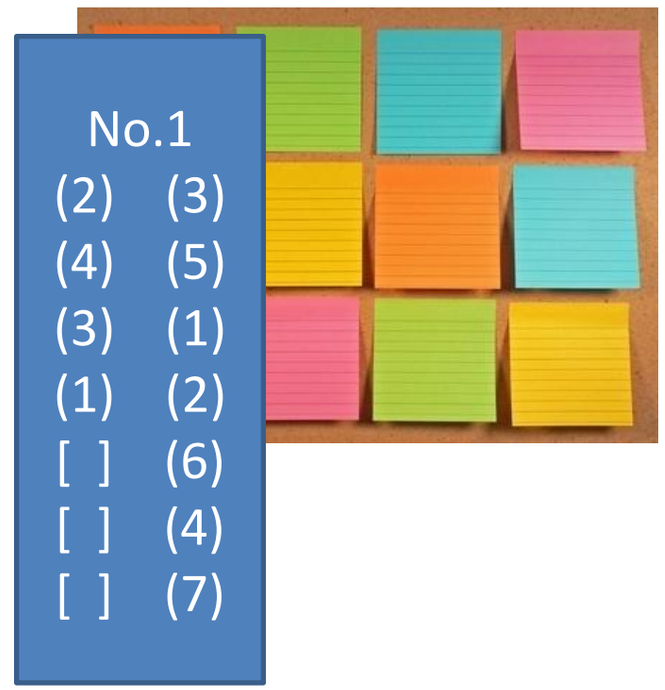
satisfy/modify



③ No.1: {2,4,3,1}, [], {3,5,1,2,6,4,7}

Submit to WBB

Bulletin Board



No. 1
(2)
(4)
(3)
(1)
[ ]
[X]
[ ]

No. 1
( )
( )
( )
( )
( )
( )

② over print

Overprinted Signature

① {No.1: {2,4,3,1}, [2], {}}_SK(WBB)

Bulletin Board

No.1	
(2)	( )
(4)	( )
(3)	( )
(1)	( )
[ ]	( )
[X]	( )
[ ]	( )

No. 1
(2)
(4)
(3)
(1)
[ ]
[ ]
[ ]

No. 1
(3)
(5)
(1)
(2)
(6)
(4)
(7)

② over print

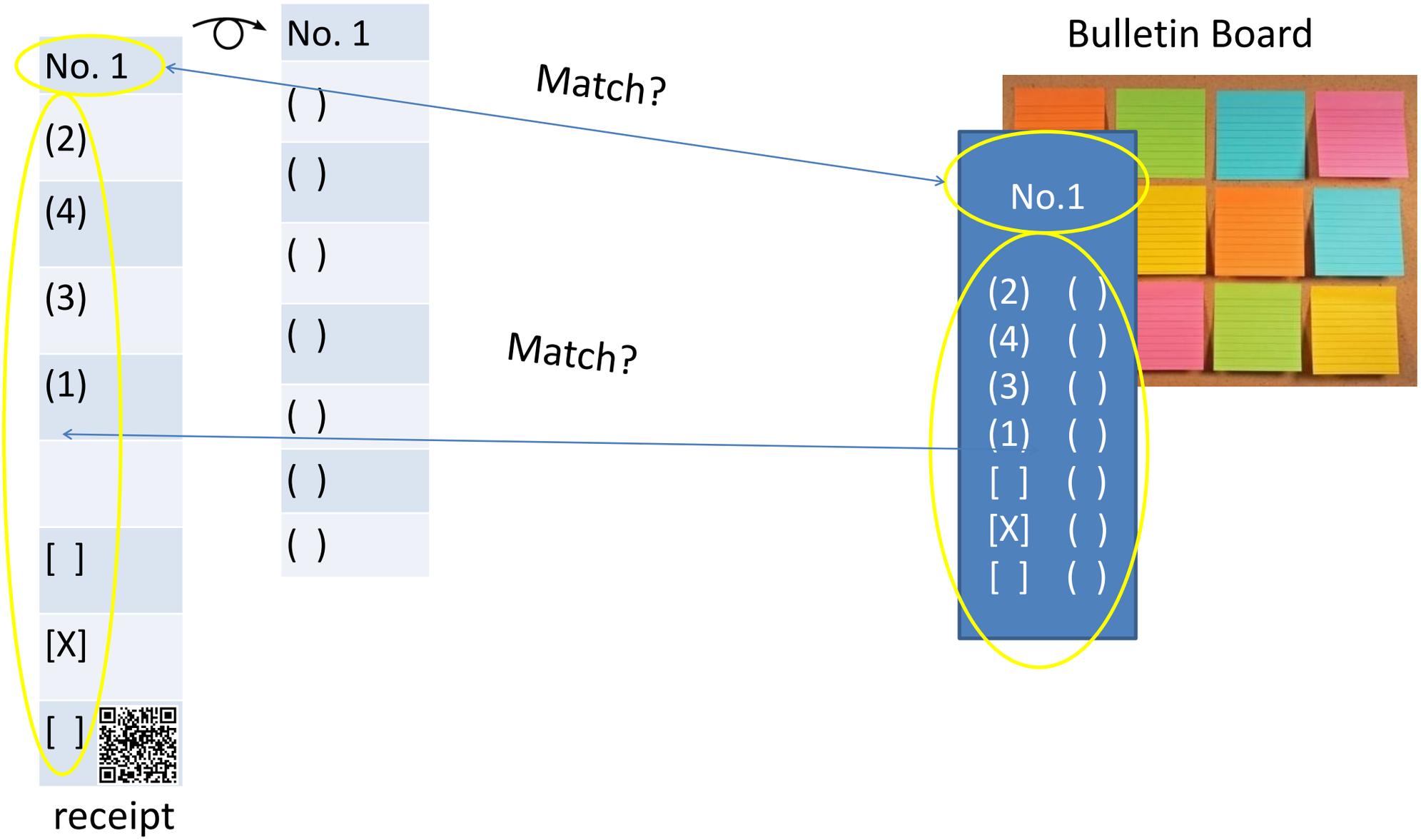
Overprinted Signature

① {No.1: {2,4,3,1}, [], {3,5,1,2,6,4,7}}_SK(WBB)

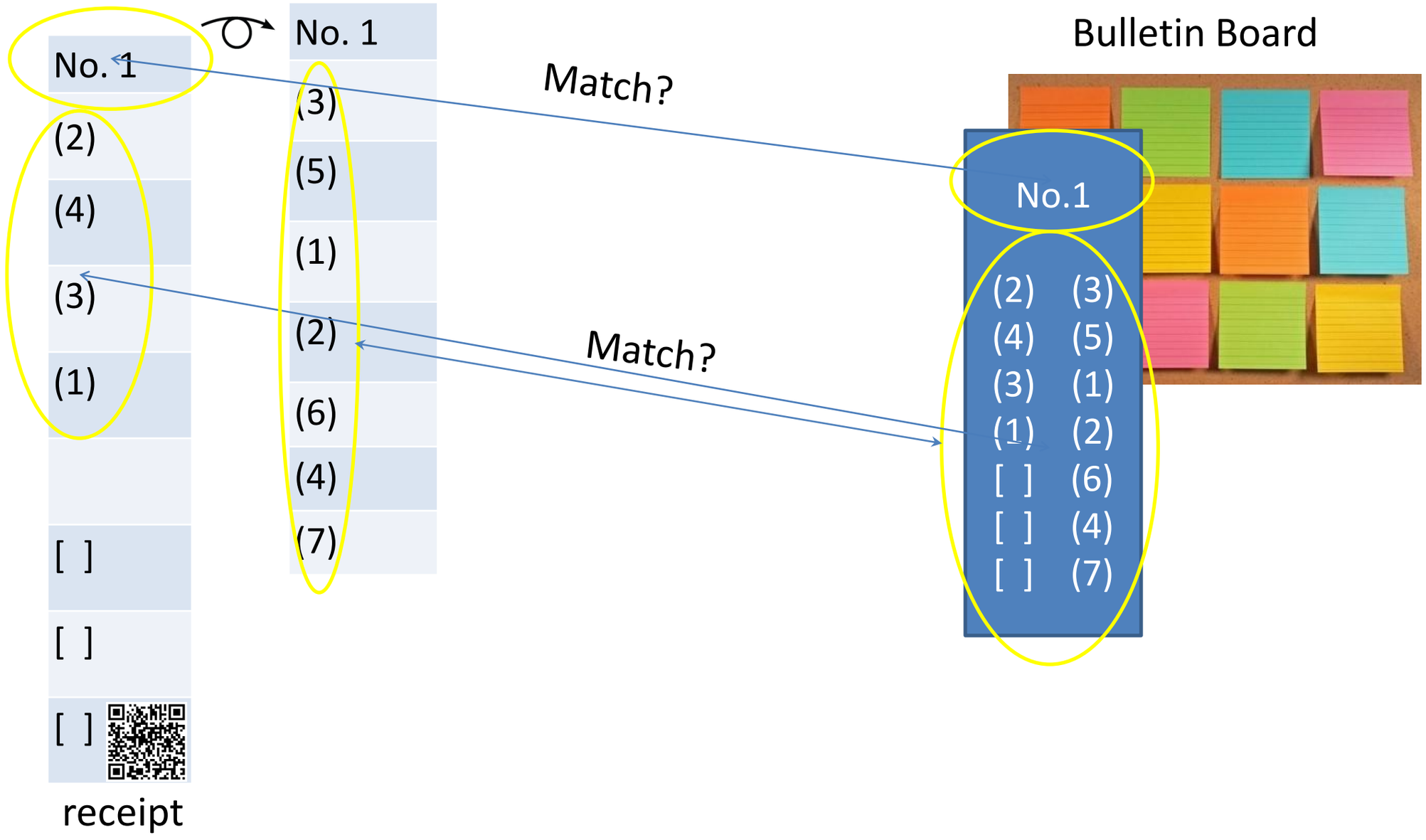
Bulletin Board

No.1	
(2)	(3)
(4)	(5)
(3)	(1)
(1)	(2)
[ ]	(6)
[ ]	(4)
[ ]	(7)

8a. WBB check later (LA + LC-ATL)



8b. WBB check later (LA + LC-BTL)



Adapting Prêt à Voter: Processing the votes

- We use Douglas Wikström's implementation of a re-encryption mixnet: the **Verificatum** system.
  - This provides shuffles, re-encryptions and proofs.
    - It also provides the final decryption step following the mix, to produce a list of plaintext votes.
- Given the large numbers of candidates, each preference list is compressed into a small number of ciphertexts to optimise the mixing process, and expanded at the other end. These steps are also verifiable. [Technical details in the paper]

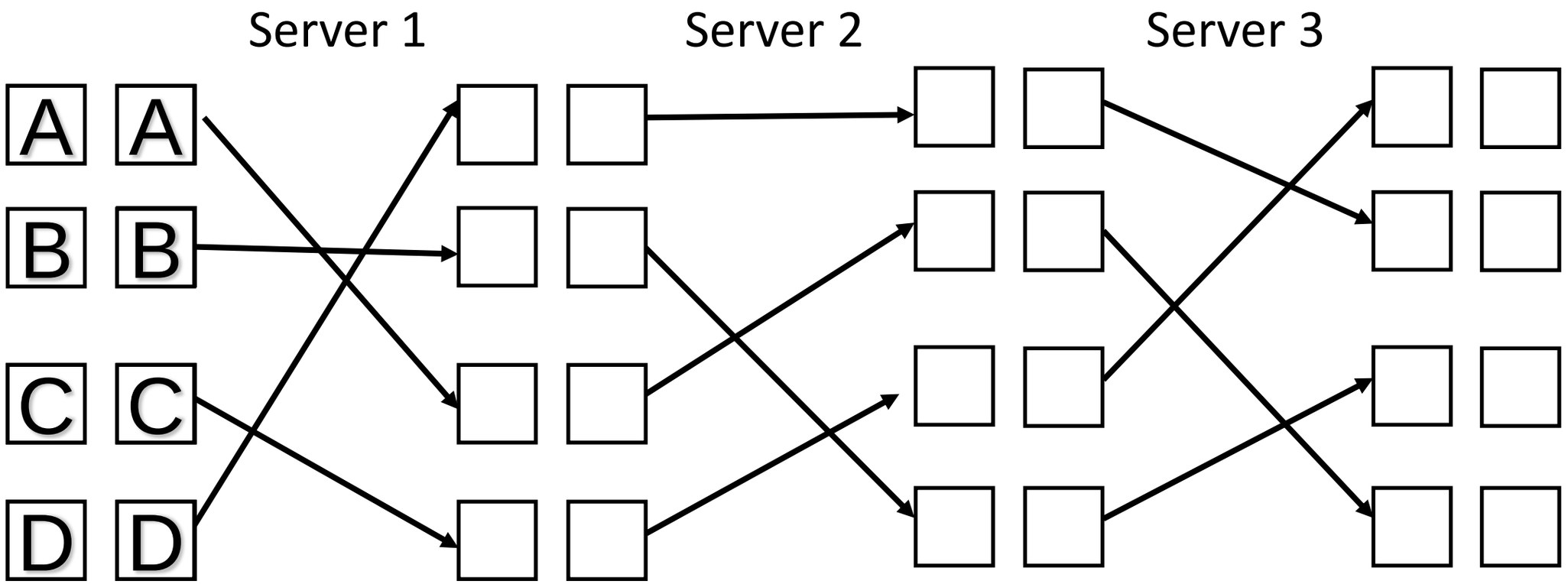
Implementation Timings

Processing stage	Time taken	Approximation
Cipher generation	39hrs 34mins	1.4 seconds per ballot
Mixing ATL	2hrs 0mins	12 ballots per second
Decryption ATL	12mins 9s	120 ballots per second
Mixing BTL	1hr 33mins	2 ballots per second
Decryption BTL	9mins 27sec	18 ballots per second
Reconstructing BTL	57mins 10sec	3 ballots per second

100,000 ballots:

38 candidates, 8 parties, 90000 ATL + 10000 BTL votes

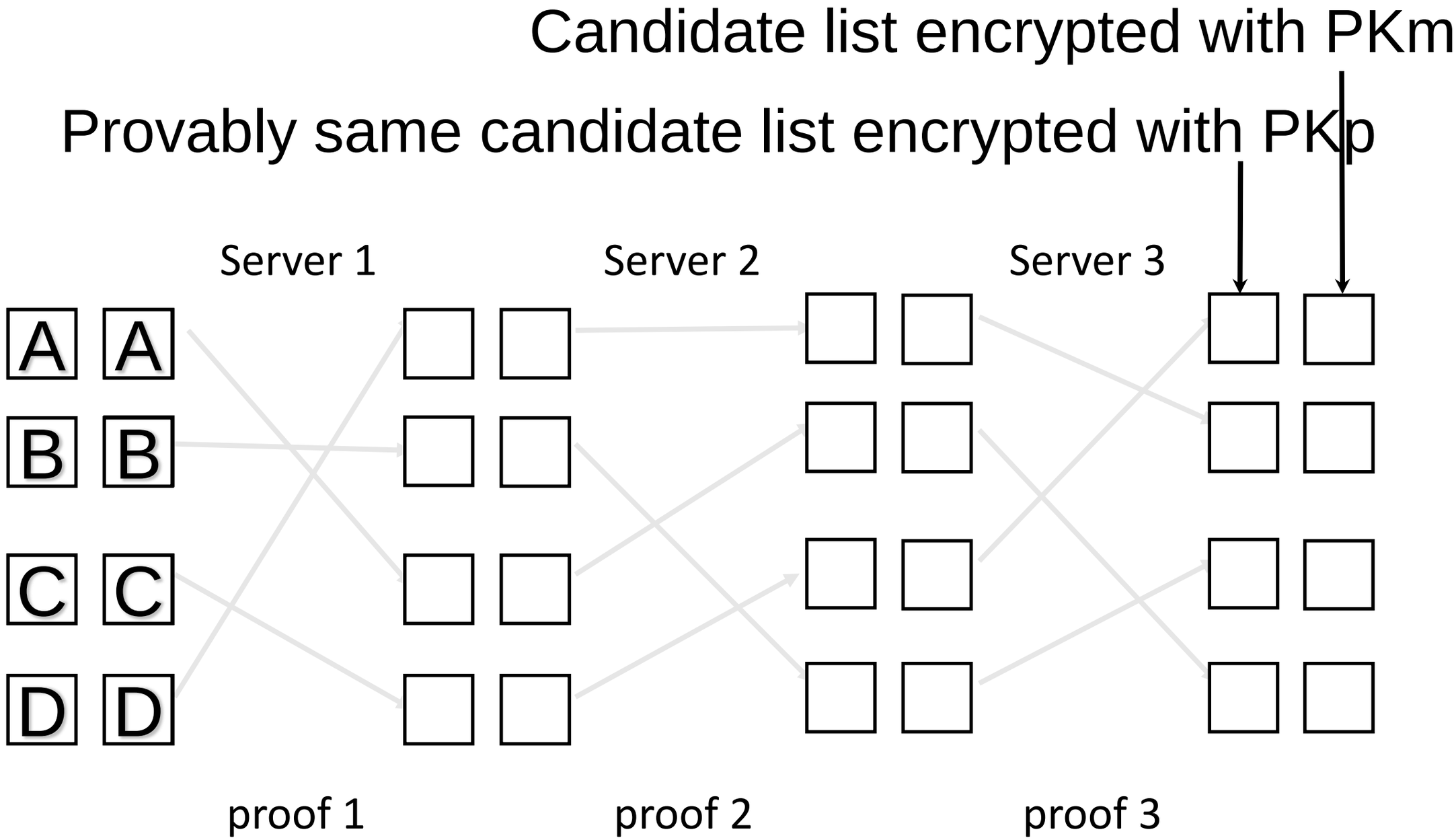
Distributed Ballot Generation



- Servers inject randomness, and re-encrypt with a different key for the two parts:

  (PKp{c,r1}, PKm{c,r1'}) → (PKp{c,r2}, PKm{c,r2'})

Distributed Ballot Generation



- Servers publish proofs of shuffle
- PKm and PKp are threshold keys

Print on Demand: step 1

Ballot printer

< PKp(b_i) >

< ZKP(b_i) >

Bulletin Board

- Printer generates a blinding factor b_i for each candidate.
- Encrypts them with PKp
- Sends them to the ballot servers as a ballot request, with a proof of knowledge (ZKP)

Print on Demand: step 2

Bulletin Board

Ballot #N

PKp(c_1)

PKp(c_2)

PKp(c_3)

PKp(c_4)

- Ballot server selects an unused ballot: #N

Print on Demand: step 2

Bulletin Board

Ballot #N

PKp(c_1+b_1)

PKp(c_2+b_2)

PKp(c_3+b_3)

PKp(c_4+b_4)

- Ballot server selects an unused ballot: #N
- Combines the blinding factors with the encrypted names

Print on Demand: step 2

Bulletin Board

Ballot #N

c_1+b_1

c_2+b_2

c_3+b_3

c_4+b_4

- Ballot server selects an unused ballot: #N
- Combines the blinding factors with the encrypted names
- (Threshold) decrypts the blinded names

Print on Demand: step 3

Ballot printer

< c_i + b_i >

Bulletin Board

- Blinded candidate names returned to the printer

Print on Demand: step 4

Ballot printer

Ballot #N

c_1+b_1

c_2+b_2

c_3+b_3

c_4+b_4

- Printer removes blindings on names

Print on Demand: step 4

Ballot printer

Ballot #N

c_1

c_2

c_3

c_4

- Printer removes blindings on names

Print on Demand: step 4

Ballot printer

Ballot #N

c_1

c_2

c_3

c_4

- Printer removes blindings on names
- Printer can then print ballot form

Auditing printed ballots

- If a printed ballot is challenged...
- ... the ballot servers can threshold decrypt the blinding factors PKp(b_i) provided by the printer,
  ... which enables the c_i + b_i values to be unblinded and checked against the printed ballot
- ... or can threshold decrypt the candidate names Kp(c_i) directly, and check against the printed ballot

Conclusion

- Usability, accessibility, and remote voting, while retaining assurance in the system, are key drivers.
- Prêt à Voter can be customised to the VEC requirements. The main new design feature is the EBM, which introduces fresh challenges. Scaling up also raises issues with processing the votes
- A demonstrator is currently being implemented for evaluation, with a view to VEC trialling it next year
- The system can handle the scale of Australian state elections
- Verifiability comes from the ability to check the information published by the system. The code is also open to inspection, though it's the output of the code that is verified