Authentication Codes

Chris Culnane, David Bismark,
James Heather, Steve Schneider,
Sriramkrishnan Srinivasan, and Zhe Xia

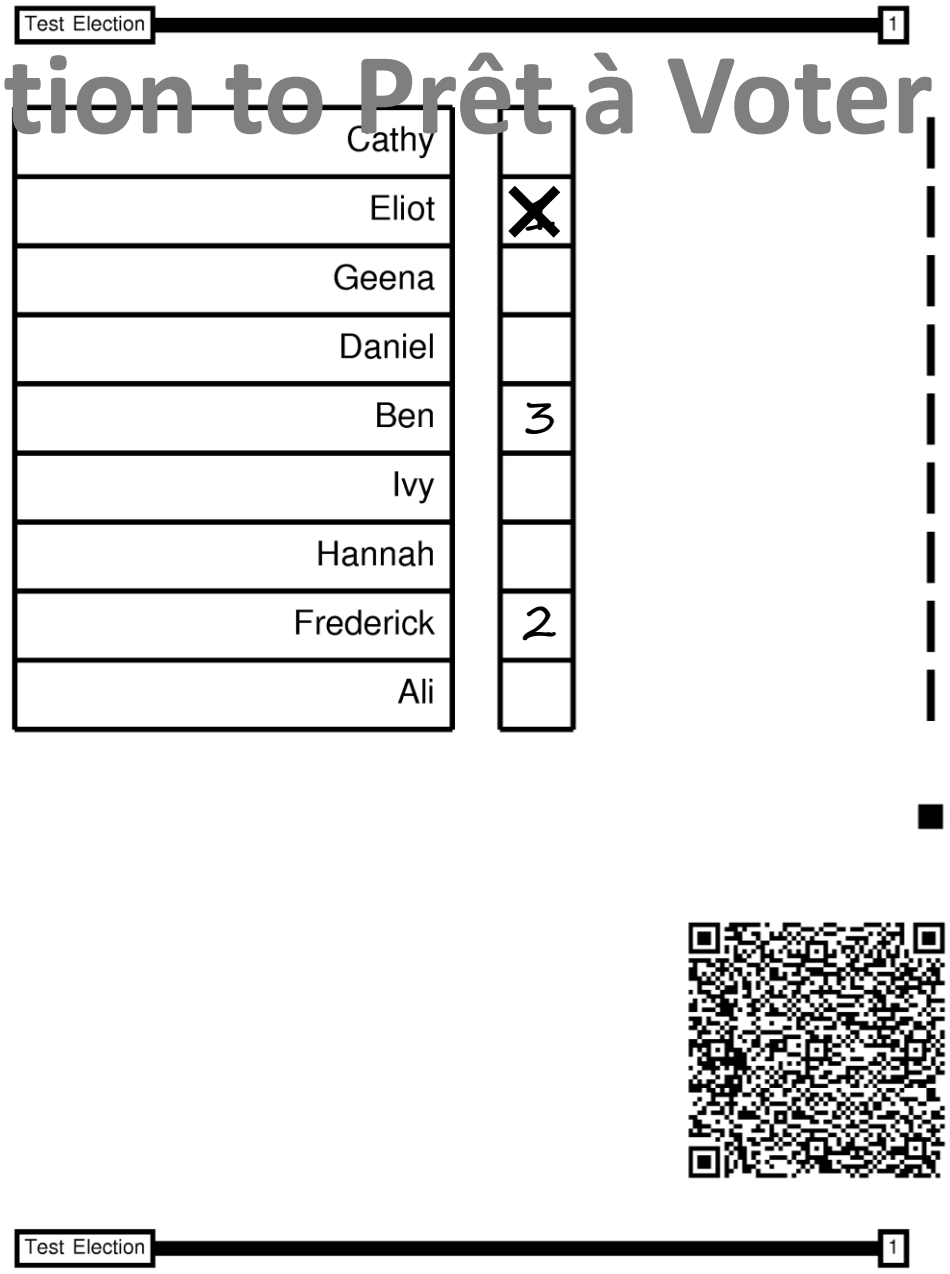
Trustworthy Voting Systems Project

UNIVERSITY OF SURREY

Overview

- Introduction to Prêt à Voter
- Importance of Digital Signatures
- Human Verifiable Codes
- Authentication Codes
- Short Code Variant
- Future Work

Introduction to Prêt à Voter



Thank you for voting!

By the time you see this receipt, your vote will already have been submitted electronically.

User Trial Election 2010 000172

How to check your voting receipt

This receipt contains the information you need in order to check that your vote has been correctly counted. It is your protection against election fraud or misconduct.

Before leaving the polling station, you need to follow this procedure:

Mark a cross (X) in the right hand box next to the name of the candidate you wish to vote for.

68nav-b71f4-477
b88cv-eh7qf-r7k

1. First, check that the vote orderings on your form match with those on this receipt, and that the security codes (letters and numbers beneath the grid of black and white squares) match too. The black and white squares need **not** match.

2. If your vote information or your security code does **not** match, you need to take this receipt and the right-hand side of your ballot paper to the desk so that your form can be cancelled and you can be issued with a new one.

If you wish to check that your vote has been counted correctly, then when you have left the polling station, you can go to the election web site and click on '**Where's my vote?**'. You will need to have this receipt with you.

RECEIPT

Human Verifiable Codes

- Acknowledgement Codes in PGD
- Matrix of codes
- New simpler approach proposed

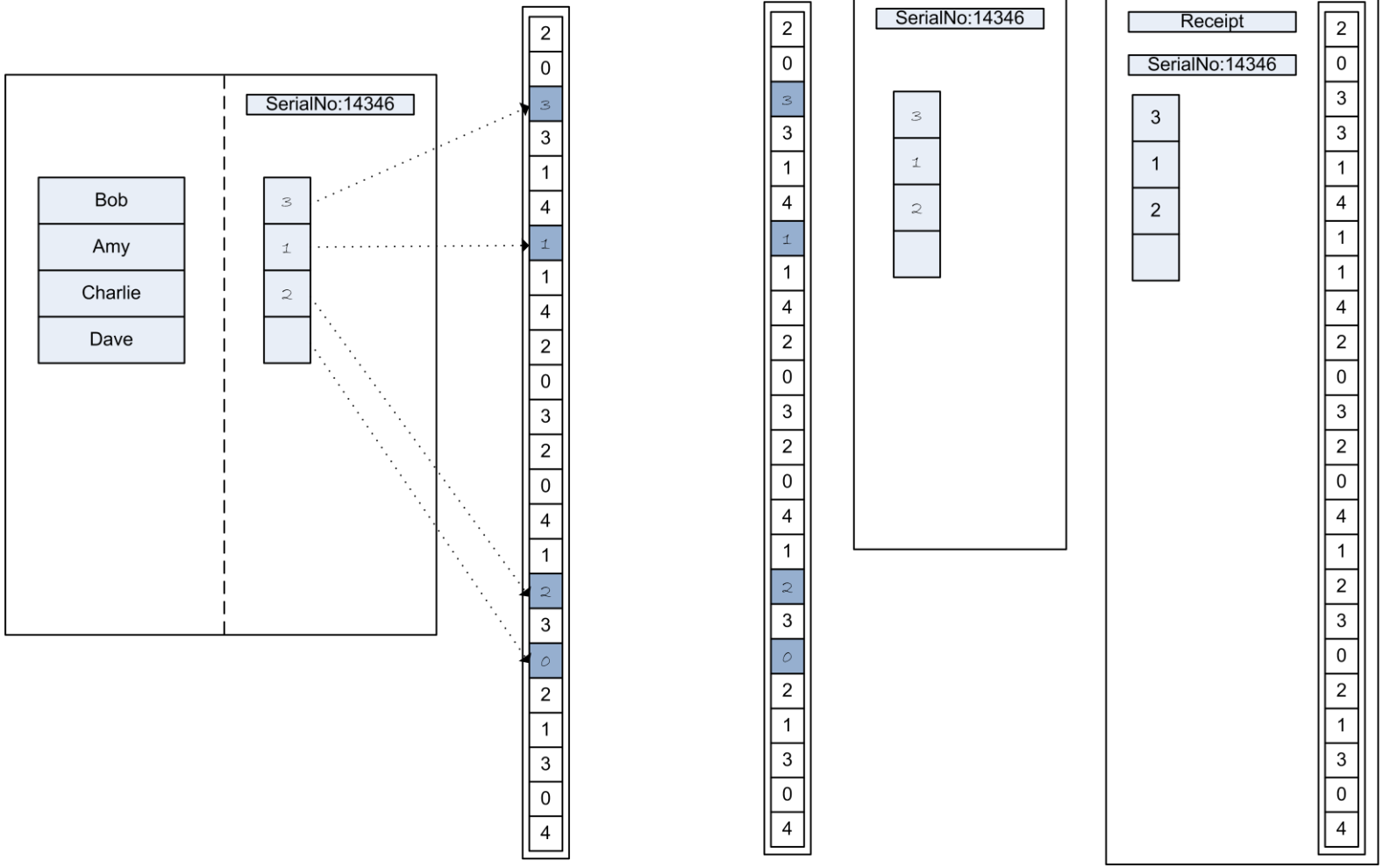
Authentication Codes

- Universal front-end for both ranked and plurality elections
- Simple to use
- Provides assurance that vote has been recorded as cast
- Verification, and any challenge, is performed in the polling station

Assumptions

- Peered Web Bulletin Board
- Trusted Election Manager
- Chain of custody

Overview


SerialNo:14346
Bob
Amy
Charlie
Dave
3
1
2
SerialNo:14346
3
1
2
Receipt
SerialNo:14346
3
1
2

Election Manager

- Notation
  - n = number of candidates
  - m = preference range (n in ranked elections, 1 in plurality elections)
  - φ denotes blank spaces
- Take values between 0 and m, along with one φ
- Randomly permute and concatenate, n times
- The following example uses n =4

Election Manager

$$0, 1, 2, 3, 4, \phi$$

$$20\phi 314, \phi 14203, 2041\phi 3, \phi 21304$$

- Extract locations of φ [3,7,17,19]
- Replace φ with zero

$$20031401420320410302 1304$$

- Create Authentication Values
  - Zero value with a 1 in the location of φ

Election Manager

- Locations of φ [3,7,17,19]

$$0000000000000000000000$$

$$0010000000000000000000$$

$$0000001000000000000000$$

$$0000000000000010000000$$

$$0000000000000000100000$$

Election Manager

- The Authentication Values and Authentication Code are encrypted using the shared public key

$$E_{PK_{wbb}}(200314014203204103021304)$$

$$E_{PK_{wbb}}(001000000000000000000000)$$

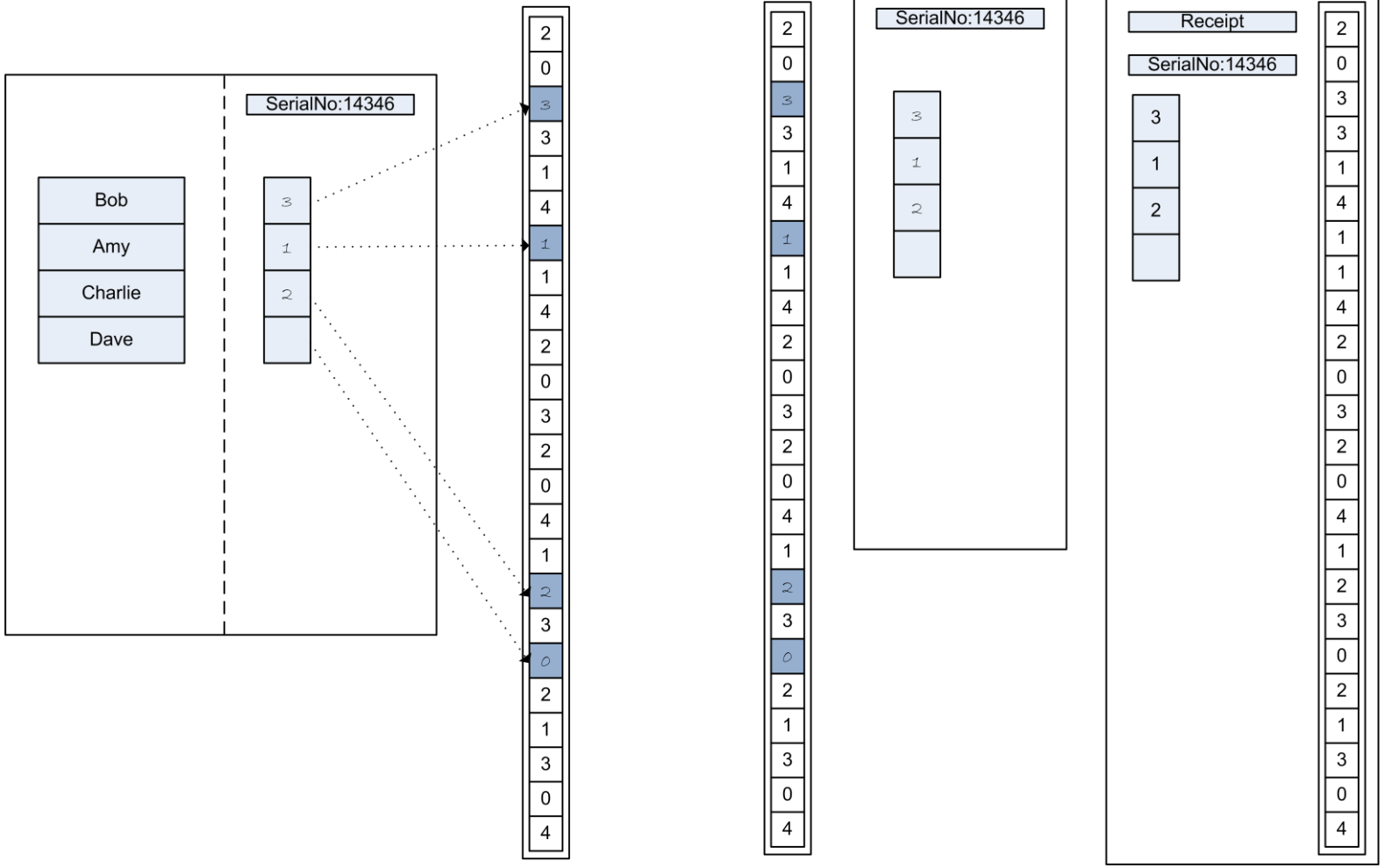
$$E_{PK_{wbb}}(000000100000000000000000)$$

$$E_{PK_{wbb}}(000000000000000010000000)$$

$$E_{PK_{wbb}}(000000000000000000100000)$$

- These encrypted values are sent to each peer

Voter Perspective



WBB Perspective

- Receives voting preferences [3,1,2,0]
- Each peer, independently, constructs Authentication Code from encrypted values and decrypts
- Partial decryptions from peers are combined and plaintext returned to voter

Scaling

$$E_{PK_{wbb}}(00100000000000000000000)$$

$$E_{PK_{wbb}}(00000010000000000000000)$$

$$E_{PK_{wbb}}(00000000000000010000000)$$

$$E_{PK_{wbb}}(00000000000000000100000)$$

[3,1,2,0]

$$E_{PK_{wbb}}(00300000000000000000000)$$

$$E_{PK_{wbb}}(00000010000000000000000)$$

$$E_{PK_{wbb}}(00000000000000020000000)$$

$$E_{PK_{wbb}}(00000000000000000000000)$$

Addition

$$E_{PK_{wbb}}(20031401420320410302130 4)$$

$$E_{PK_{wbb}}(00300000000000000000000)$$

$$E_{PK_{wbb}}(00000010000000000000000)$$

$$E_{PK_{wbb}}(00000000000000020000000)$$

$$E_{PK_{wbb}}(00000000000000000000000)$$

$$E_{PK_{wbb}}(20331411420320412302130 4)$$

Decryption

- Each peer performs partial decryption and provides proof of decryption
- Each peer should have reconstructed exactly the same value to perform the decryption on
- Valid partial decryptions are combined and plaintext Authentication Code is returned to the voter

Summary

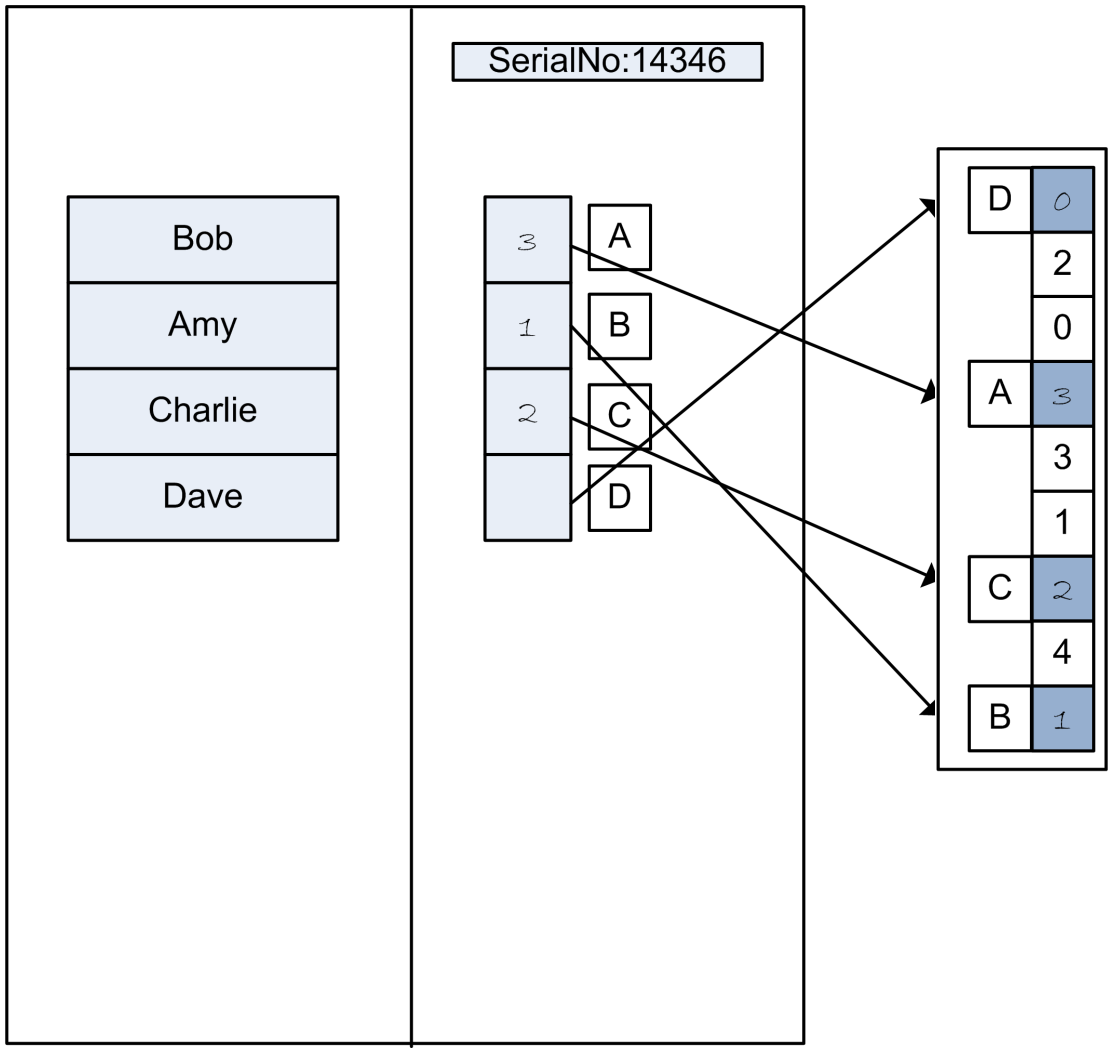
- Easy user interface
- Intuitive how preference is blinded
- Code length grows quadratically with n

Short Code Variant

- Reduce to linear growth
- Shorten initial code
- Additional level of indirection

- Code Length is given by: $n + (p-1)(n+1)$
- Where n is the number of candidates and p is $1/p$ probability of guessing location
- ½ probability -> p=2, if n=4
- 4+(2-1)(4+1) = 9

Short Code – Voter Perspective



Short Code Election Manager

- Notation
  - n = number of candidates
  - m = preference range (n in ranked elections, 1 in plurality elections)
  - φ denotes blank spaces
- Take values between 0 and m, along with n φ
- Randomly permute
- The following example uses n =4

Short Code Election Manager

$$0, 1, 2, 3, 4, \phi\, \phi\, \phi\, \phi$$

$$\phi 20 \phi 31 \phi 4 \phi$$

- Extract locations of φ [1,4,7,9]
- Replace φ with zero

$$020031040$$

- Create Authentication Values
  - Zero value with a 1 in the location of φ

Short Code Election Manager

- Locations of φ [1,4,7,9]

$$000000000$$

$$100000000$$

$$000100000$$

$$000000100$$

$$000000001$$

Short Code Election Manager

- The Authentication Values and Authentication Code are encrypted using the shared public key
- Each value is associated with a set of *n* labels in canonical order $E_{PK_{wbb}}(020031040)$

$$E_{PK_{wbb}}(100000000)(A)$$

$$E_{PK_{wbb}}(000100000)(B)$$

$$E_{PK_{wbb}}(000000100)(C)$$

$$E_{PK_{wbb}}(000000001)(D)$$

Short Code Election Manager

- Create indirection by randomly permuting labels

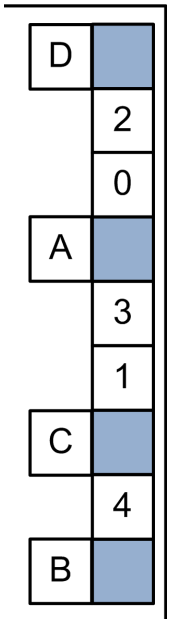
$$E_{PK_{wbb}}(020031040)$$

$$E_{PK_{wbb}}(100000000)(D)$$

$$E_{PK_{wbb}}(000100000)(A)$$

$$E_{PK_{wbb}}(000000100)(C)$$

$$E_{PK_{wbb}}(000000001)(B)$$



- The permuted list of letters is printed on the Authentication Strip

Short Code Election Manager

- Re-order Authentication Values according to canonical order of labels

$$E_{PK_{wbb}}(020031040)$$

$$E_{PK_{wbb}}(000100000)(A)$$

$$E_{PK_{wbb}}(000000001)(B)$$

$$E_{PK_{wbb}}(000000100)(C)$$

$$E_{PK_{wbb}}(100000000)(D)$$

- These values are sent to the WBB peers

WBB Perspective

- Identical to full length scheme

Summary

- Same level of security by using an additional level of indirection
- More work for the voter
  - Once a voter has destroyed their left hand side they can be assisted in filling in the Authentication Strip without breaking secrecy

Further Discussion

- Since the unverified digital signature does not provide the properties we desire, can we remove it and in doing so remove the need to check the WBB?
- There is an additional chain of custody burden for the Authentication Strip
  - There is already a chain of custody for the ballot form (in terms of privacy)

Future Work

- Out of band construction of Authentication Strip
  - Removes chain of custody problem
  - Possibly increases coercion?
- How to audit Authentication Strips
- How can Authentication Strips be used during the Prêt à Voter ballot form audit

QUESTIONS?