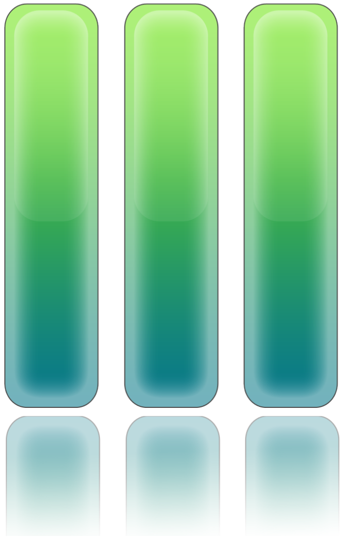
Eperio

Mitigating Technical Complexity in Cryptographic Election Verification



Aleksander Essex, **Jeremy Clark**
Urs Hengartner, Carlisle Adams*

University of Waterloo,
**University of Ottawa*

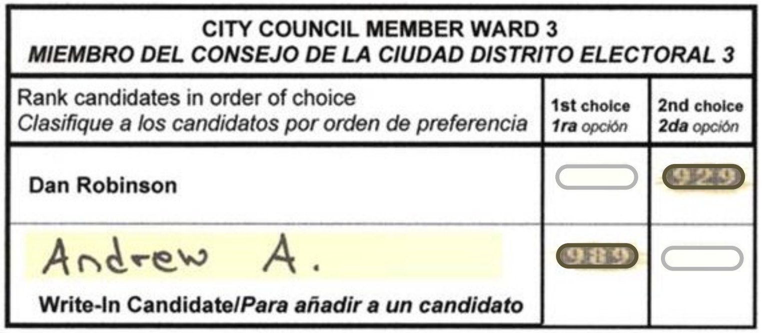
EVT/WOTE '10 August 10, 2010

End-to-end elections

- Cryptographic election verification with **strong integrity** and **privacy** assurance

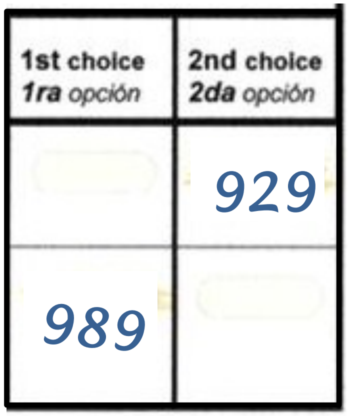
- **Universal** verification:
  - **Anyone** has option to participate

End-to-end elections



CITY COUNCIL MEMBER WARD 3 *MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 3*		
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*
Dan Robinson	○	929
Andrew A. Write-In Candidate/*Para añadir a un candidato*	989	○

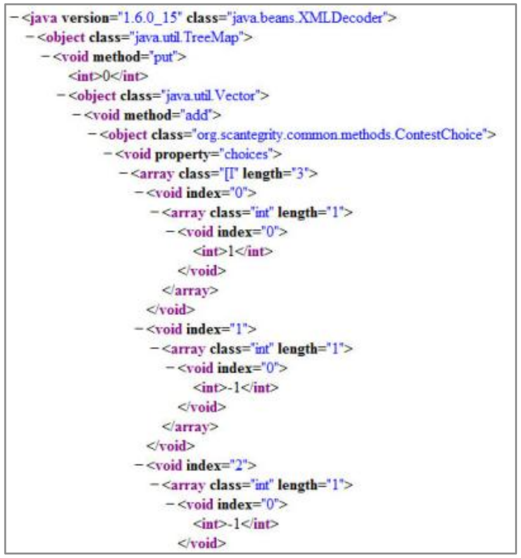
Enhanced Ballot



1st choice *1ra opción*	2nd choice *2da opción*
	929
989	

Receipt

http://www.election



```
- <java version="1.6.0_15" class="java.beans.XMLDecoder">
  - <object class="java.util.TreeMap">
    - <void method="put">
        <int>0</int>
      - <object class="java.util.Vector">
        - <void method="add">
          - <object class="org.scantegrity.common.methods.ContestChoice">
            - <void property="choices">
              - <array class="[I" length="3">
                - <void index="0">
                  - <array class="int" length="1">
                    - <void index="0">
                        <int>1</int>
                      </void>
                    </array>
                  </void>
                - <void index="1">
                  - <array class="int" length="1">
                    - <void index="0">
                        <int>-1</int>
                      </void>
                    </array>
                  </void>
                - <void index="2">
                  - <array class="int" length="1">
                    - <void index="0">
                        <int>-1</int>
                      </void>
```

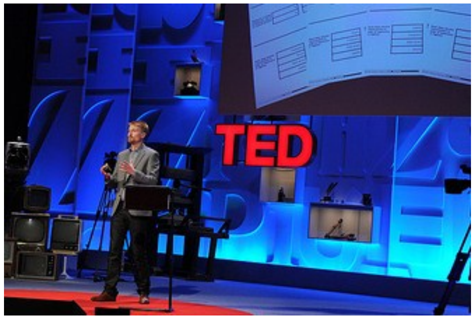
Public audit data

End-to-end elections

- Worldwide research
- Over a dozen elections
- Thousands of voters
- Debut in public-sector
- Growing interest

scantegrity

UNIVERSITY OF Waterloo



GSAÉD Élections 2007

Prêt à Voter

CITY OF TAKOMA PARK MARYLAND 1890

THE UNIVERSITY OF IOWA

CPSR Computer Professionals For Social Responsibility

Newcastle University

Punchscan

The University of Surrey Students' Union

claimdemocracy

a prodemocracy gathering

Washington, DC - Nov. 9th to 11th

5236235 2538345

ACCURATE

Microsoft Research

uni.lu UNIVERSITÉ DU LUXEMBOURG

VE RI TAS

Universität Karlsruhe (TH)

Forschungsuniversität • gegründet 1825

Helios

THE GEORGE WASHINGTON UNIVERSITY WASHINGTON DC

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

THE UNIVERSITY OF MELBOURNE

NIST

PRINCETON UNIVERSITY

End-to-end Elections

- Recent research focused on making E2E:
  - Easy to **vote**
  - Easy to **administer**
- What about easy to **audit**?

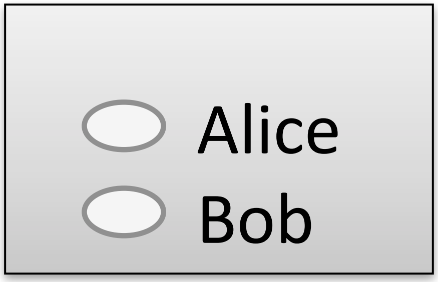
End-to-end Elections

- Conflicting views on **cryptography** in **elections**:
  - **Max-crypto**
    - Security at **expense** of inclusiveness
  - **No-crypto**
    - Inclusiveness at **expense** of security
- Our goal:
  - **Min-crypto** ✓
    - **Balance** security and inclusiveness

Eperio

- What it is
  - **E2E** election verification protocol
- What it means for verification
  - Fewer cryptographic **primitives**
  - Smaller **datasets**
  - Faster **execution**
  - Fewer **lines of code**

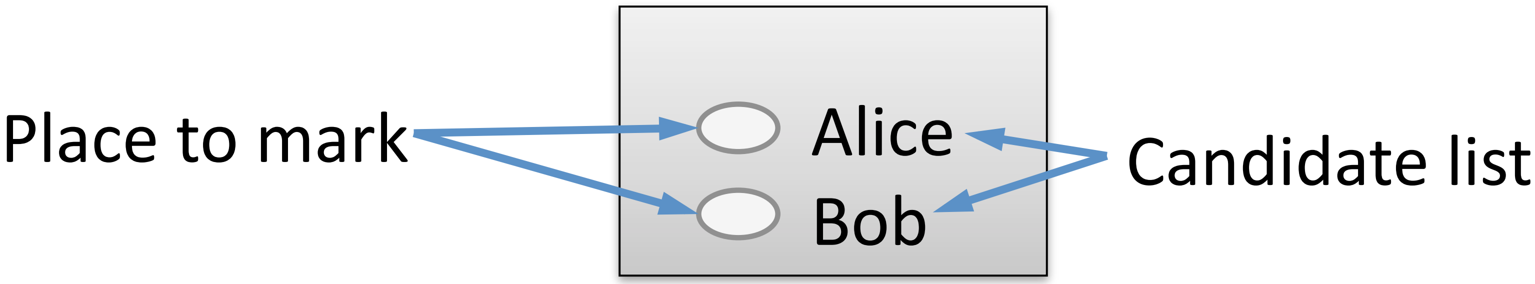
Consider an optical scan ballot



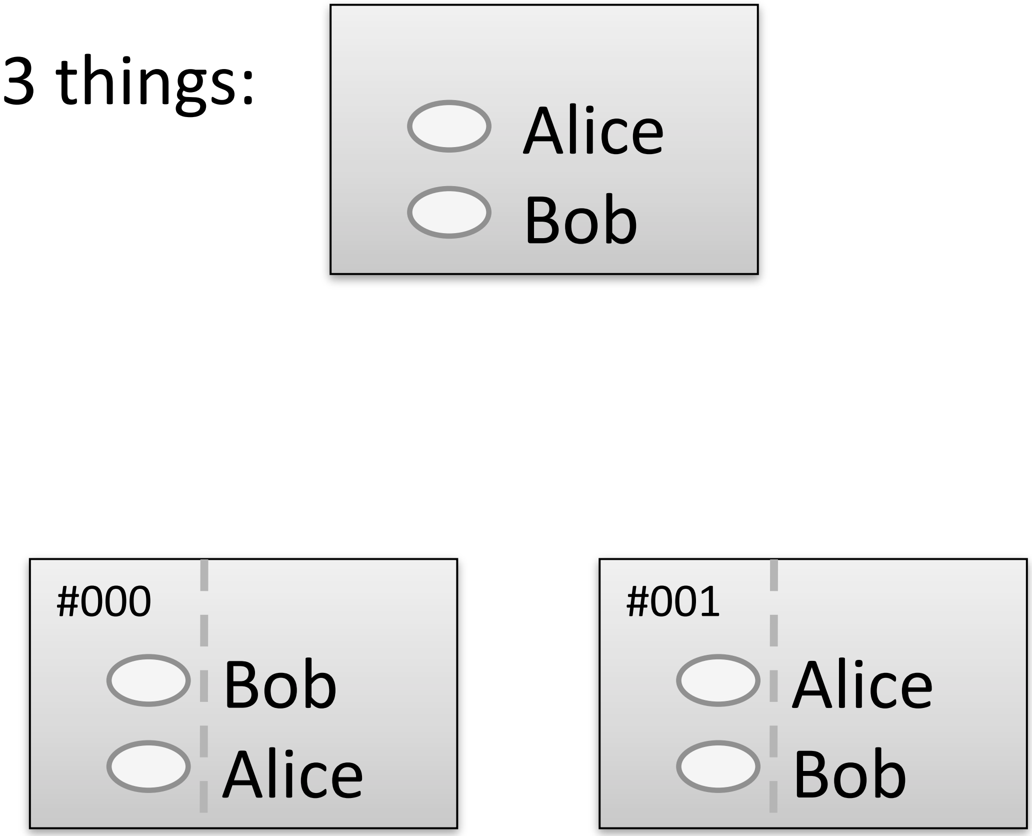
○ Alice

○ Bob

Consider an optical scan ballot



Let’s add 3 things:

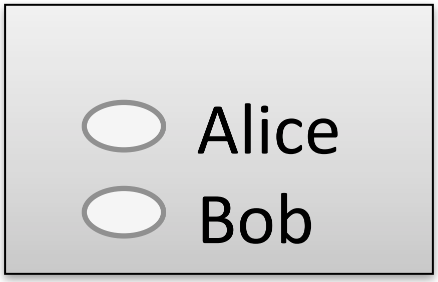


○ Alice
○ Bob

#000
○ Bob
○ Alice

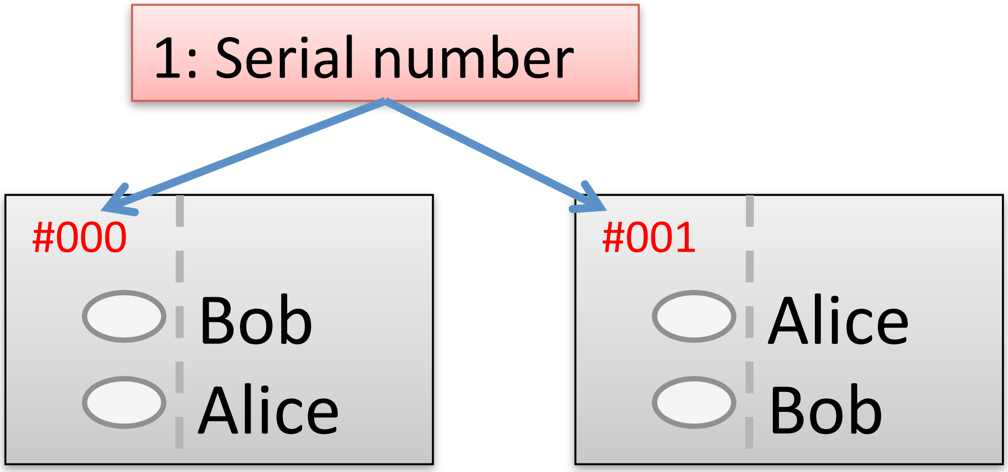
#001
○ Alice
○ Bob

Let’s add 3 things:



○ Alice

○ Bob



1: Serial number

#000

○ Bob

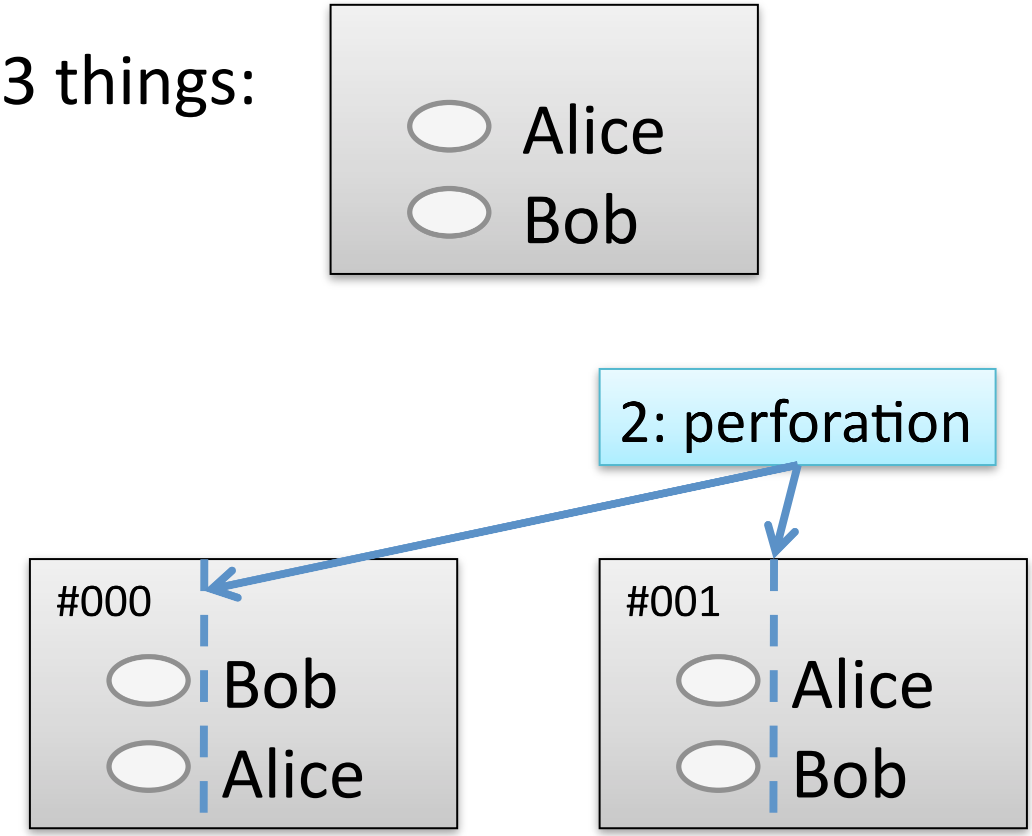
○ Alice

#001

○ Alice

○ Bob

Let’s add 3 things:



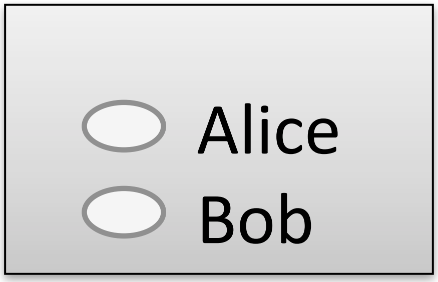
○ Alice
○ Bob

2: perforation

#000
○ Bob
○ Alice

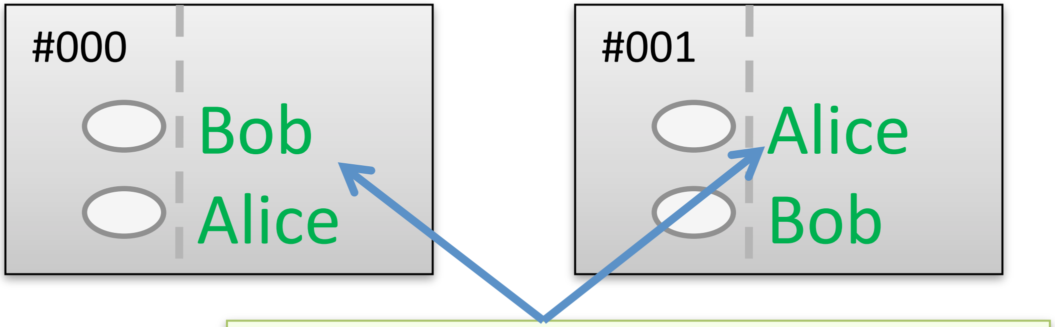
#001
○ Alice
○ Bob

Let’s add 3 things:



○ Alice

○ Bob



#000

○ Bob

○ Alice

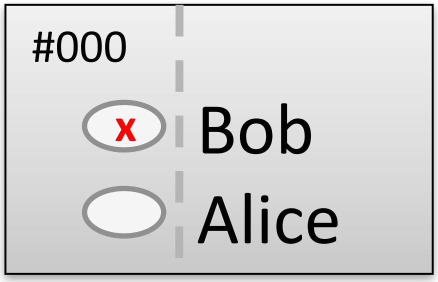
#001

○ Alice

○ Bob

3: Randomized candidate list

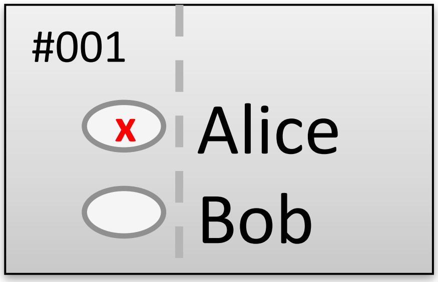
Marking...



#000

☒ Bob

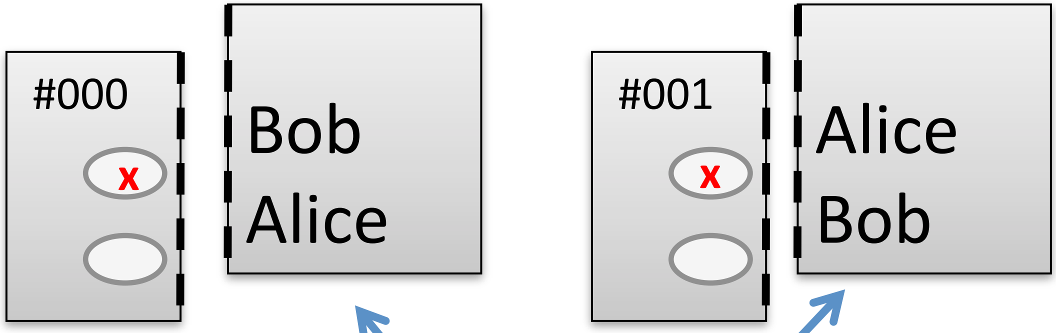
○ Alice



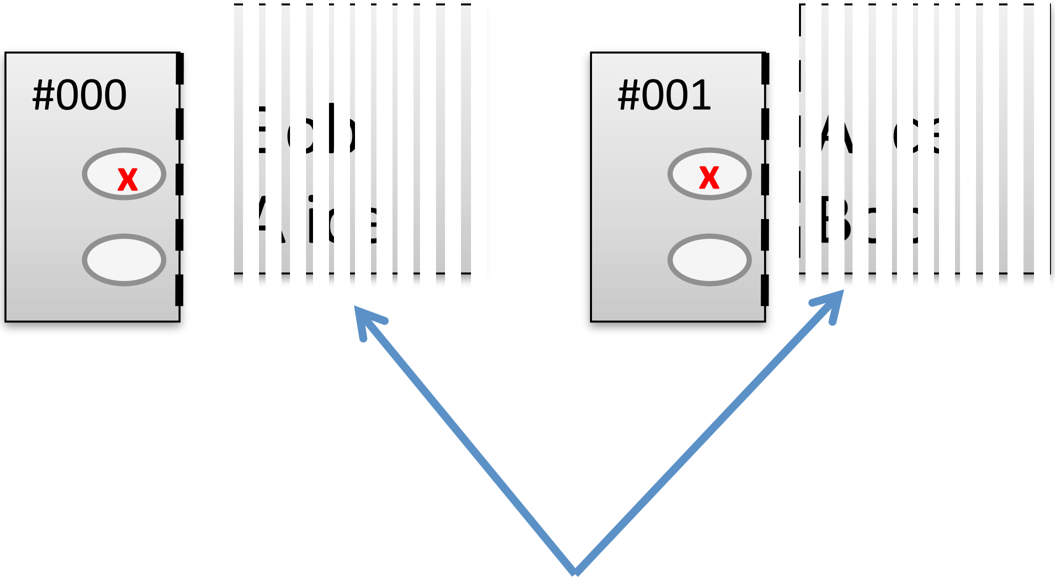
#001

☒ Alice

○ Bob

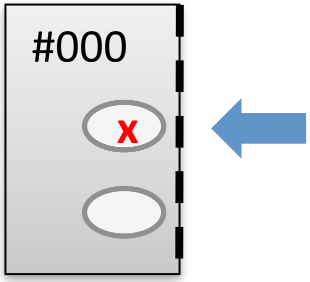


Tear off…



...and destroy

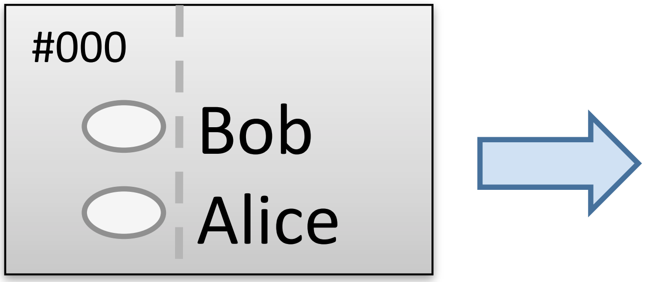
Voila. Receipts!



Alice? Bob?

Before the election….

Trustees* copy ballots into a table

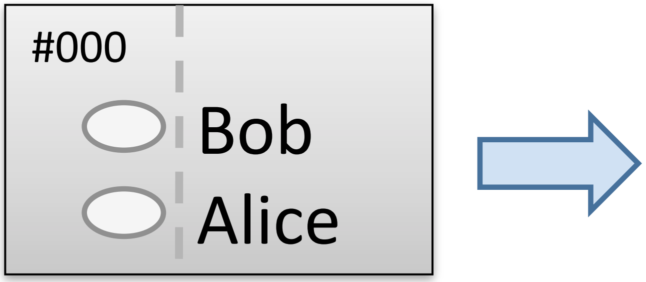


Bubble ID	Marked?	Candidate

*Done obliviously

Before the election….

Trustees* copy ballots into a table

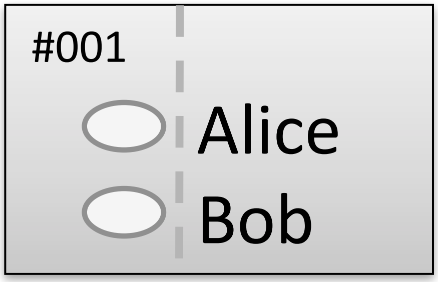


Bubble ID	Marked?	Candidate
#000-1st		Bob
#000-2nd		Alice

*Done obliviously

Before the election….

Trustees* copy ballots into a table



Bubble ID	Marked?	Candidate
#000-1st #000-2nd		Bob Alice
#001-1st #001-2nd		Alice Bob

*Done obliviously

Before the election….

Bubble ID	Marked?	Candidate
#000-1st #000-2nd		Bob Alice
#001-1st #001-2nd		Alice Bob
… …	… …	… …

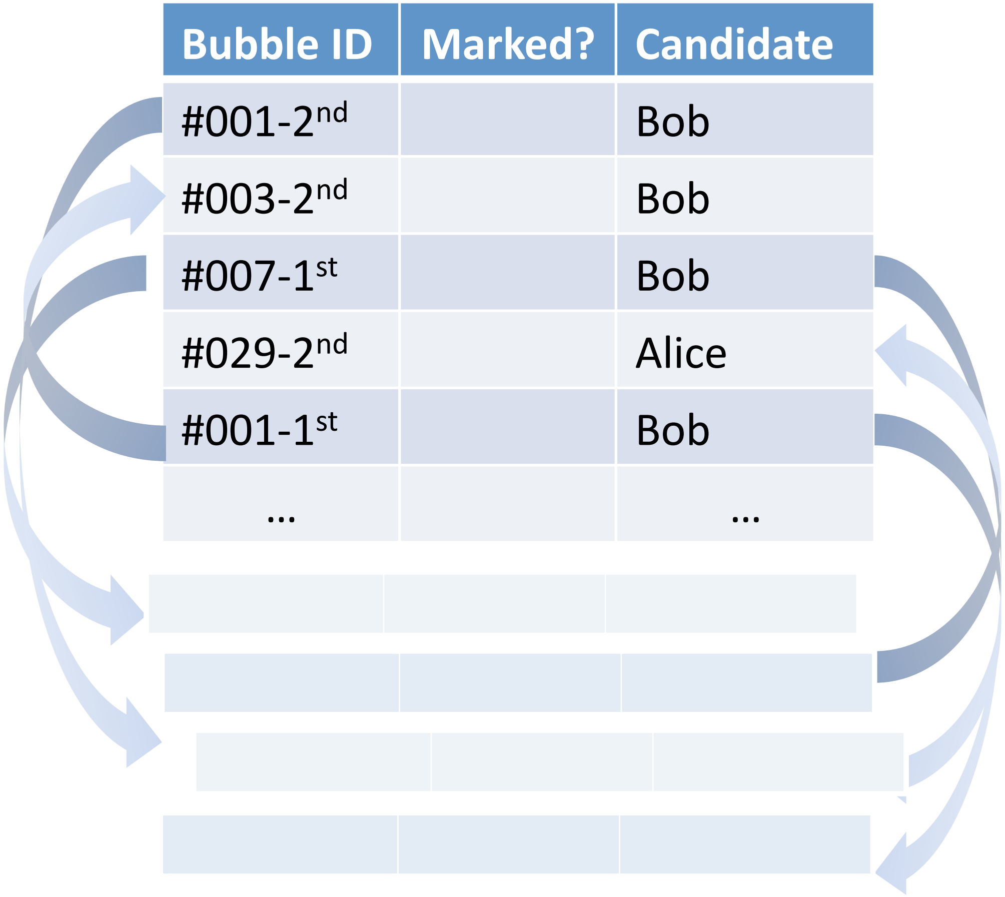
And so on…

The Eperio Table:

Bubble ID	Marked?	Candidate
#000-1st		Bob
#000-2nd		Alice
#001-1st		Alice
#001-2nd		Bob
…		…

Remember: it’s ***just*** the ballots in table-form.

Trustees shuffle rows

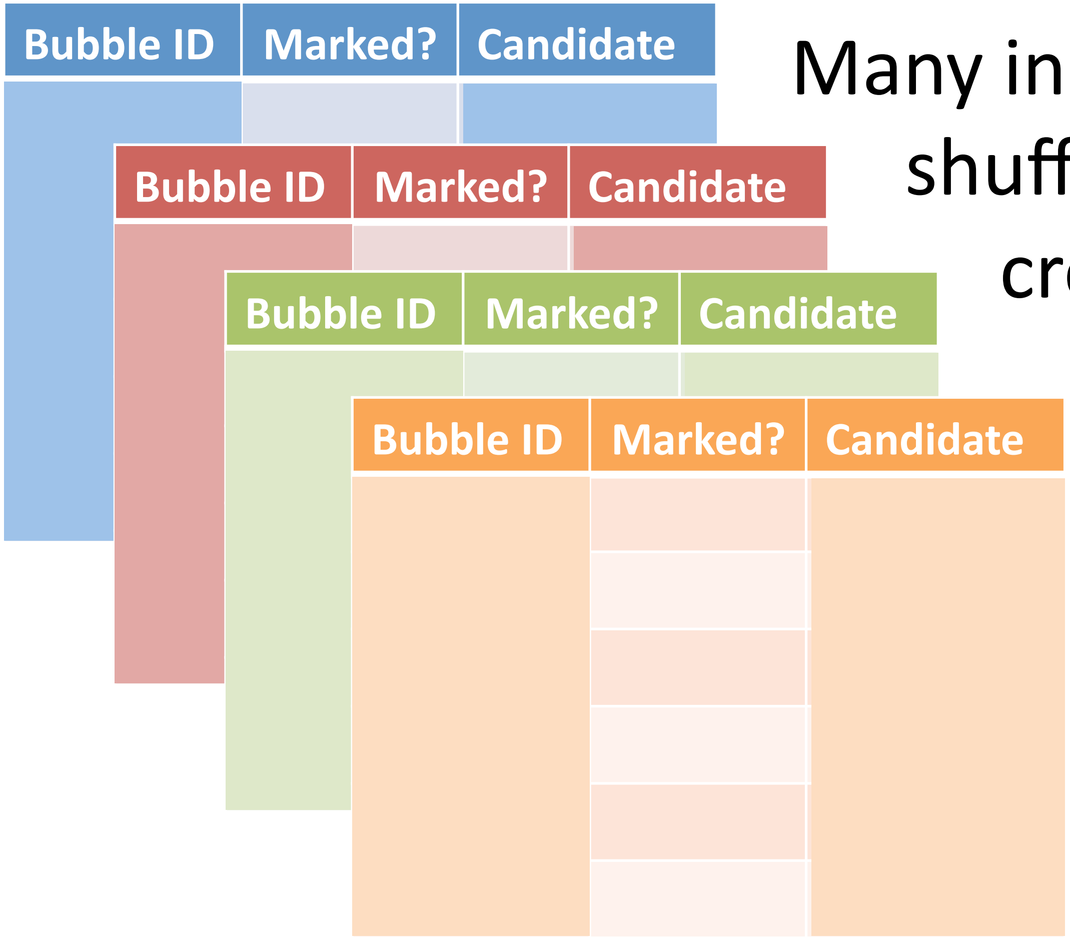


Bubble ID	Marked?	Candidate
#001-2nd		Bob
#003-2nd		Bob
#007-1st		Bob
#029-2nd		Alice
#001-1st		Bob
…		…

Trustees mask columns

Bubble ID	Marked?	Candidate
#001-2nd		Bob
#003-2nd		Bob
#007-1st		Bob
#029-2nd		Alice
#001-1st		Bob
…		…

Cryptographically committed and **published**



Bubble ID Marked? Candidate

Bubble ID Marked? Candidate

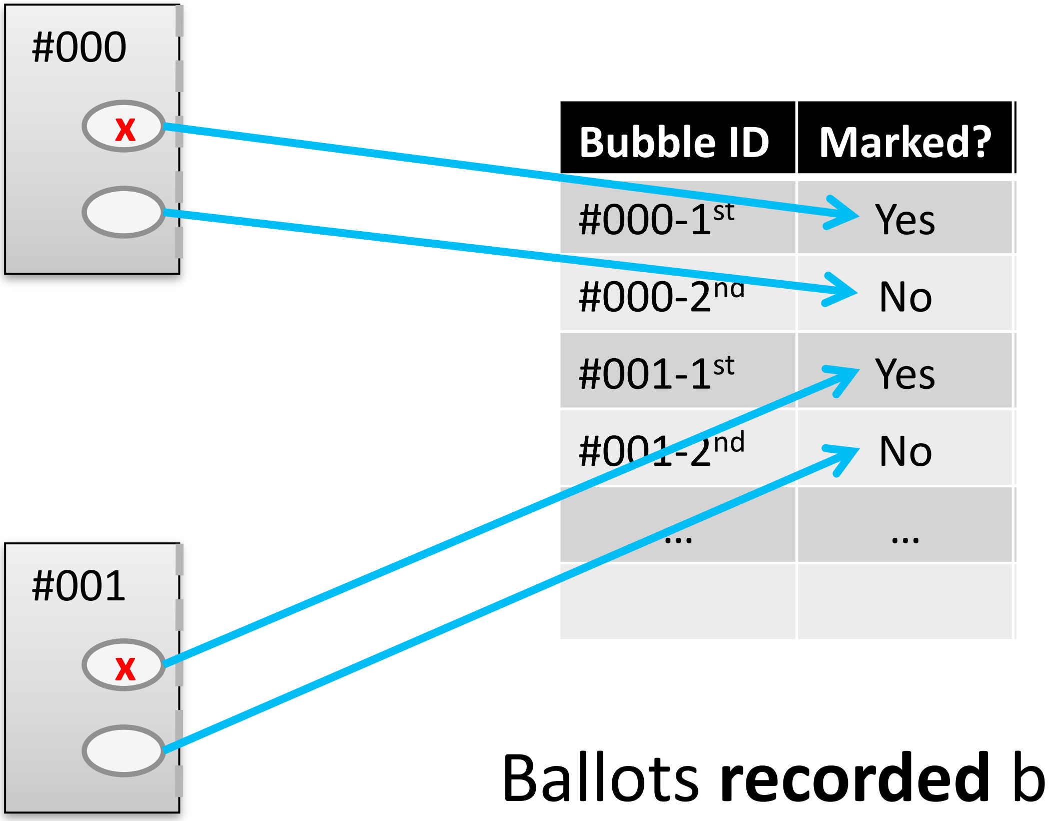
Bubble ID Marked? Candidate

Bubble ID Marked? Candidate

Many independent shuffled copies created

More instances scales security assurance

During the election…



Bubble ID	Marked?
#000-1st	Yes
#000-2nd	No
#001-1st	Yes
#001-2nd	No
…	…

Ballots **recorded** by scanner

After the election:

Bubble ID	Marked?
#000-1st	Yes
#000-2nd	No
#001-1st	Yes
#001-2nd	No
…	…

Bubble ID	Marked?	Candidate
#001-2nd	No	Bob
#003-2nd	Yes	Bob
#007-1st	Yes	Bob
#029-2nd	No	Alice
#001-1st	Yes	Alice
…	…	…

Trustees **fill in** middle columns

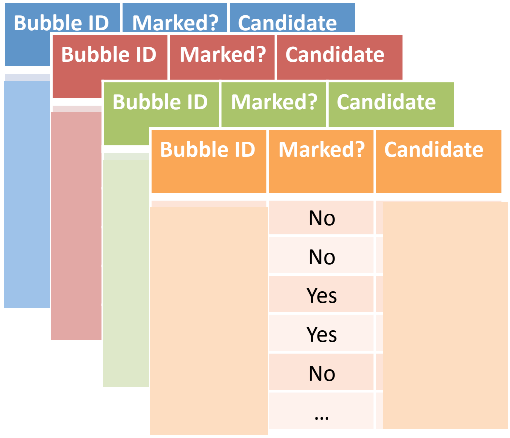
After the election:

Bubble ID	Marked?
#000-1st	Yes
#000-2nd	No
#001-1st	Yes
#001-2nd	No
…	…

Bubble ID	Marked?	Candidate
#001-2nd	Yes	Bob
#031-2nd	Yes	Bob
#001-1st	Yes	Alice
#029-2nd	No	Alice
#021-1st	Yes	Bob
…	…	…

Trustees **fill in** middle columns

The Audit Challenge



Bubble ID	Marked?	Candidate
	No	
	No	
	Yes	
	Yes	
	No	
	…	

- Challenge
  - Public coin toss
  - **One** column from each instance **challenged**
- Response
  - Trustees post decommitments

Checking receipts

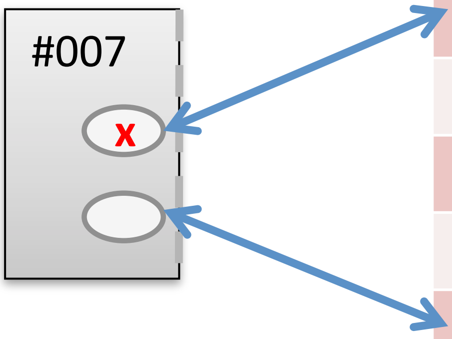
Bubble ID	Marked?	Candidate
	Yes	
	Yes	
	Yes	
	No	
	Yes	
	…	

Checking receipts

Bubble ID	Marked?	Candidate
#007-1st	Yes	
#006-2nd	Yes	
#042-1st	Yes	
#029-2nd	No	
#007-2nd	No	
…	…	

Bubble ID column decommitted

Checking receipts



Bubble ID	Marked?	Candidate
#007-1st	**Yes**	
#006-2nd	Yes	
#042-1st	Yes	
#029-2nd	No	
#007-2nd	**No**	
…	…	

Voter looks up receipt. Checks for match.

Tally audit

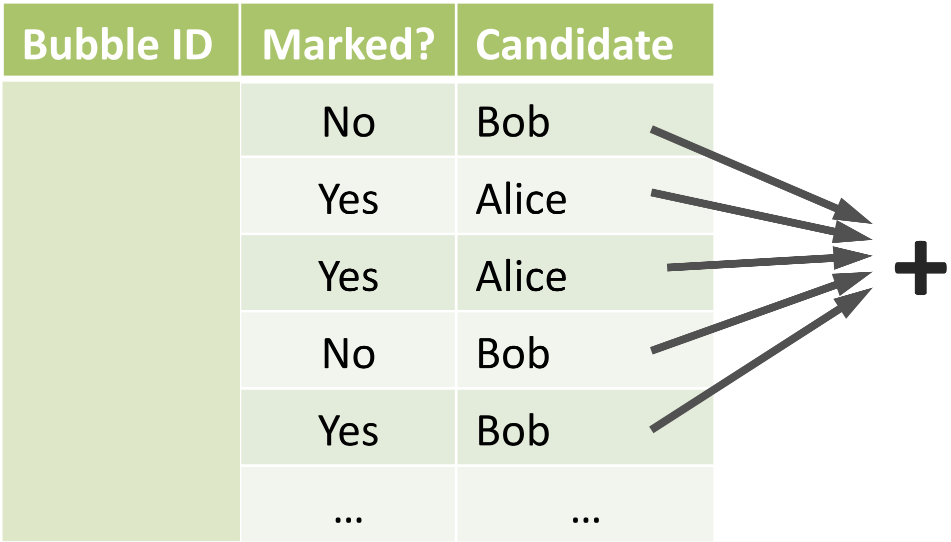
Bubble ID	Marked?	Candidate
	No	
	Yes	
	Yes	
	No	
	Yes	
	…	

Tally audit

Bubble ID	Marked?	Candidate
	No	Bob
	Yes	Alice
	Yes	Alice
	No	Bob
	Yes	Bob
	…	…

Candidate column decommitted

Tally audit



Bubble ID	Marked?	Candidate
	No	Bob
	Yes	Alice
	Yes	Alice
	No	Bob
	Yes	Bob
	…	…

Tally like any election

Repeat as necessary…

Bubble ID	Marked?	Candidate
	No	Bob

Bubble ID	Marked?	Candidate
#001-2nd	No	
#003-		
#007-		
#029-		
#001-		
..		

Bubble ID	Marked?	Candidate
#007-1st	Yes	
#006-2		
#042-1		
#029-2		
#007-2		
…		

Bubble ID	Marked?	Candidate
	No	Alice
	Yes	Bob
	Yes	Bob
	Yes	Alice
	No	Bob
	…	…

Review

- Eperio table instance
  - Just a **copy** of ballots
  - Independently **shuffled**
  - **Committed**
  - **Published**

Bubble ID	Marked?	Candidate
#001-2nd	No	Bob
#003-2nd	Yes	Bob
#007-1st	Yes	Bob
#029-2nd	No	Alice
#001-1st	Yes	Bob
…	…	…

- Columns
  - Right + middle = **tally**
  - Left + middle = **receipt info**

How is Eperio different?

- Table structure
- Commitment scheme
- Implementation options

What does this mean?

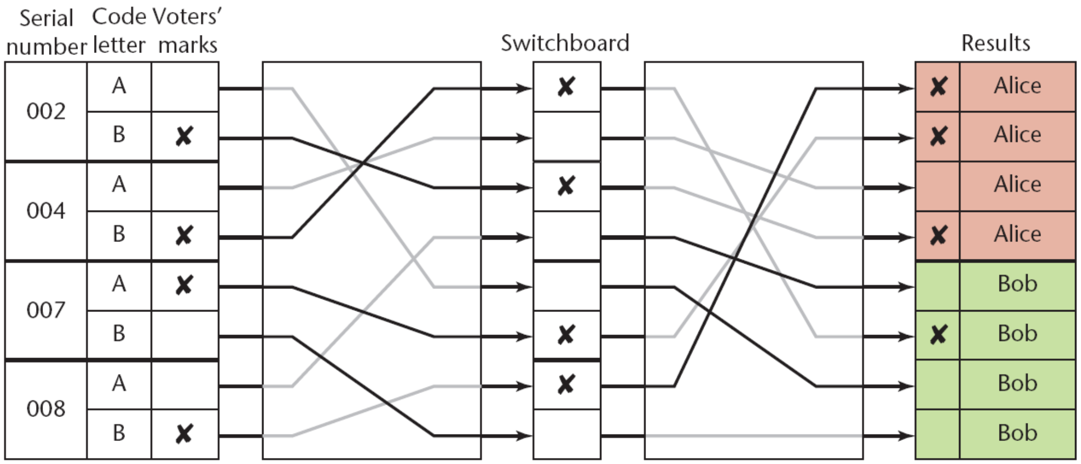
- Speed (10-100x faster)
- Data download (10-100x smaller)
- Small code size (50 lines of Python)

Table structure: a comparison

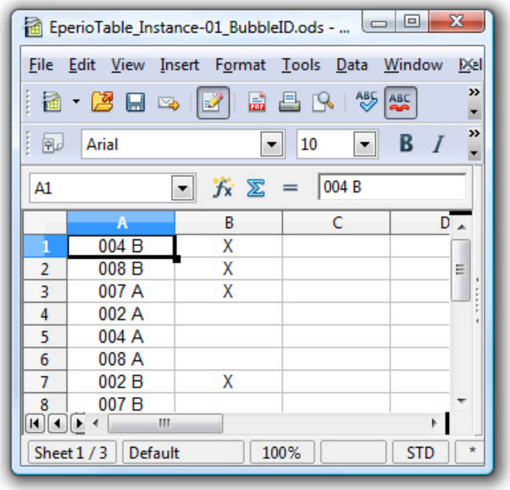
Eperio

Bubble ID	Marked?	Candidate
004 B	X	Bob
008 B	X	Alice
007 A	X	Alice
002 A		Bob
004 A		Alice
008 A		Bob
002 B	X	Alice
007 B		Bob

scantegrity



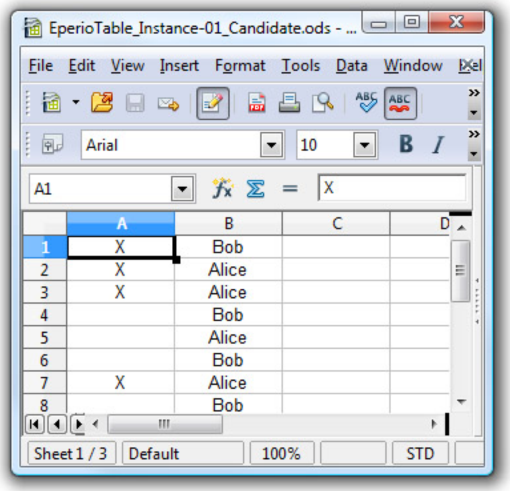
Verification in a spreadsheet!


EperioTable_Instance-01_BubbleID.ods - ...
File Edit View Insert Format Tools Data Window Exel
Arial
10
A1
004 B
Sheet 1 / 3
Default
100%
STD

	A	B	C	D
1	004 B	X		
2	008 B	X		
3	007 A	X		
4	002 A			
5	004 A			
6	008 A			
7	002 B	X		
8	007 B			

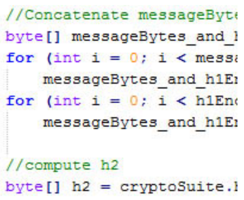
Bubble ID	Marked?	Candidate
004 B	X	Bob
008 B	X	Alice
007 A	X	Alice
002 A		Bob
004 A		Alice
008 A		Bob
002 B	X	Alice
007 B		Bob

Bubble ID	Marked?	Candidate
004 B	X	Bob
008 B	X	Alice
007 A	X	Alice
002 A		Bob
004 A		Alice
008 A		Bob
002 B	X	Alice
007 B		Bob


EperioTable_Instance-01_Candidate.ods - ...
File Edit View Insert Format Tools Data Window Exel
Arial
10
A1
X
Sheet 1 / 3
Default
100%
STD

	A	B	C	D
1	X	Bob		
2	X	Alice		
3	X	Alice		
4		Bob		
5		Alice		
6		Bob		
7	X	Alice		
8		Bob		

Implementation options

	Custom code 	Small script + Encryption utility python™ OpenSSL	Spreadsheet + Encryption utility OpenSSL	Spreadsheet all-in-one?
scantegrity	✓			
Punchscan	✓			
Helios	✓			
Prêt à Voter	✓			
Eperio	✓	✓	✓	✓

```
//Concatenate messageByt
byte[] messageBytes_and_
for (int i = 0; i < messa
    messageBytes_and_h1E
for (int i = 0; i < h1En
    messageBytes_and_h1E

//compute h2
byte[] h2 = cryptoSuite.
```

Eperio

Find out more at

eperio.org