Microsoft

Microsoft Research

Faculty Summit 2012

ADVANCING THE STATE OF THE ART

Verifiable Election Technologies

Josh Benaloh
Senior Cryptographer, Microsoft Research

July 16, 2012


WHERE IS MY VOTE?
WHERE IS MY VOTE?
WHERE IS MY VOTE?


WHERE
IS MY
VOTE?


OUR PRESIDENT
WHERE
IS MY
VOTE?
WHERE
IS MY
VOTE?


Where is
my VOTE
?!?


WHERE
IS
MY VOTE?


Where is my Vote ...?
موج سبز
رأی من کجاست؟
WHERE IS MY VOTE?


IRAN
ELECTION
NOT
SELECTION
WHERE IS MY
Where is My VOTE?


رأی من کجاست ؟
WHERE
IS MY
VOTE ?


WHERE
IS MY
VOTE?
WHERE
IS MY
VOTE?
Iranian Students in Hanno


WHERE
IS MY
VOTE?
WHERE
IS MY
VOTE?


WHERE
IS MY


WHERE
IS
MY VOTE


WHERE IS
MY VOTE?


WHERE
IS MY
VOTE?


?
WHERE
IS MY
VOTE?
Student Movement
for Democracy in Iran

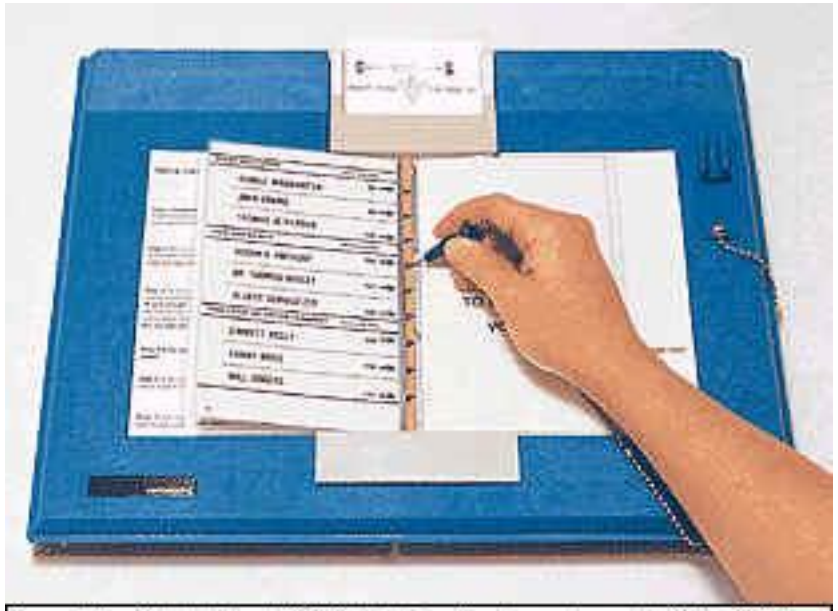
Traditional Voting Methods

Traditional Voting Methods

- Hand-Counted Paper

Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards



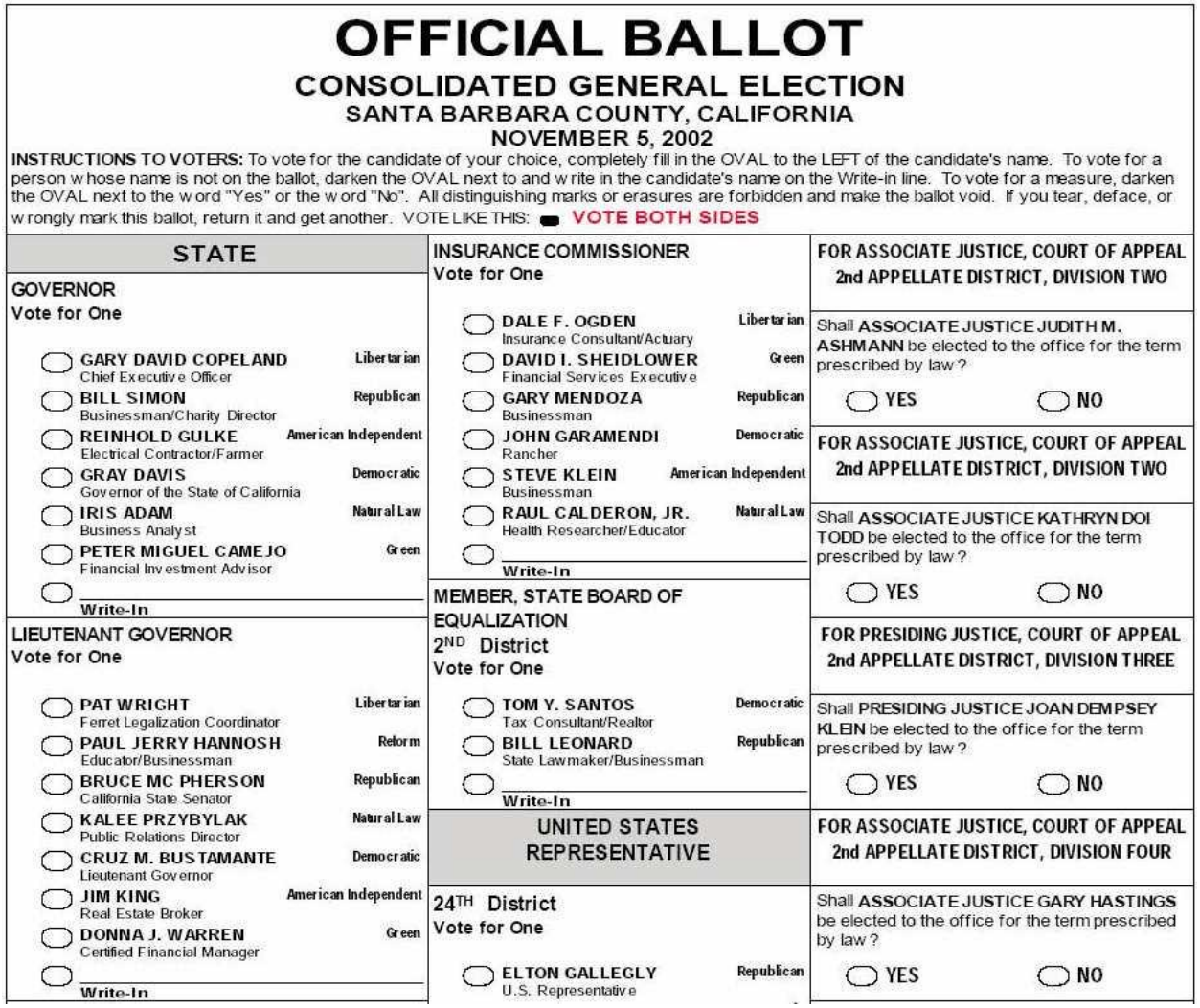
From The World Book (TM) Multimedia Encyclopedia (c) 1998 World Book, Inc., 525 W. Monroe, Chicago, IL 60661. All rights reserved. Larry Korb, Business Records Corporation

Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines

Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots



OFFICIAL BALLOT

CONSOLIDATED GENERAL ELECTION

SANTA BARBARA COUNTY, CALIFORNIA

NOVEMBER 5, 2002

INSTRUCTIONS TO VOTERS: To vote for the candidate of your choice, completely fill in the OVAL to the LEFT of the candidate's name. To vote for a person whose name is not on the ballot, darken the OVAL next to and write in the candidate's name on the Write-in line. To vote for a measure, darken the OVAL next to the word "Yes" or the word "No". All distinguishing marks or erasures are forbidden and make the ballot void. If you tear, deface, or wrongly mark this ballot, return it and get another. VOTE LIKE THIS: ▬ **VOTE BOTH SIDES**

STATE

GOVERNOR
Vote for One

- GARY DAVID COPELAND — Chief Executive Officer — Libertarian
- BILL SIMON — Businessman/Charity Director — Republican
- REINHOLD GULKE — Electrical Contractor/Farmer — American Independent
- GRAY DAVIS — Governor of the State of California — Democratic
- IRIS ADAM — Business Analyst — Natural Law
- PETER MIGUEL CAMEJO — Financial Investment Advisor — Green
- Write-In

LIEUTENANT GOVERNOR
Vote for One

- PAT WRIGHT — Ferret Legalization Coordinator — Libertarian
- PAUL JERRY HANNOSH — Educator/Businessman — Reform
- BRUCE MC PHERSON — California State Senator — Republican
- KALEE PRZYBYLAK — Public Relations Director — Natural Law
- CRUZ M. BUSTAMANTE — Lieutenant Governor — Democratic
- JIM KING — Real Estate Broker — American Independent
- DONNA J. WARREN — Certified Financial Manager — Green
- Write-In

INSURANCE COMMISSIONER
Vote for One

- DALE F. OGDEN — Insurance Consultant/Actuary — Libertarian
- DAVID I. SHEIDLOWER — Financial Services Executive — Green
- GARY MENDOZA — Businessman — Republican
- JOHN GARAMENDI — Rancher — Democratic
- STEVE KLEIN — Businessman — American Independent
- RAUL CALDERON, JR. — Health Researcher/Educator — Natural Law
- Write-In

MEMBER, STATE BOARD OF EQUALIZATION
2ND District
Vote for One

- TOM Y. SANTOS — Tax Consultant/Realtor — Democratic
- BILL LEONARD — State Lawmaker/Businessman — Republican
- Write-In

UNITED STATES REPRESENTATIVE

24TH District
Vote for One

- ELTON GALLEGLY — U.S. Representative — Republican

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE JUDITH M. ASHMANN be elected to the office for the term prescribed by law?
YES NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE KATHRYN DOI TODD be elected to the office for the term prescribed by law?
YES NO

FOR PRESIDING JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION THREE

Shall PRESIDING JUSTICE JOAN DEMPSEY KLEIN be elected to the office for the term prescribed by law?
YES NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION FOUR

Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law?
YES NO

Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines

Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
- Touch-Screen Terminals

Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
- Touch-Screen Terminals
- Various Hybrids

Vulnerabilities and Trust

All of these systems have substantial vulnerabilities.

All of these systems require trust in the honesty and expertise of election officials (and usually the equipment vendors as well).

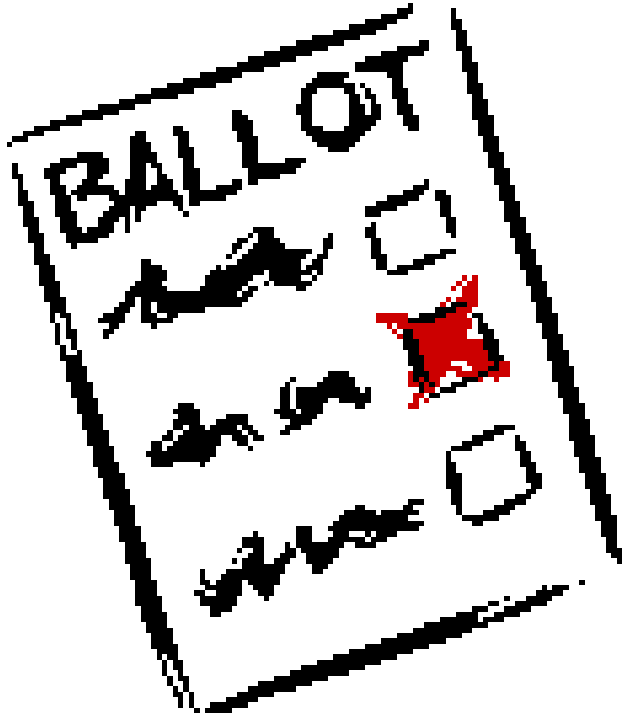
Can we do better?

The Voter's Perspective

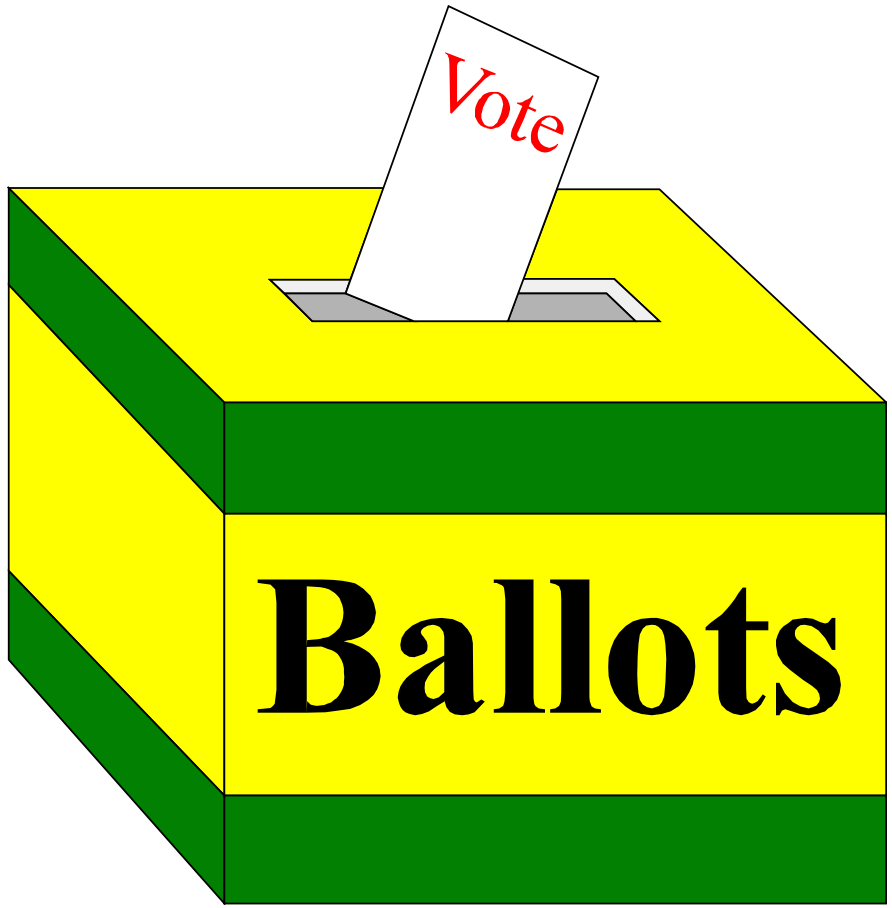
The Voter's Perspective

The Voter's Perspective

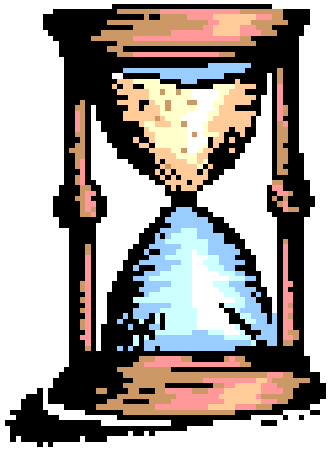
The Voter's Perspective



The Voter's Perspective



The Voter's Perspective



The Voter's Perspective

The Voter's Perspective

The Voter's Perspective

- As a voter, you don't really know what happens behind the curtain.
- You have no choice but to trust the people working behind the curtain.
- You don't even get to choose the people who you will have to trust.

Fully-Verifiable Election Technologies

(aka End-to-End Verifiable)

Allow voters to track their individual (sealed) votes and ensure that they are properly counted…

… even in the presence of faulty or malicious election equipment …

… and/or careless or dishonest election personnel.

Voters can check …

… that their (sealed) votes have been properly recorded

… and that *all* recorded votes have been properly counted

This is *not* just checking a claim that the right steps have been taken …

This is actually a check that the counting is correct.

Where is *My* Vote?

Where is *My* Vote?

Alice Johnson, 123 Main – **YES**

Bob Ramirez, 79 Oak – **NO**

Carol Wilson, 821 Market – **NO**

End-to-End Voter-Verifiability

As a voter, I can be sure that

- My vote is
  - **Cast as intended**
  - **Counted as cast**
- All votes are counted as cast

… without having to trust *anyone* or *anything.*

But wait …

This isn't a *secret-ballot* election.

Quite true, but it's enough to show that voter-verifiability is possible

… and also to falsify arguments that electronic elections are inherently untrustworthy.

Privacy

The only ingredient missing from this *transparent* election is privacy – and the things which flow from privacy (e.g. protection from coercion).

Performing tasks while preserving privacy is the bailiwick of cryptography.

Cryptographic techniques can enable *fully-verifiable* elections while preserving voter privacy.

Where is *My* Vote?

Alice Johnson, 123 Main –

Bob Ramirez, 79 Oak –

Carol Wilson, 821 Market –

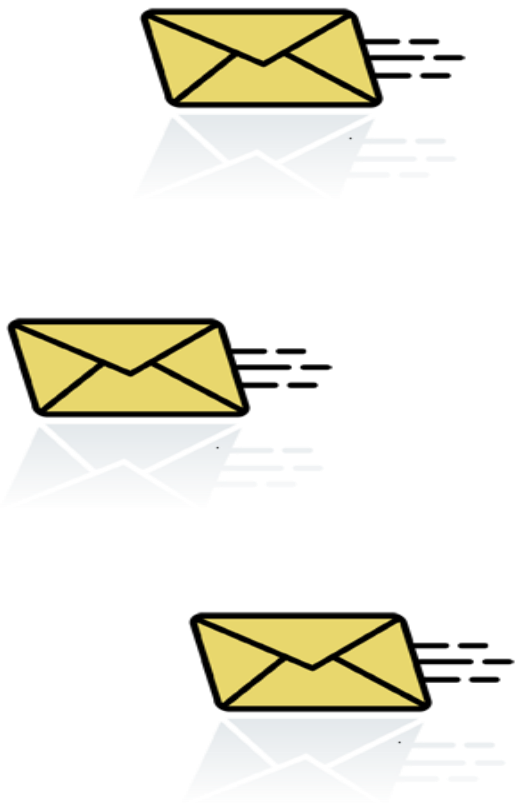
Where is *My* Vote?

Alice Johnson, 123 Main –

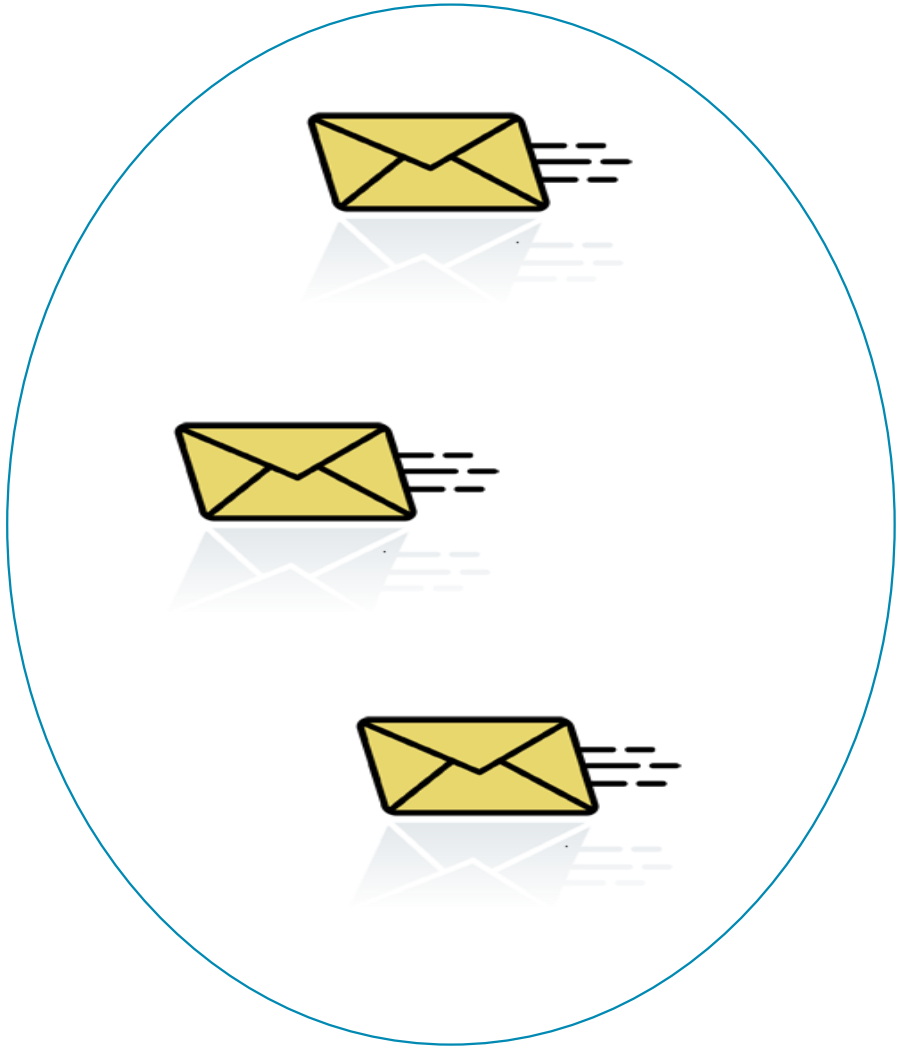
Bob Ramirez, 79 Oak –

Carol Wilson, 821 Market –

Where is *My* Vote?



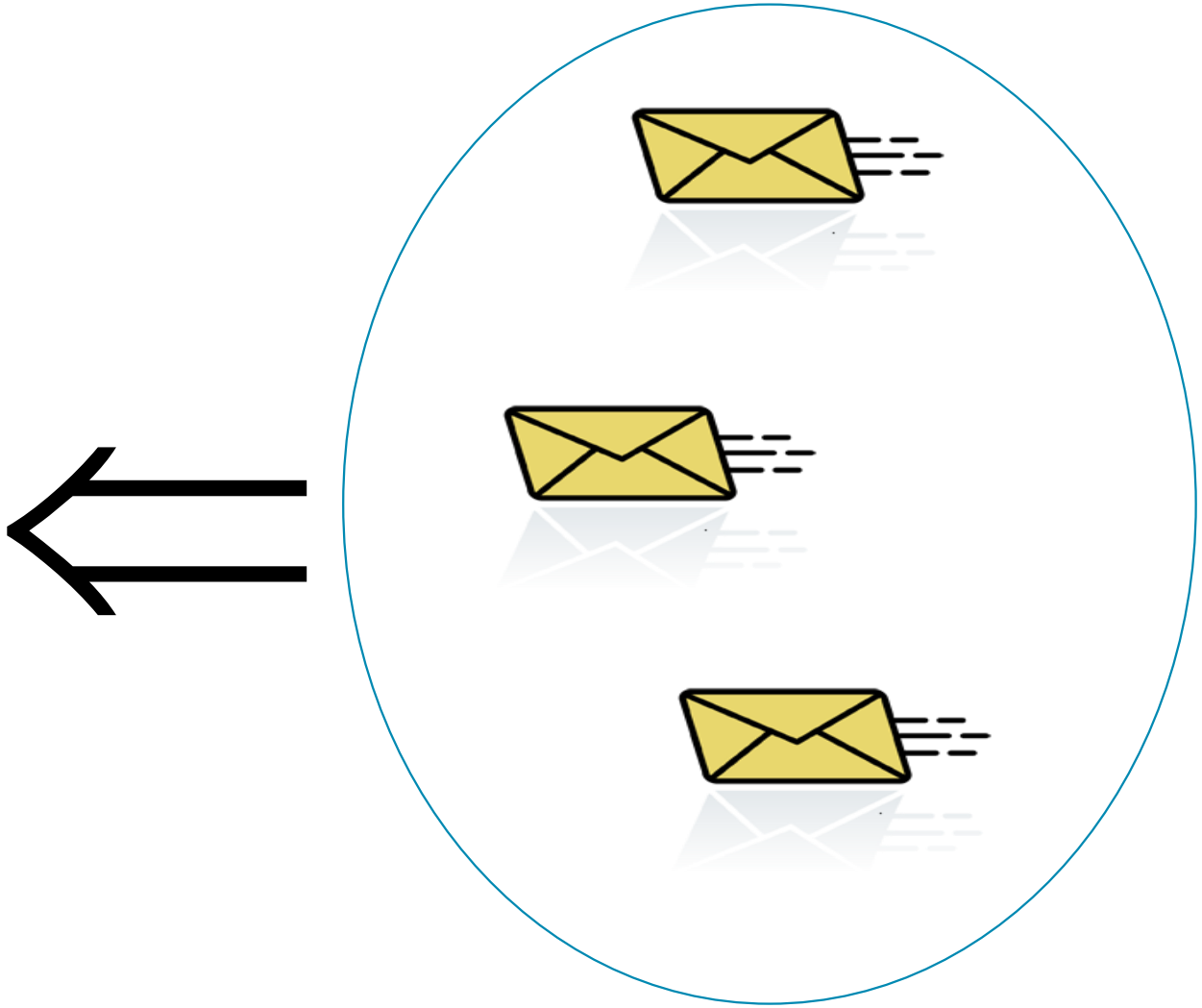
Where is *My* Vote?



Where is *My* Vote?

No – 2

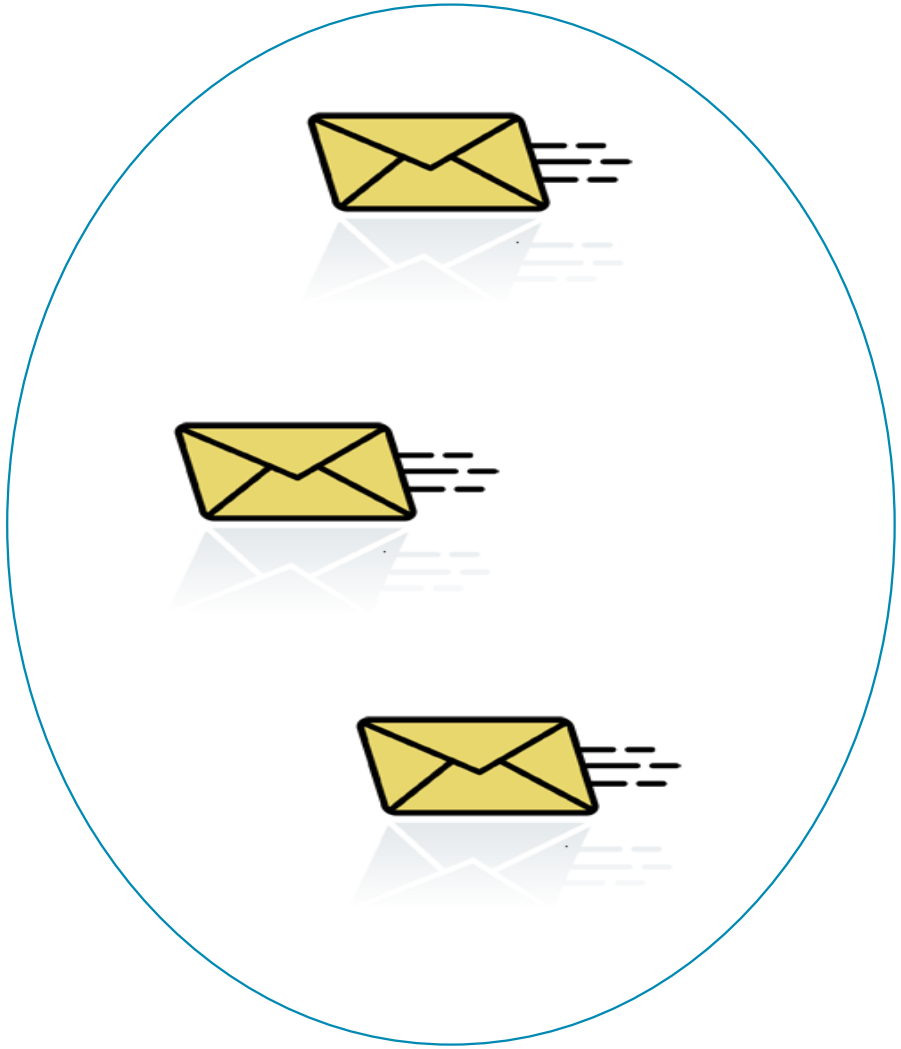
Yes – 1



Where is *My* Vote?

No – 2

Yes – 1



Mathematical Proof

End-to-End Voter-Verifiability

As a voter, I can be sure that

- My vote is
  - **Cast as intended**
  - **Counted as cast**
- All votes are counted as cast

… without having to trust *anyone* or *anything.*

The Voter's Perspective

Verifiable election systems can be built to look exactly like current systems …

… with one addition …

A Verifiable Receipt

Precinct 37 – Machine 4
Nov. 6, 2012 1:39PM

Vote receipt tag:

7A34ZR9K4BX

VOTE CONFIRMED

The Voter's Perspective

Voters can …

- Use their receipts to check that their results are properly recorded on a public web site.
- Throw their receipts in the trash.

- Verify the accuracy of the election with apps they wrote themselves.
- Download apps from sources of their choice to verify the election.
- Believe verifications done by their political parties, LWV, ACLU, etc.
- Accept the results without question.

End-to-End Verifiable Elections

Anyone who cares to do so can

- Check that their own *encrypted* votes are correctly listed
- Check that other voters are legitimate
- Check the cryptographic proof of the correctness of the announced tally

Is it *Really* This Easy?

Yes …

… but there are lots of details to get right.

End-to-End Verifiable Elections

Two questions must be answered …

- How do voters turn their preferences into encrypted votes?
- How are voters convinced that the published set of encrypted votes corresponds to the announced tally?

Tallying

Many tools are available …

… including “homomorphic encryption”:

A is an encryption of a

B is an encryption of b

$A \otimes B$ is an encryption of $a \oplus b$

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1
	$\Sigma =$

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1
	Σ =
	2

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1
	$\otimes =$
	2

Homomorphic Tallying

Alice	0
Bob	0
Carol	1
David	0
Eve	1
	$\otimes =$
	2

Ballot Encryption

Most pre-2000 verifiable election protocols:

Step 1

Encrypt your vote.

How?

How do Humans Encrypt?

If voters encrypt their votes with devices of their own choosing, they are subject to coercion and compromise.

If voters encrypt their votes on “official” devices, how can they trust that their intentions have been properly captured?

The Human Encryptor

We need to find ways to engage humans in an *interactive proof* process to ensure that their intentions are accurately reflected in encrypted ballots cast on their behalf.

MarkPledge Ballot

Alice	367	248	792	141	390	863	427	015
Bob	629	523	916	504	129	077	476	947
Carol	285	668	049	732	859	308	156	422
David	863	863	863	863	863	863	863	863
Eve	264	717	740	317	832	399	441	946

MarkPledge Ballot

Alice	367	248	792	141	390	863	427	015
Bob	629	523	916	504	129	077	476	947
Carol	285	668	049	732	859	308	156	422
David	863	863	863	863	863	863	863	863
Eve	264	717	740	317	832	399	441	946

MarkPledge Ballot

Alice	367	248	792	141	390	863	427	015
Bob	629	523	916	504	129	077	476	947
Carol	285	668	049	732	859	308	156	422
David	863	863	863	863	863	863	863	863
Eve	264	717	740	317	832	399	441	946

Device commitment to voter: "You're candidate's number is 863."

MarkPledge Ballot

Alice	367	248	792	141	390	863	427	015
Bob	629	523	916	504	129	077	476	947
Carol	285	668	049	732	859	308	156	422
David	863	863	863	863	863	863	863	863
Eve	264	717	740	317	832	399	441	946

Device commitment to voter: "You're candidate's number is 863."

Voter challenge: "Decrypt column number 5."

MarkPledge Ballot

Alice	367	248	792	141	390	863	427	015
Bob	629	523	916	504	129	077	476	947
Carol	285	668	049	732	859	308	156	422
David	863	863	863	863	863	863	863	863
Eve	264	717	740	317	832	399	441	946

Device commitment to voter: "You're candidate's number is 863."

Voter challenge: "Decrypt column number 5."

MarkPledge Ballot

Alice	367	248	792	141	390	863	427	015
Bob	629	523	916	504	129	077	476	947
Carol	285	668	049	732	859	308	156	422
David	863	863	863	863	863	863	863	863
Eve	264	717	740	317	832	399	441	946

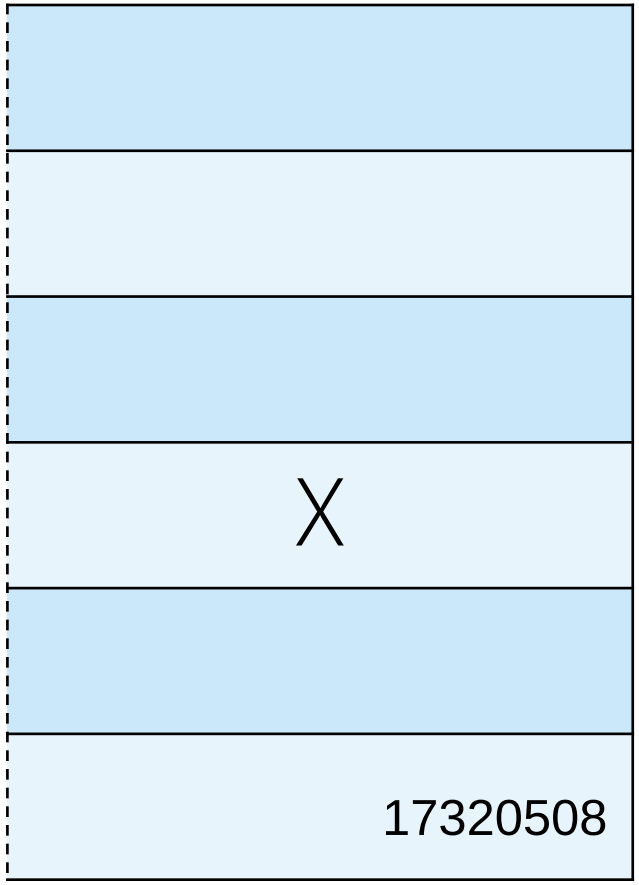
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	
David	
	17320508

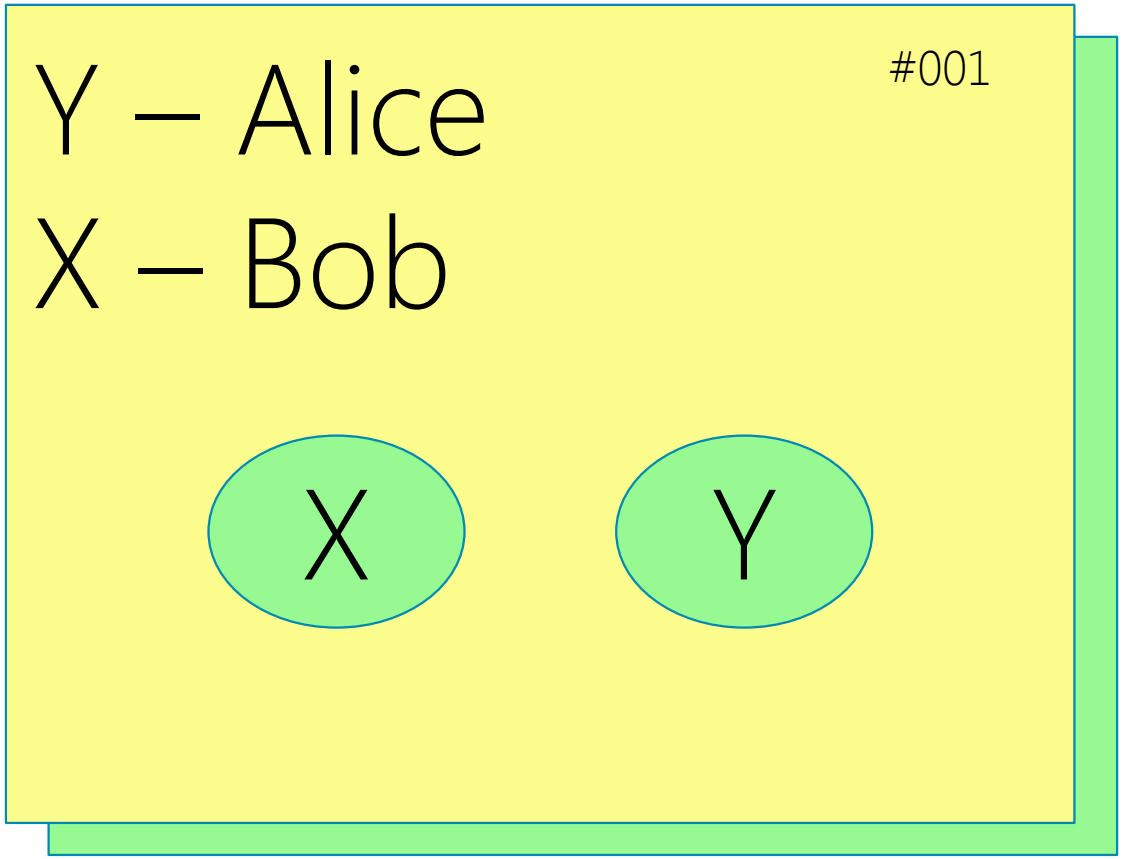
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	X
David	
	17320508

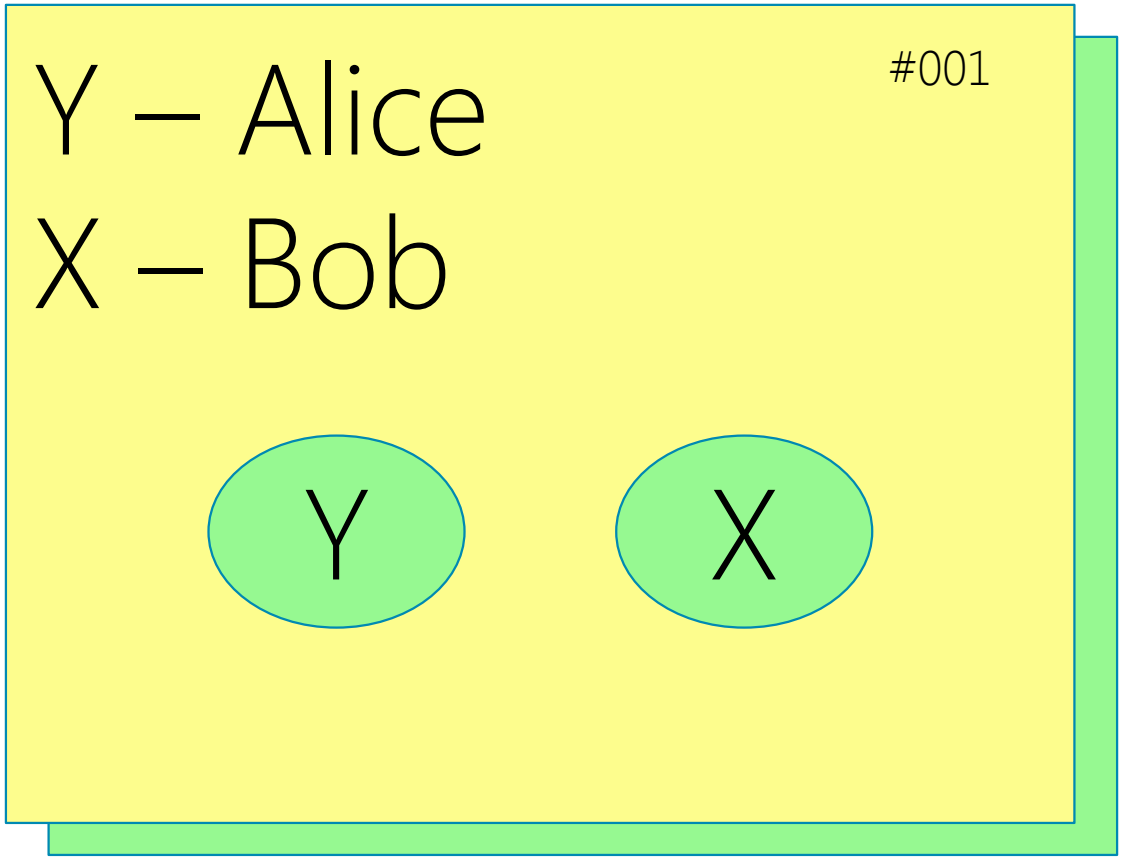
Prêt à Voter Ballot



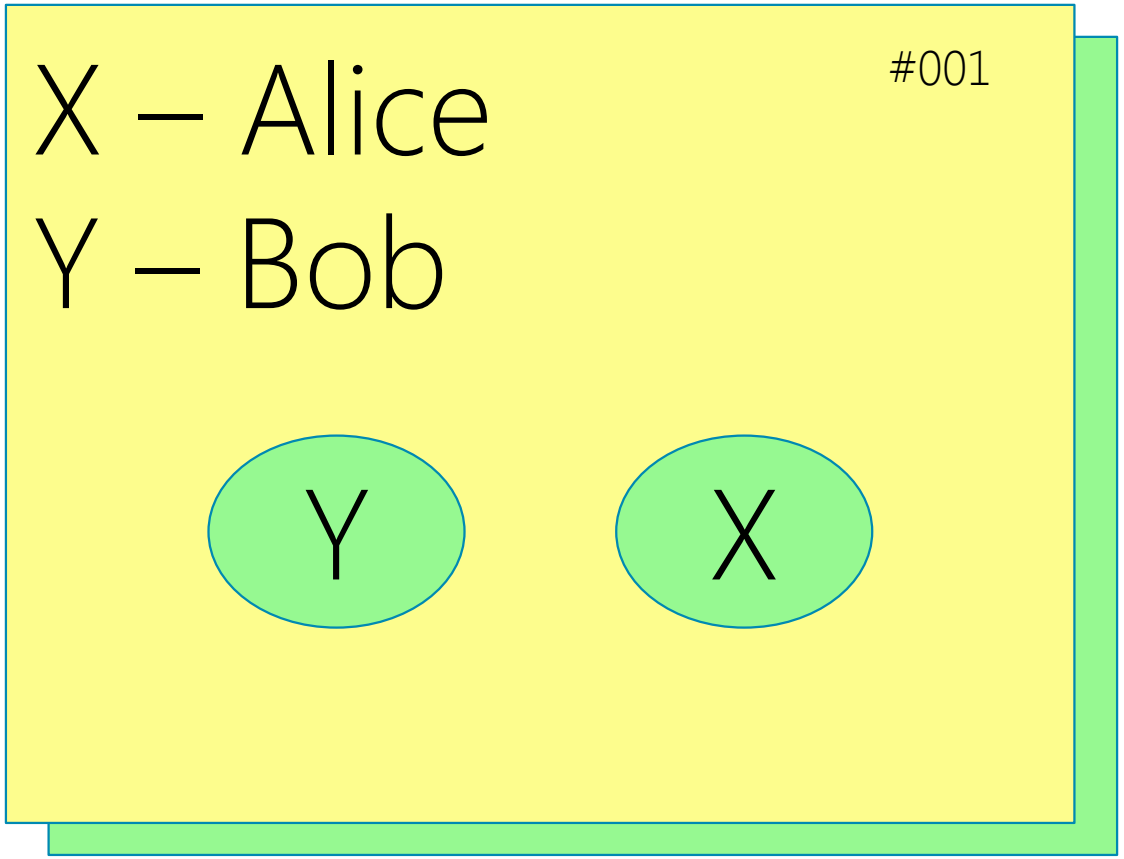
PunchScan Ballot



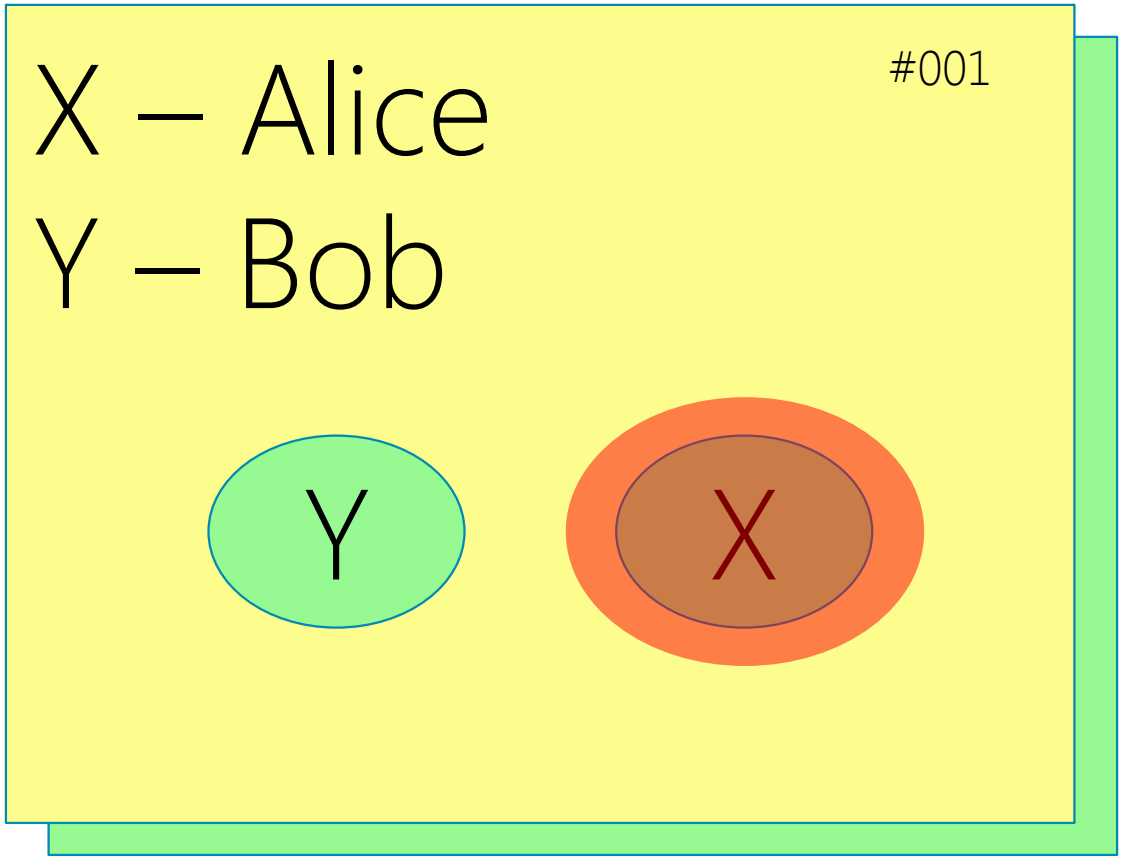
PunchScan Ballot



PunchScan Ballot



PunchScan Ballot

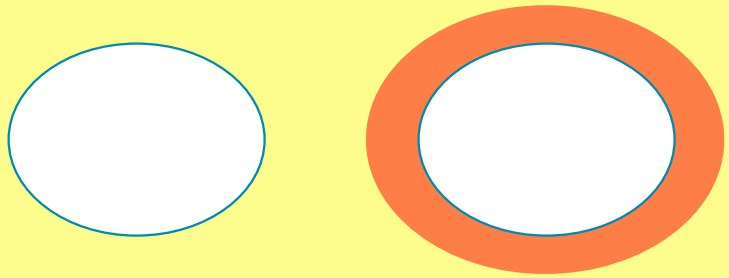


PunchScan Ballot

X – Alice

Y – Bob

#001

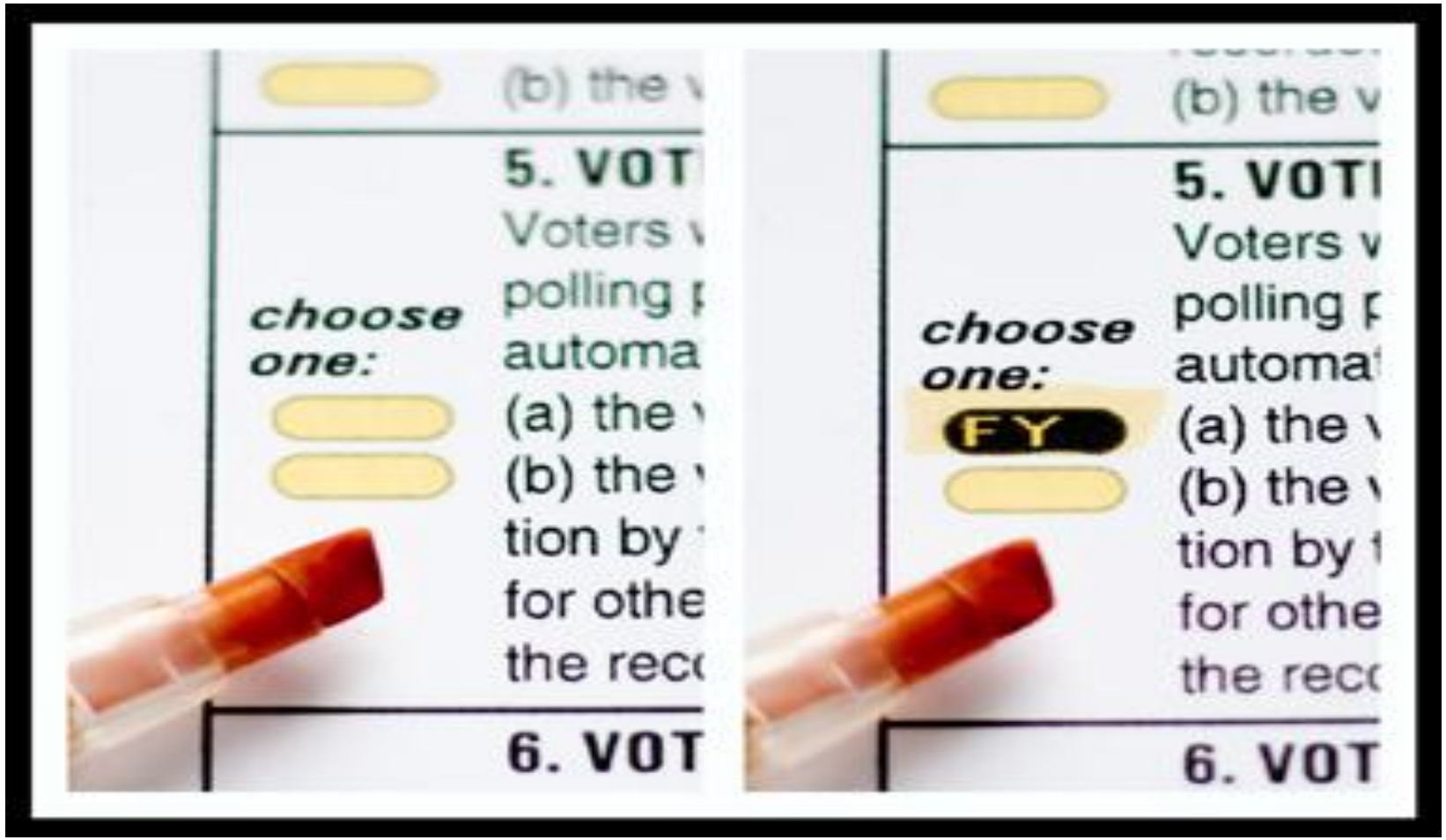


#001

Y

X

Scantegrity



Voter-Initiated Auditing

Voter can use “any” device to make selections (touch-screen DRE, OpScan, etc.)

After selections are made, voter receives an encrypted receipt of the ballot.

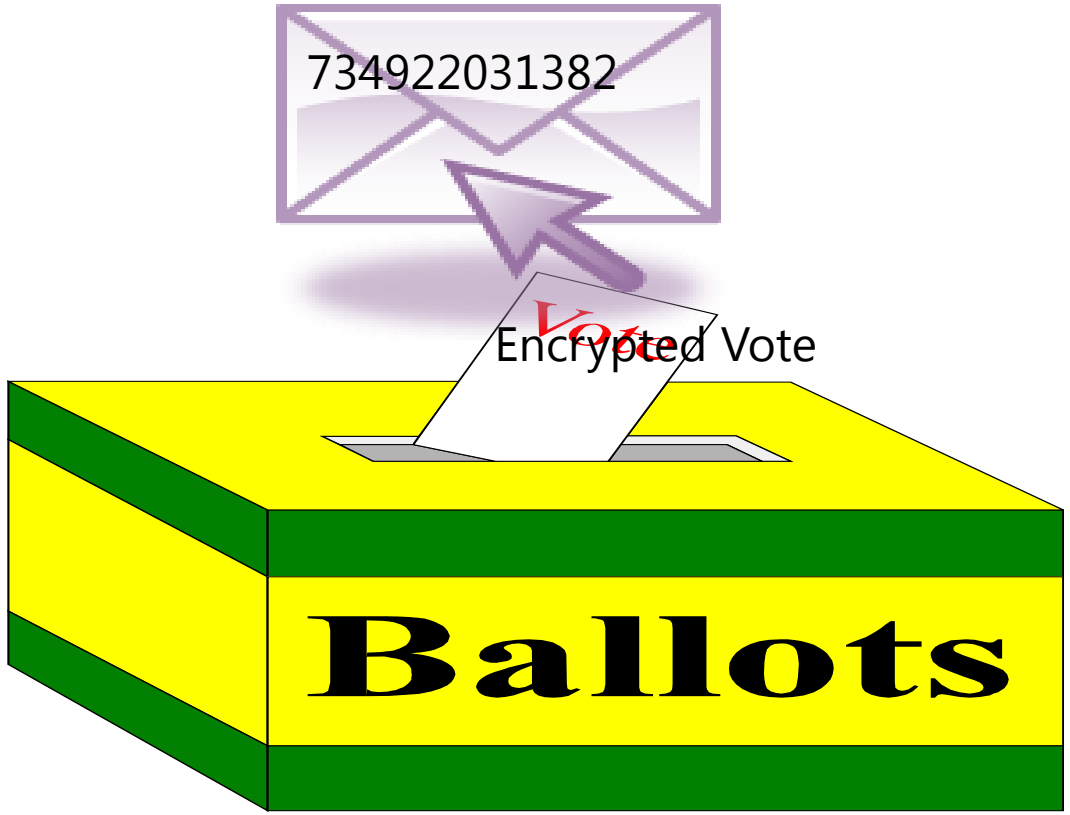
Voter-Initiated Auditing

Encrypted Vote

Voter choice: Cast or Challenge

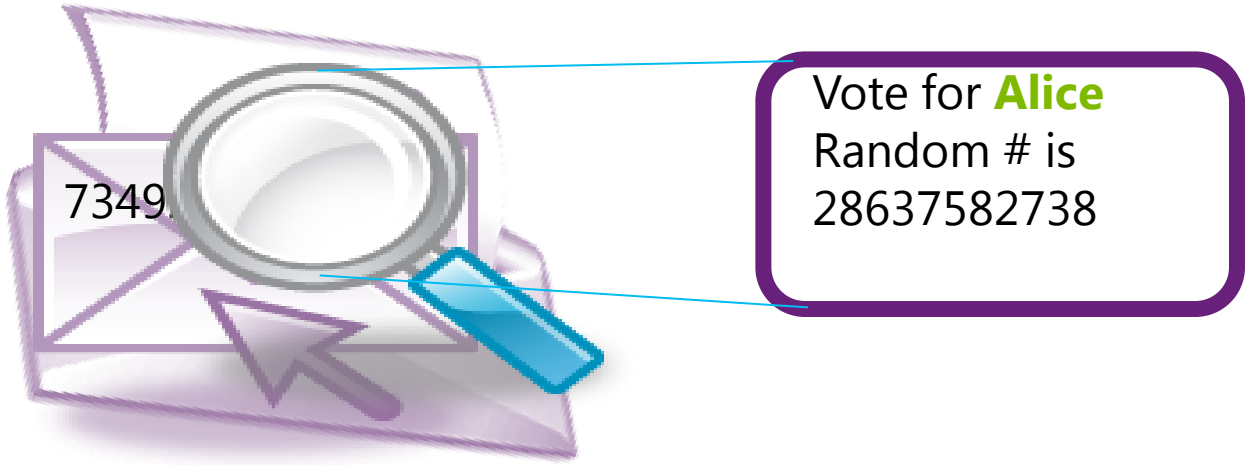
Voter-Initiated Auditing

Cast



Voter-Initiated Auditing

Challenge



Real-World Deployments

Helios (www.heliosvoting.org) – Ben Adida and others

- Remote electronic voting system using voter-initiated auditing and homomorphic backend.
- Used to elect president of UC Louvain, Belgium.
- Used in Princeton University student government.
- Used to elect IACR Board of Directors.

Scantegrity II (www.scantegrity.org) – David Chaum, Ron Rivest, many others.

- Optical scan system with codes revealed by invisible ink markers and "plugboard-mixnet" backend.
- Used for municipal elections in Takoma Park, MD.

Research Opportunities

Front End

There is great value in continuing work on the user-facing front end.

The front end should be

- Simpler to use
- Simpler to understand
- Higher assurance

Research Opportunties

Back End

Simple counting methods are well-understood with effective techniques.

More complex counting methods create substantial challenges –

- Maintaining strong privacy
- Keeping computations efficient

Microsoft

Election Technologies – Today and Tomorrow

Lillie Coney,
Electronic Privacy Information Center
J. Alex Halderman,
Univeristy of Michigan
Josh Benaloh,
Microsoft Research

July 16, 2012