Verifiable Election Technologies

How Elections *Should* Be Run

Josh Benaloh
Senior Cryptographer
Microsoft Research


WHERE
IS MY
VOTE?
Where is my
WHERE IS
MY VOTE?
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?


رای من کو؟
WHERE IS MY VOTE?


ELECTION
NOT
SELECTION
WHERE
IS MY
Vhere is My VOTE?


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


رأی من کجاست ؟
WHERE
IS MY
VOTE ?


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


WHERE
IS MY


WHERE
IS MY
VOTE?
WHERE
IS MY
VOTE?


WHERE
IS
MY VOTE


WHERE IS
MY VOTE?

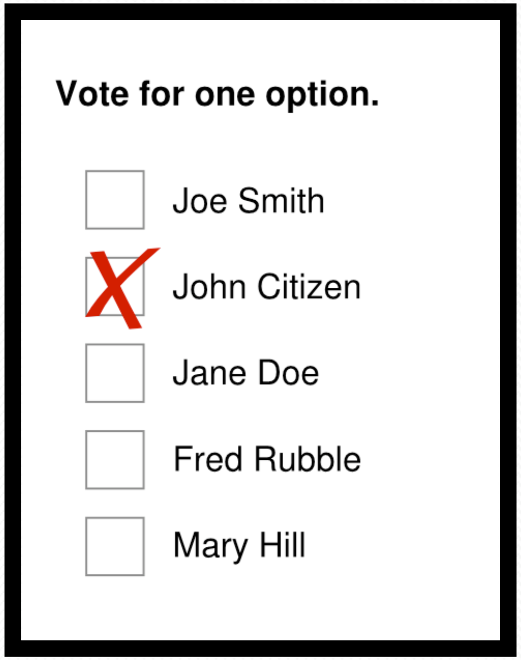

WHERE
IS MY
VOTE?


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

Traditional Voting Methods

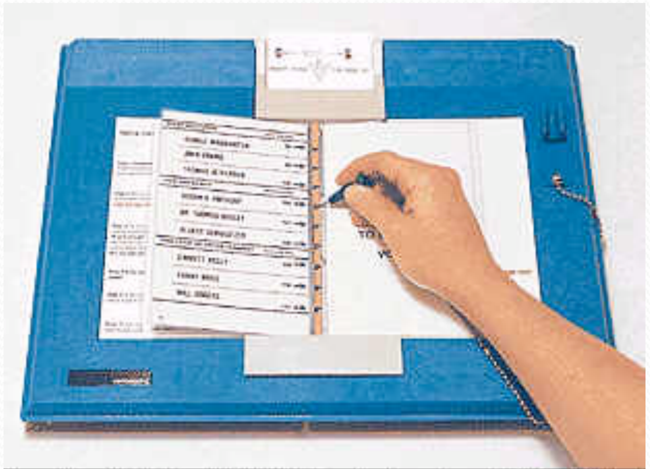
Traditional Voting Methods

- Hand-Counted Paper



Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards



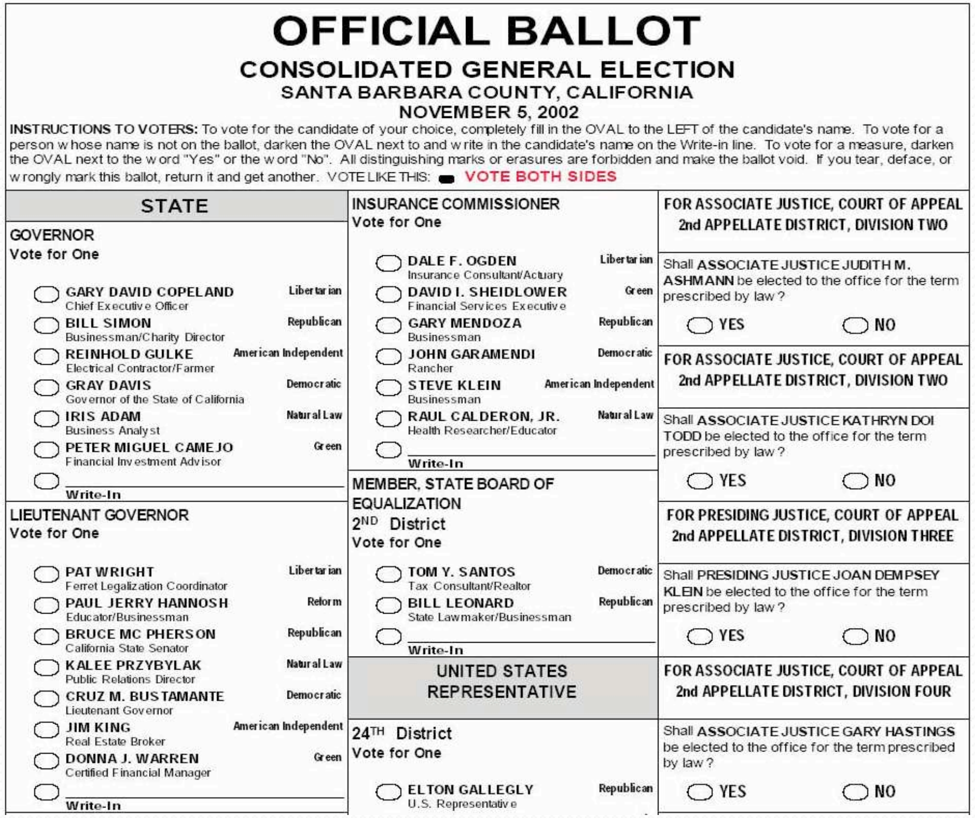
From The World Book (TM) Multimedia Encyclopedia (c) 1998 World Book, Inc., 525 W. Monroe, Chicago, IL 60661. All rights reserved. Larry Korb, Business Records Corporation

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

LIEUTENANT GOVERNOR
Vote for One

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

INSURANCE COMMISSIONER
Vote for One

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

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

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

UNITED STATES REPRESENTATIVE

24^{TH} District
Vote for One

ELTON GALLEGLY — Republican
U.S. Representative

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).

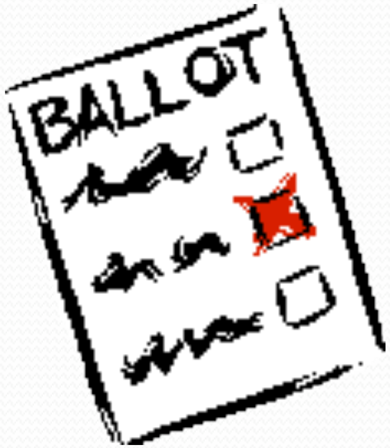
Can we do better?

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 (End-to-End Verifiable)

Allows 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 *end-to-end verifiable* elections while preserving voter privacy.

Where is *My* Vote?

Alice Johnson, 123 Main ... es

Bob Ramirez, 79 Oak ...

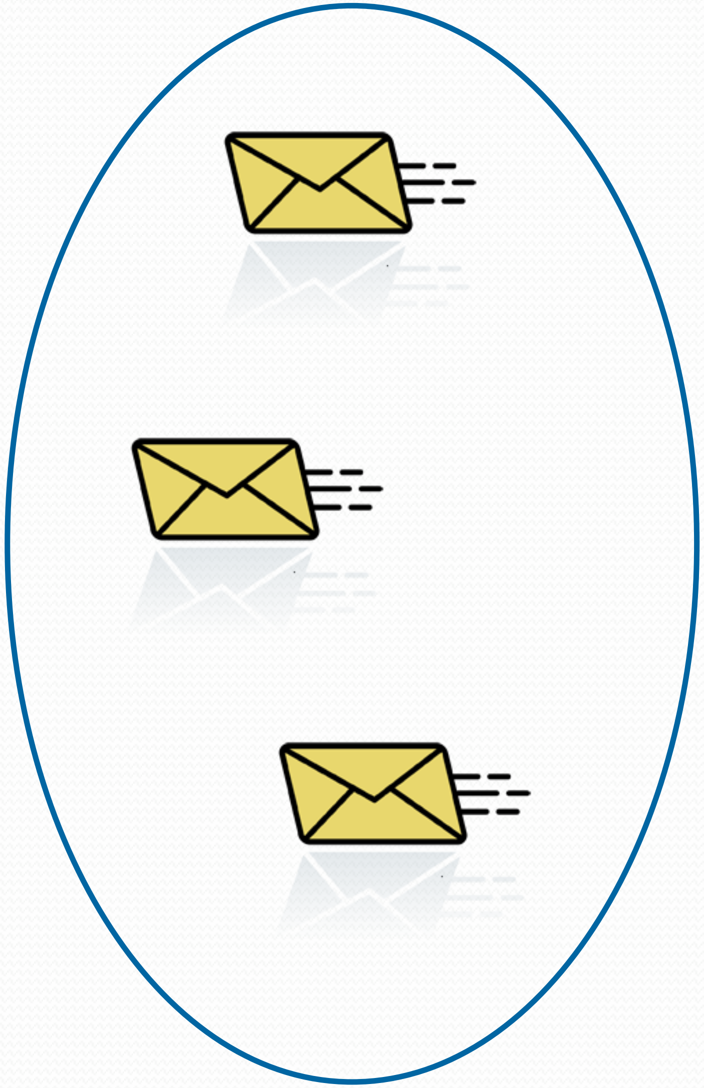
Carol Wilson, 821 Market ...

Where is *My* Vote?

- Alice Johnson, 123 Main
- Bob Ramirez, 79 Oak
- Carol Wilson, 821 Market

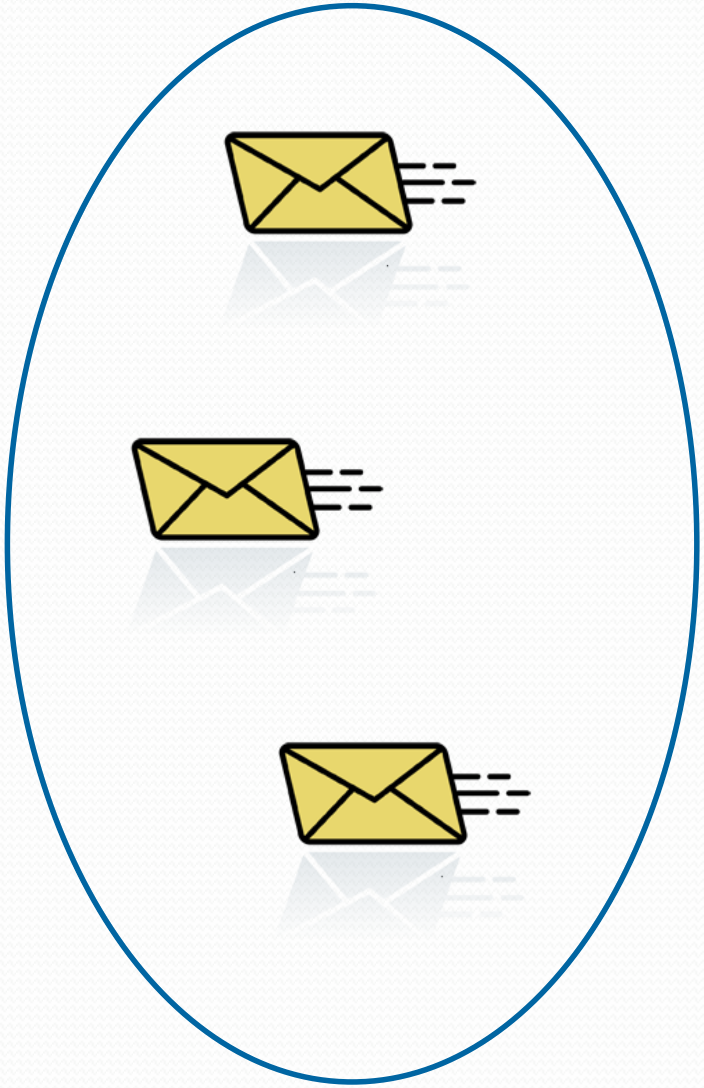
Where is *My* Vote?

Where is *My* Vote?



Where is *My* Vote?

No – 2
Yes – 1 $\Longleftarrow$



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.*

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

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 the announced tally?

Is it *Really* This Easy?

Yes …

… but there are lots of details to get right.

Some Important Details

- How is the ballot encryption and decryption done?
- How is the cryptographic proof of the tally done?

Secure MPC is *not* Enough

- Secure Multi-Party Computation allows *any* public function to be computed on any number of private inputs *without* compromising the privacy of the inputs.

- But secure MPC does not prevent parties from revealing their private inputs if they so choose.

End-to-End Verifiable Elections

Two principle phases …

1. Voters publish their names and *encrypted* votes.

2. At the end of the election, administrators compute and publish the tally together with a cryptographic proof that the tally “matches” the set of encrypted votes.

Fundamental Tallying Decision

There are essentially two paradigms to choose from …

- Anonymized Ballots
  (Mix Networks)
- Ballotless Tallying
  (Homomorphic Encryption)

Anonymized Ballots

Ballotless Tallying

Pros and Cons of Ballots

- Ballots simplify write-ins.
- Ballots make it harder to enforce privacy – especially in complex counting scenarios.

Homomorphic Encryption

We can construct a public-key encryption function E such that if

A is *an* encryption of a and

B is *an* encryption of b then

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

Homomorphic Encryption

Some Homomorphic Functions

- RSA: $E(m) = m^e \bmod n$
- ElGamal: $E(m,r) = (g^r, mh^r) \bmod p$
- GM: $E(b,r) = r^2 g^b \bmod n$
- Benaloh: $E(m,r) = r^e g^m \bmod n$
- Pallier: $E(m,r) = r^n g^m \bmod n^2$

Homomorphic Elections

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Homomorphic Elections

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

Homomorphic Elections

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

Homomorphic Elections

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Homomorphic Elections

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Homomorphic Elections

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

Homomorphic Elections

Alice	0
Bob	0
Carol	1
David	0
Eve	1

$\otimes =$

	2

Homomorphic Elections

Alice	0
Bob	0
Carol	1
David	0
Eve	1

$\otimes =$

2

Multiple Authorities

Alice	0
Bob	0
Carol	1
David	0
Eve	1

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$= \Sigma$	3	-5	2
Bob	0	$= \Sigma$	-4	5	-1
Carol	1	$= \Sigma$	2	-3	2
David	0	$= \Sigma$	-2	-1	3
Eve	1	$= \Sigma$	4	-1	-2

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$= \Sigma$	3	-5	2
Bob	0	$= \Sigma$	-4	5	-1
Carol	1	$= \Sigma$	2	-3	2
David	0	$= \Sigma$	-2	-1	3
Eve	1	$= \Sigma$	4	-1	-2
			$\Sigma =$	$\Sigma =$	$\Sigma =$

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$= \Sigma$	3	-5	2
Bob	0	$= \Sigma$	-4	5	-1
Carol	1	$= \Sigma$	2	-3	2
David	0	$= \Sigma$	-2	-1	3
Eve	1	$= \Sigma$	4	-1	-2
			$\Sigma =$	$\Sigma =$	$\Sigma =$
			3	-5	4

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$=\Sigma$	3	-5	2
Bob	0	$=\Sigma$	-4	5	-1
Carol	1	$=\Sigma$	2	-3	2
David	0	$=\Sigma$	-2	-1	3
Eve	1	$=\Sigma$	4	-1	-2
			$\Sigma=$	$\Sigma=$	$\Sigma=$
		$=\Sigma$	3	-5	4

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$=\Sigma$	3	-5	2
Bob	0	$=\Sigma$	-4	5	-1
Carol	1	$=\Sigma$	2	-3	2
David	0	$=\Sigma$	-2	-1	3
Eve	1	$=\Sigma$	4	-1	-2
			$\Sigma =$	$\Sigma =$	$\Sigma =$
	2	$=\Sigma$	3	-5	4

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$= \Sigma$	3	-5	2
Bob	0	$= \Sigma$	-4	5	-1
Carol	1	$= \Sigma$	2	-3	2
David	0	$= \Sigma$	-2	-1	3
Eve	1	$= \Sigma$	4	-1	-2
	$\Sigma =$		$\Sigma =$	$\Sigma =$	$\Sigma =$
	2	$= \Sigma$	3	-5	4

Multiple Authorities

The *sum* of the *shares* of the votes constitute *shares* of the *sum* of the votes.

Multiple Authorities

			X_1	X_2	X_3
Alice	0	$= \Sigma$	3	-5	2
Bob	0	$= \Sigma$	-4	5	-1
Carol	1	$= \Sigma$	2	-3	2
David	0	$= \Sigma$	-2	-1	3
Eve	1	$= \Sigma$	4	-1	-2
	$\Sigma =$		$\Sigma =$	$\Sigma =$	$\Sigma =$
	2	$= \Sigma$	3	-5	4

Multiple Authorities

			X_1	X_2	X_3
Alice	0		3	-5	2
Bob	0		-4	5	-1
Carol	1		2	-3	2
David	0		-2	-1	3
Eve	1		4	-1	-2

Multiple Authorities

			X_1	X_2	X_3
Alice	0		3	-5	2
Bob	0		-4	5	-1
Carol	1		2	-3	2
David	0		-2	-1	3
Eve	1		4	-1	-2
			$\otimes =$	$\otimes =$	$\otimes =$

Multiple Authorities

			X_1	X_2	X_3
Alice	0		3	-5	2
Bob	0		-4	5	-1
Carol	1		2	-3	2
David	0		-2	-1	3
Eve	1		4	-1	-2
			$\otimes =$	$\otimes =$	$\otimes =$
			3	-5	4

Multiple Authorities

			X_1	X_2	X_3
Alice	0		3	-5	2
Bob	0		-4	5	-1
Carol	1		2	-3	2
David	0		-2	-1	3
Eve	1		4	-1	-2
			$\otimes =$	$\otimes =$	$\otimes =$
			3	-5	4

Multiple Authorities

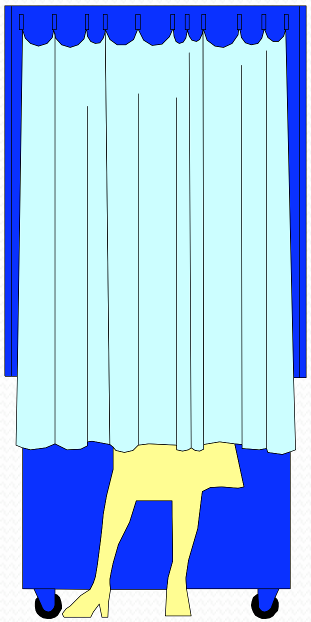
			X_1	X_2	X_3
Alice	0		3	-5	2
Bob	0		-4	5	-1
Carol	1		2	-3	2
David	0		-2	-1	3
Eve	1		4	-1	-2
			$\otimes =$	$\otimes =$	$\otimes =$
		$= \Sigma$	3	-5	4

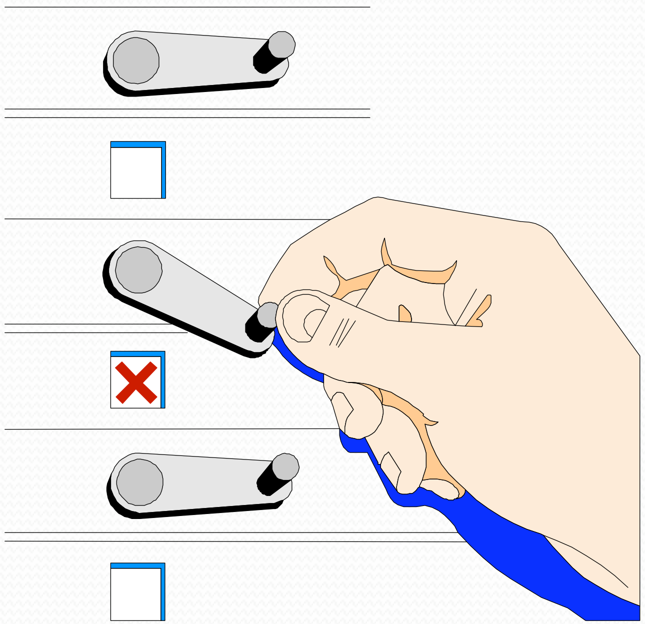
Multiple Authorities

			X_1	X_2	X_3
Alice	0		3	-5	2
Bob	0		-4	5	-1
Carol	1		2	-3	2
David	0		-2	-1	3
Eve	1		4	-1	-2
			$\otimes =$	$\otimes =$	$\otimes =$
	2	$= \Sigma$	3	-5	4

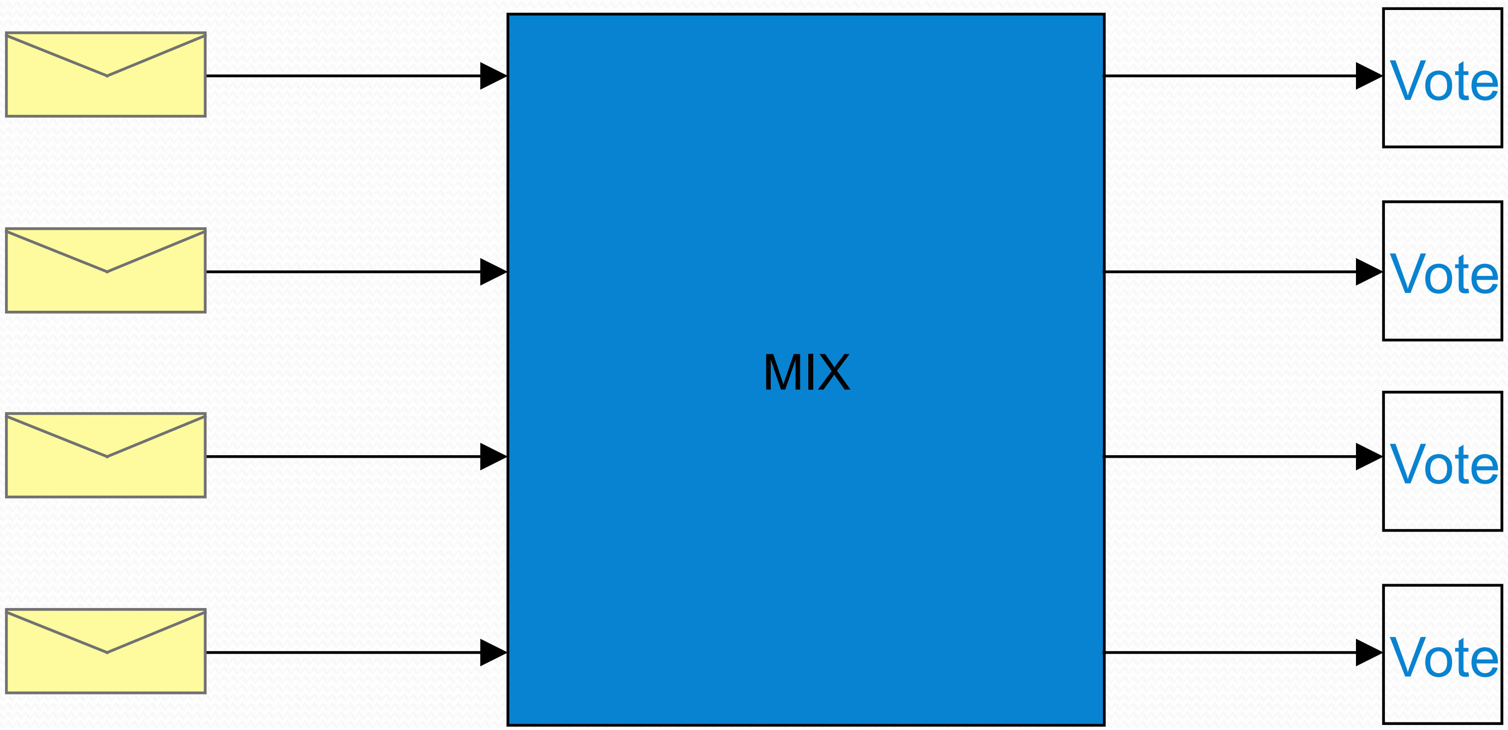
Mix-Based Elections

Homomorphic Tallying

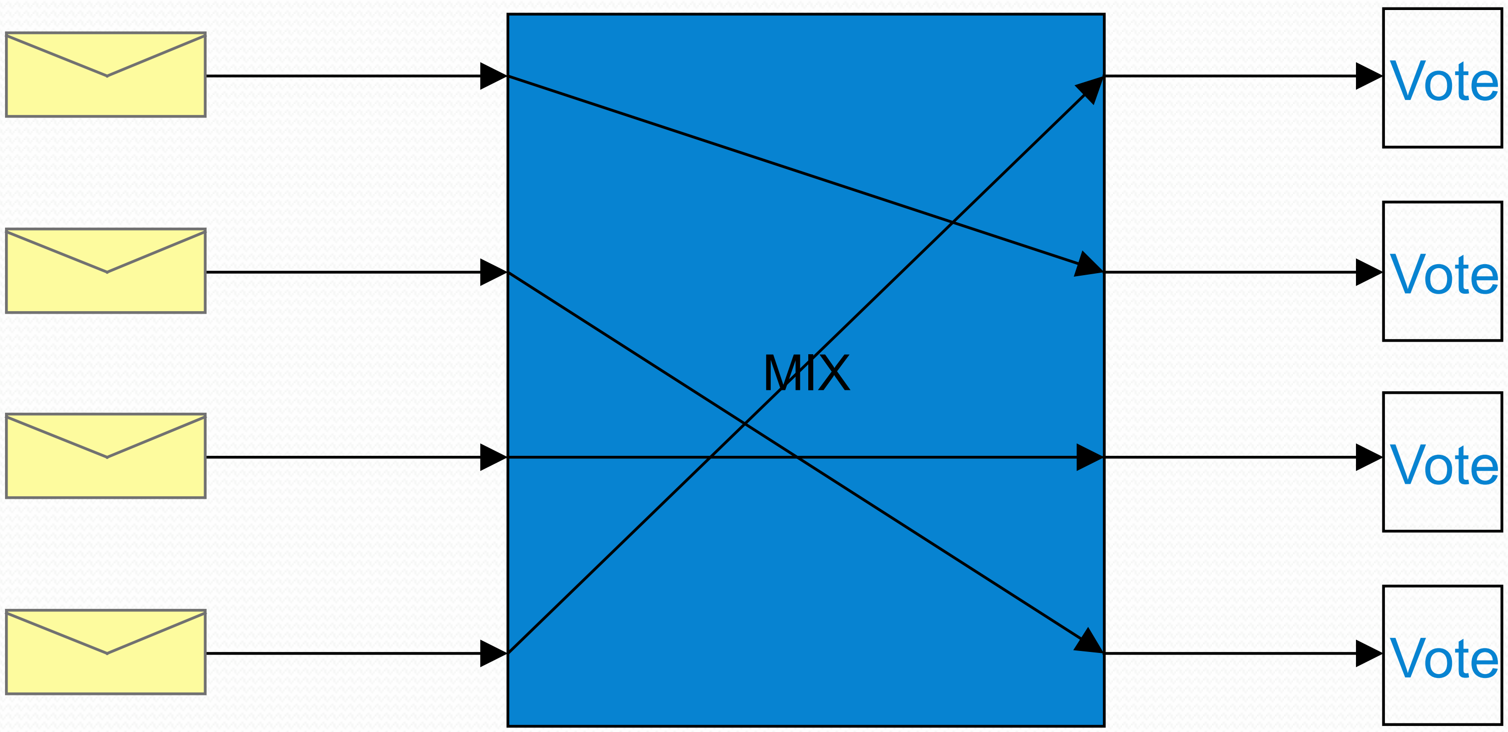




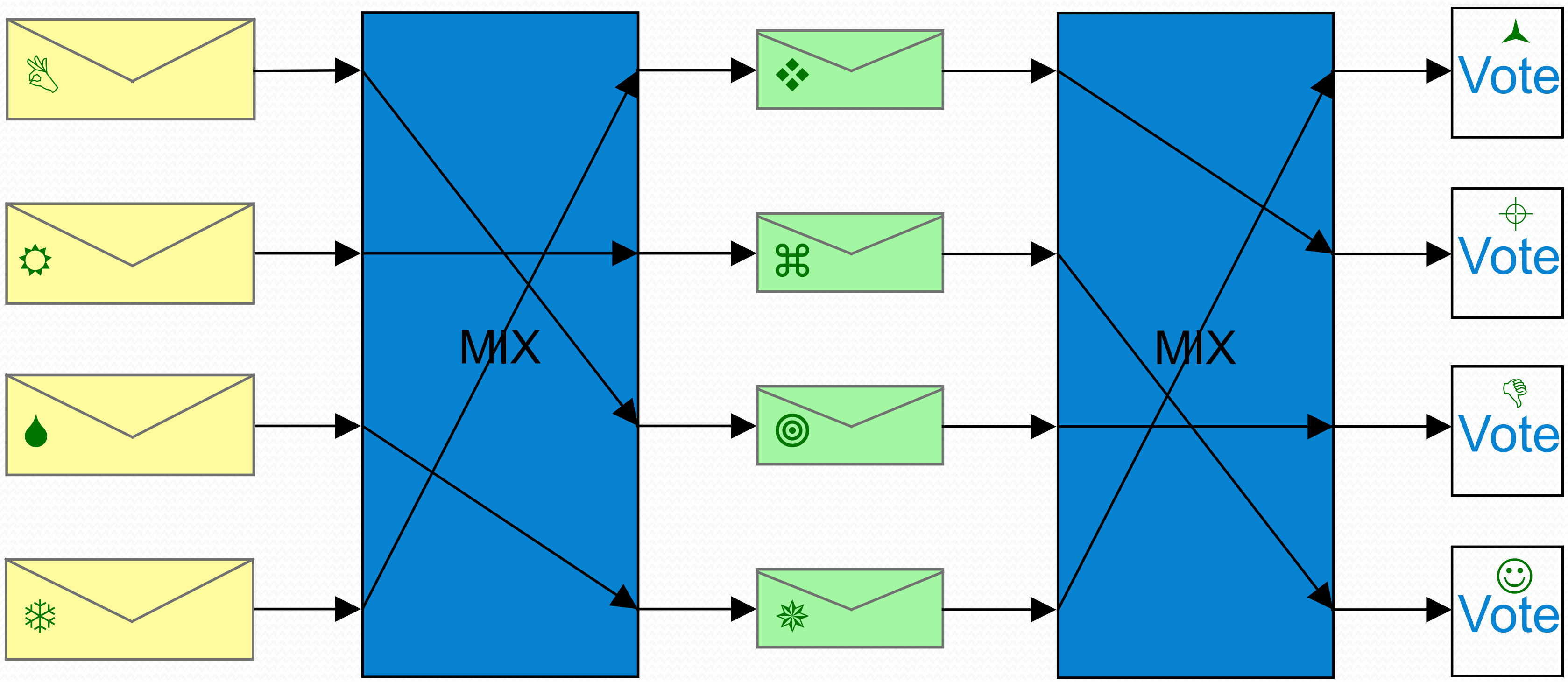
The Mix-Net Paradigm



The Mix-Net Paradigm



Multiple Mixes



Decryption Mix-net

Each object is encrypted with a pre-determined set of encryption layers.

Each mix, in pre-determined order performs a decryption to remove its associated layer.

Re-encryption Mix-net

- The decryption and shuffling functions are decoupled.
- Mixes can be added or removed dynamically with robustness.
- Proofs of correct mixing can be published and independently verified.

Recall Homomorphic Encryption

We can construct a public-key encryption function E such that if

A is *an* encryption of a and

B is *an* encryption of b then

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

Re-encryption (additive)

A is *an* encryption of a and

Z is *an* encryption of 0 then

$A \otimes Z$ is *another* encryption of a.

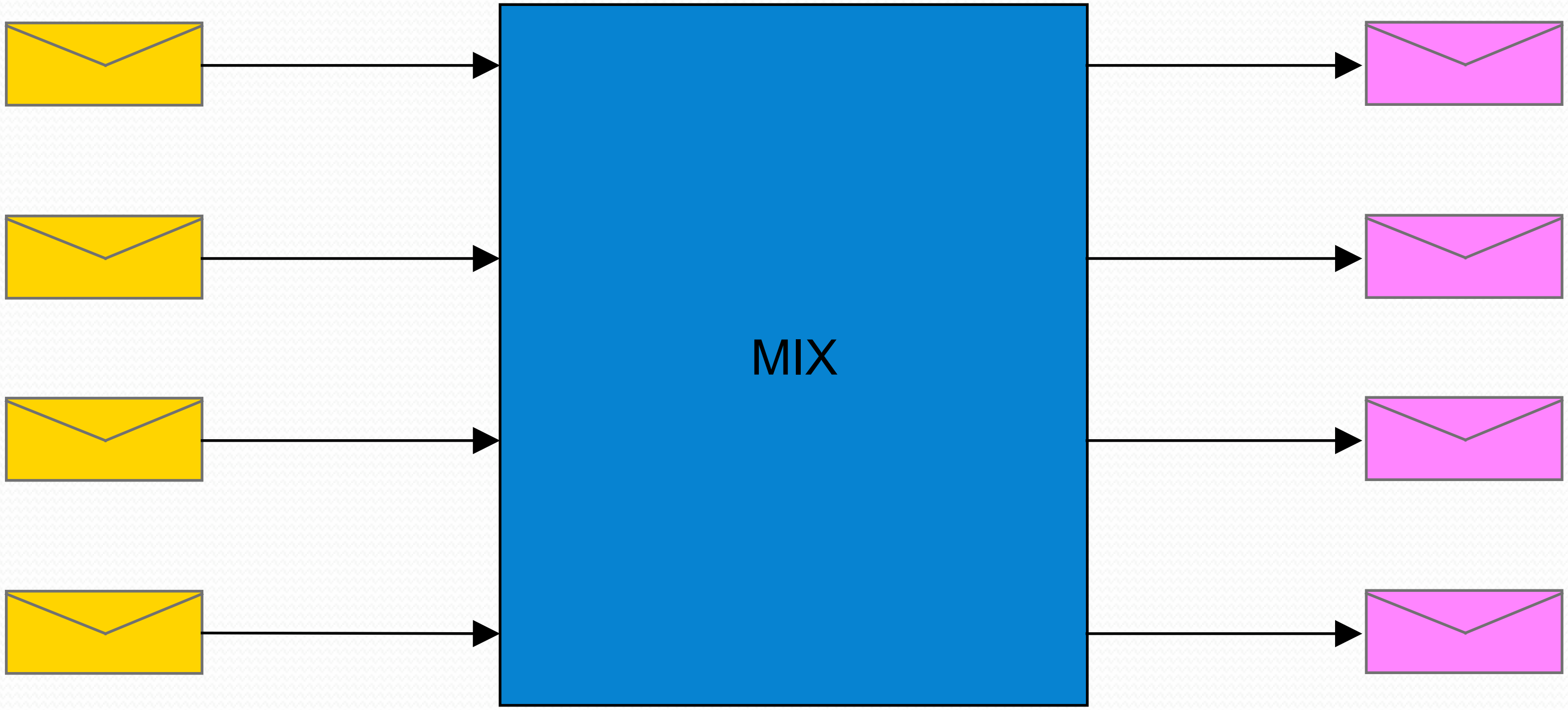
Re-encryption (multiplicative)

A is *an* encryption of *a* and

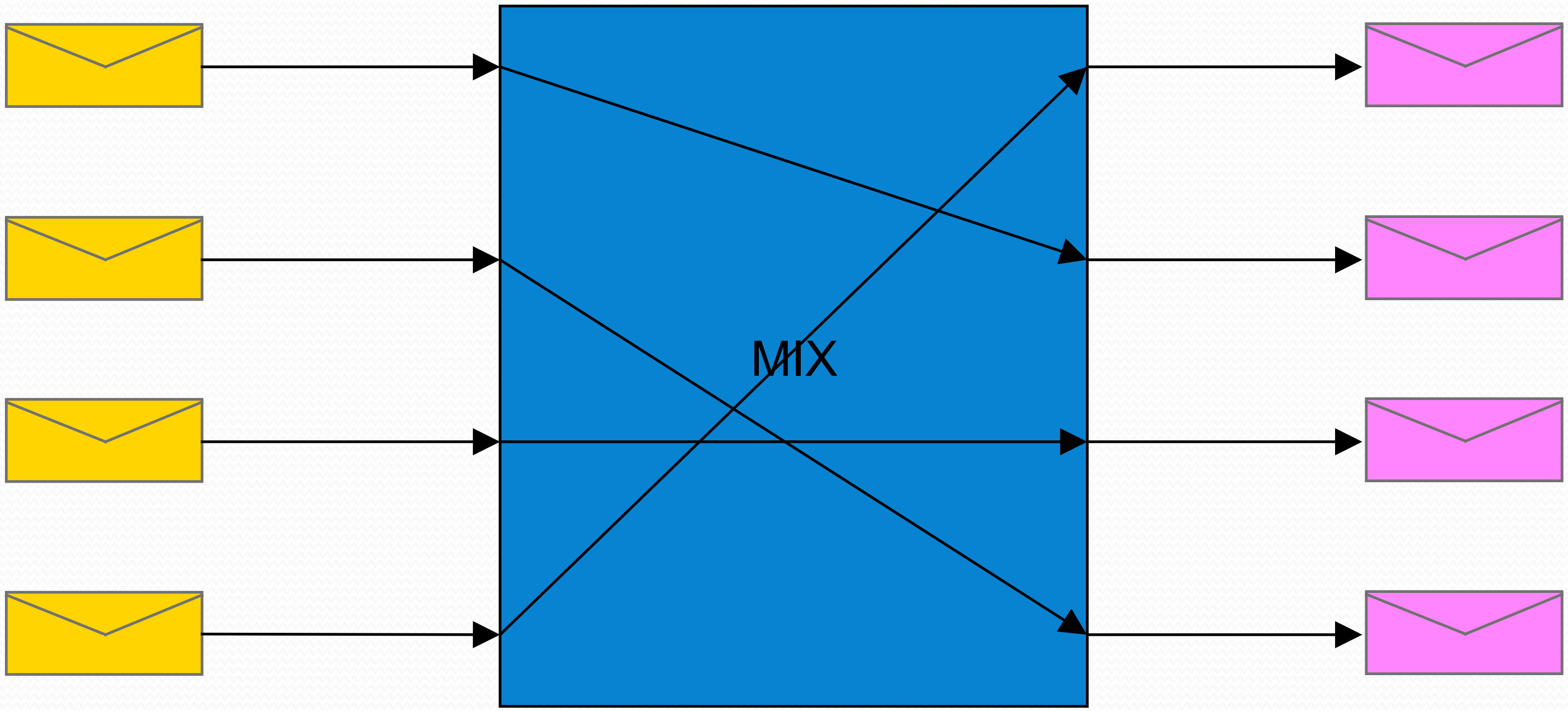
I is *an* encryption of *1* then

$A \otimes I$ is *another* encryption of *a*.

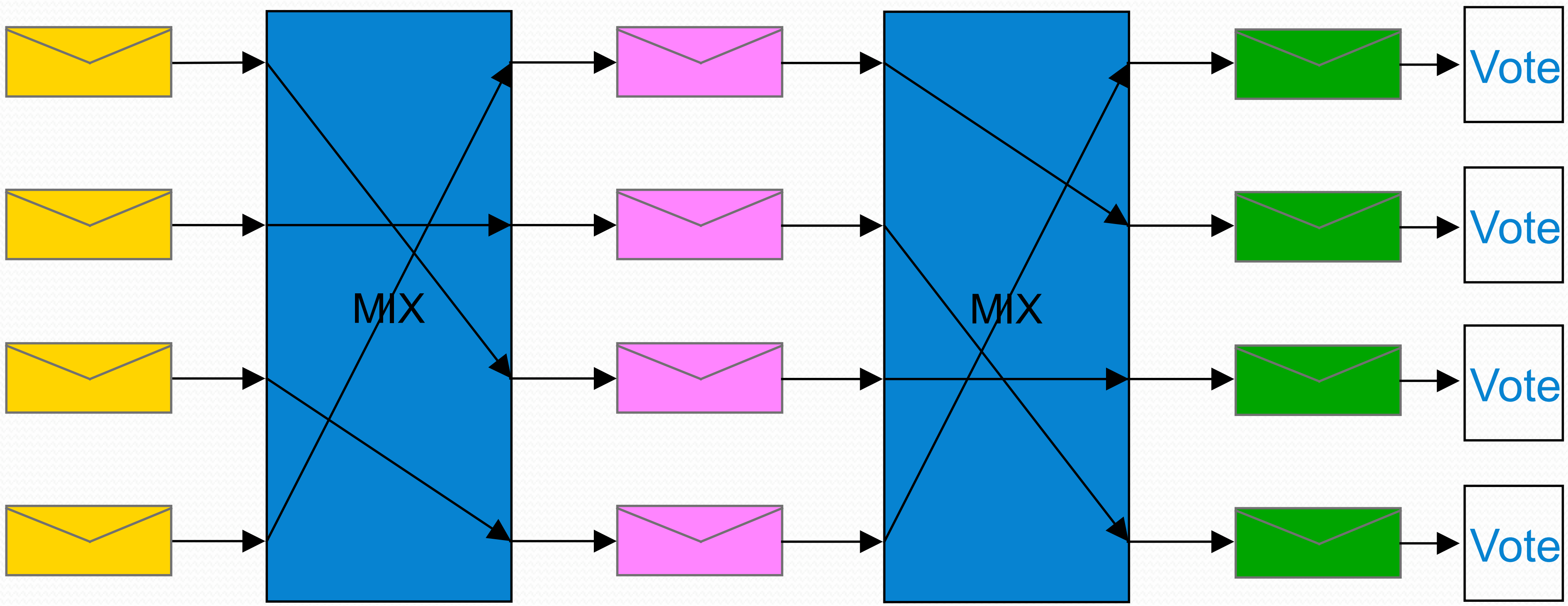
A Re-encryption Mix



A Re-encryption Mix



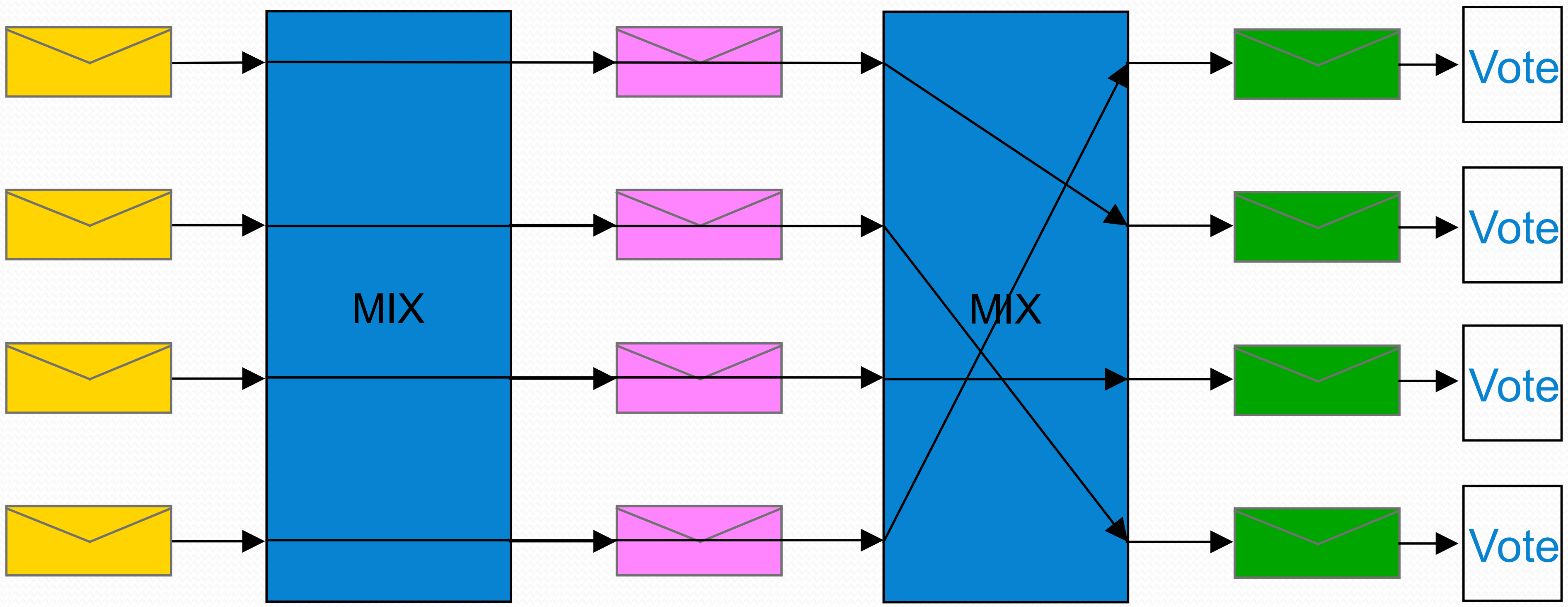
Re-encryption Mix-nets



Verifiability

- Each re-encryption mix provides a mathematical proof that its output is a permutation of re-encryptions of its input.
- Any observer can verify this proof.
- The decryptions are also proven to be correct.
- If a mix's proof is invalid, its mixing will be bypassed.

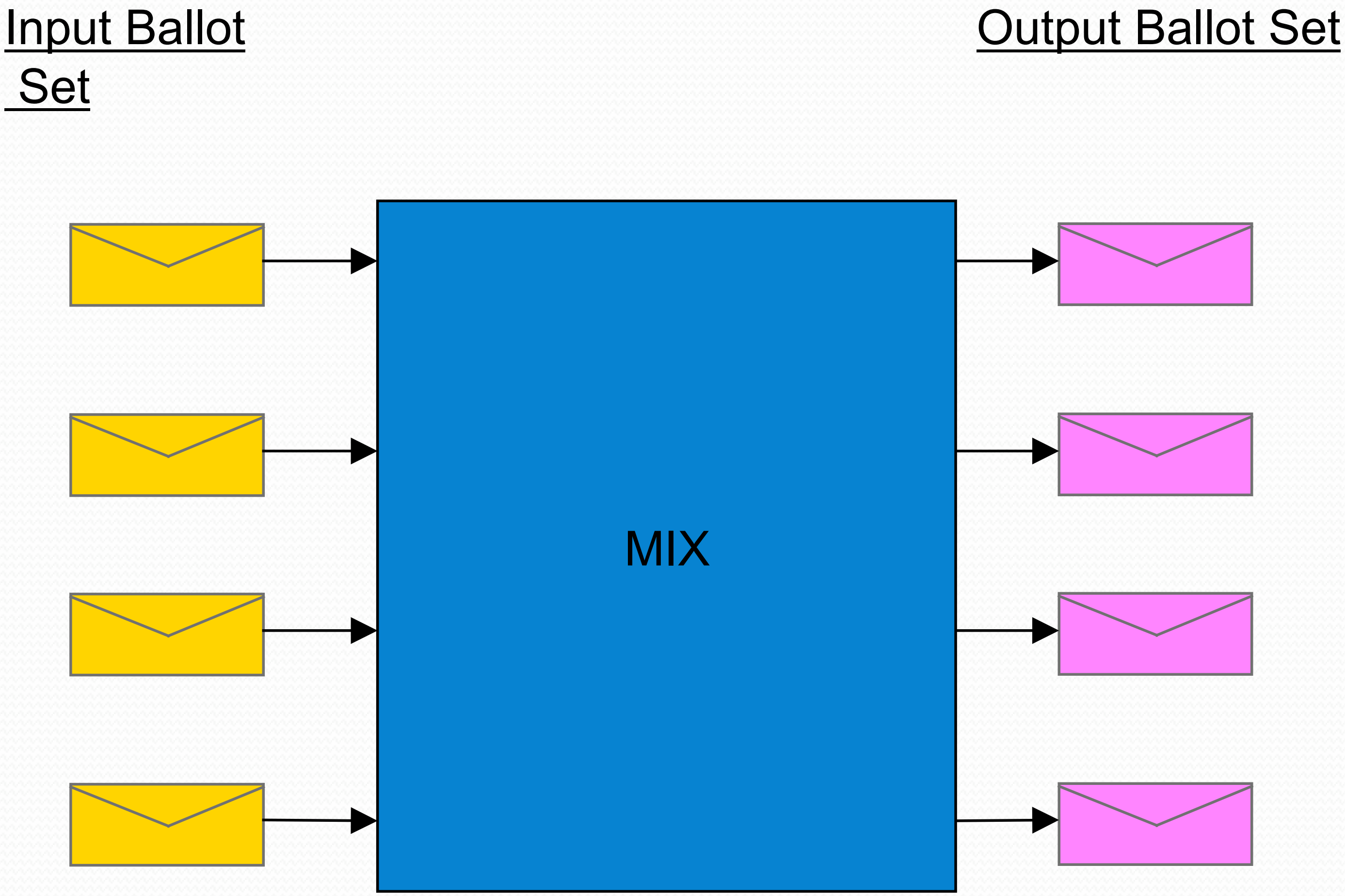
Faulty Mixes



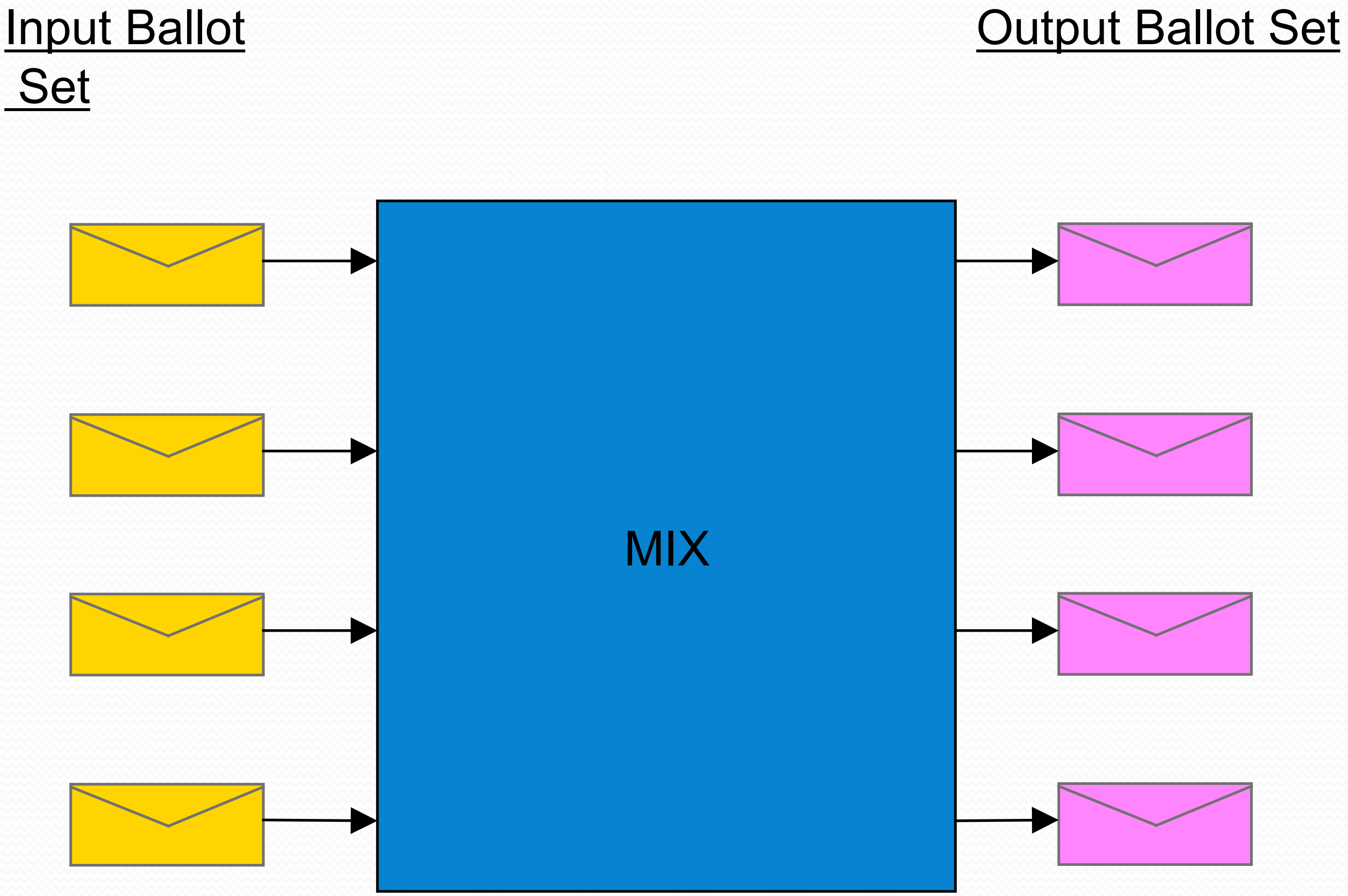
Recent Mix Work

- 1993 Park, Itoh, and Kurosawa
- 1995 Sako and Kilian
- 2001 Furukawa and Sako
- 2001 Neff
- 2002 Jakobsson, Juels, and Rivest
- 2003 Groth

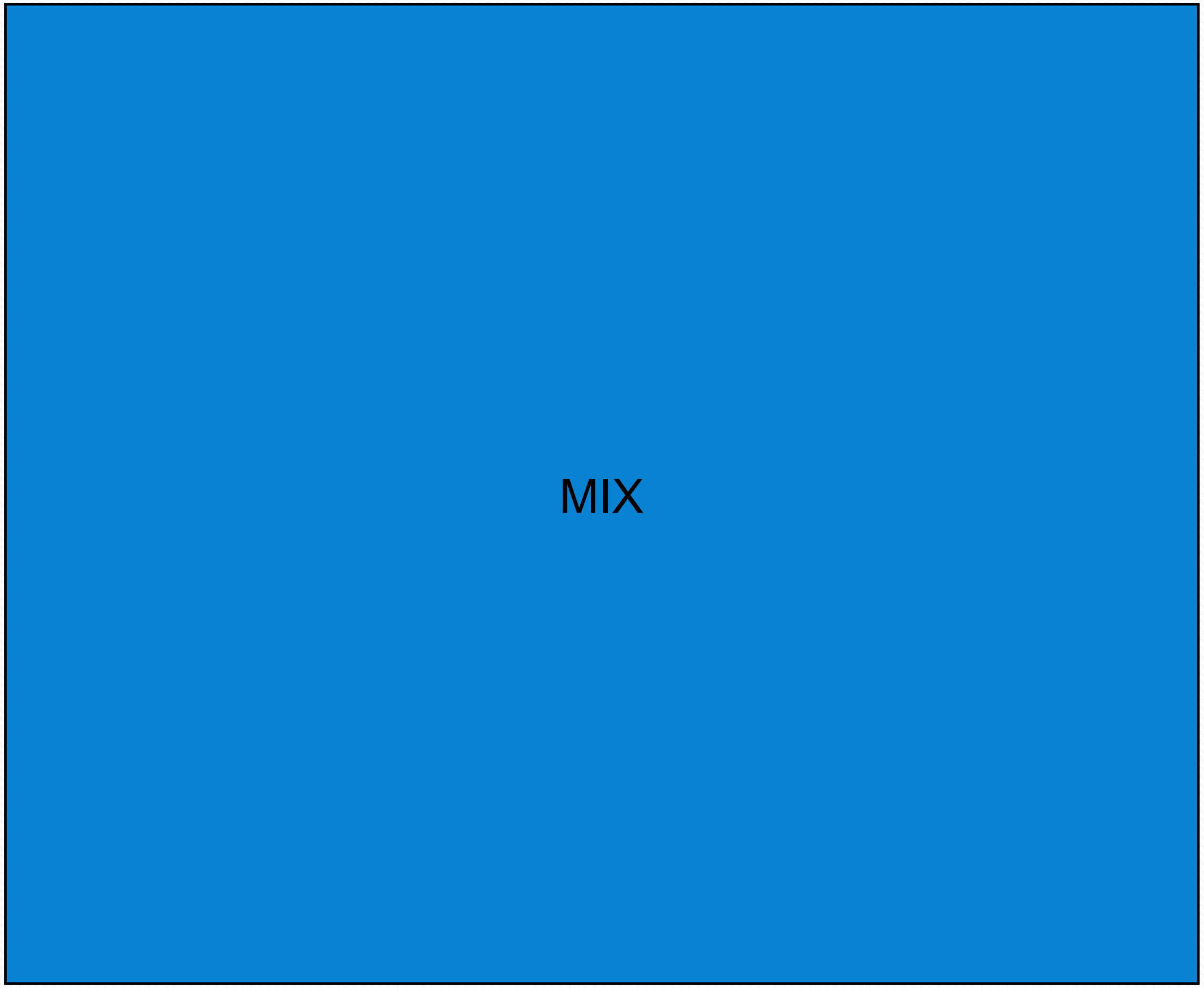
Re-encryption Mix Operation



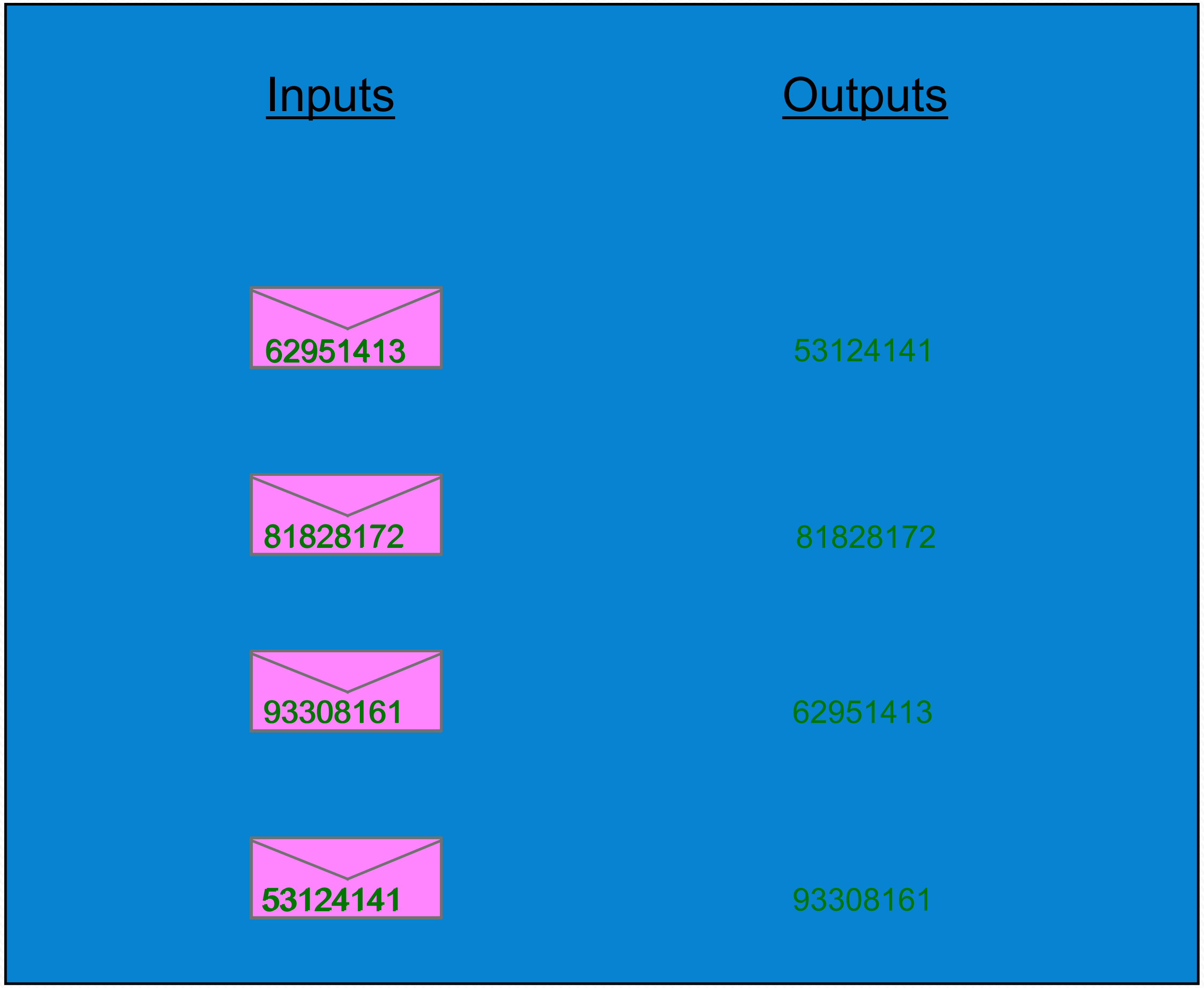
Re-encryption Mix Operation



Re-encryption Mix Operation



Re-encryption Mix Operation

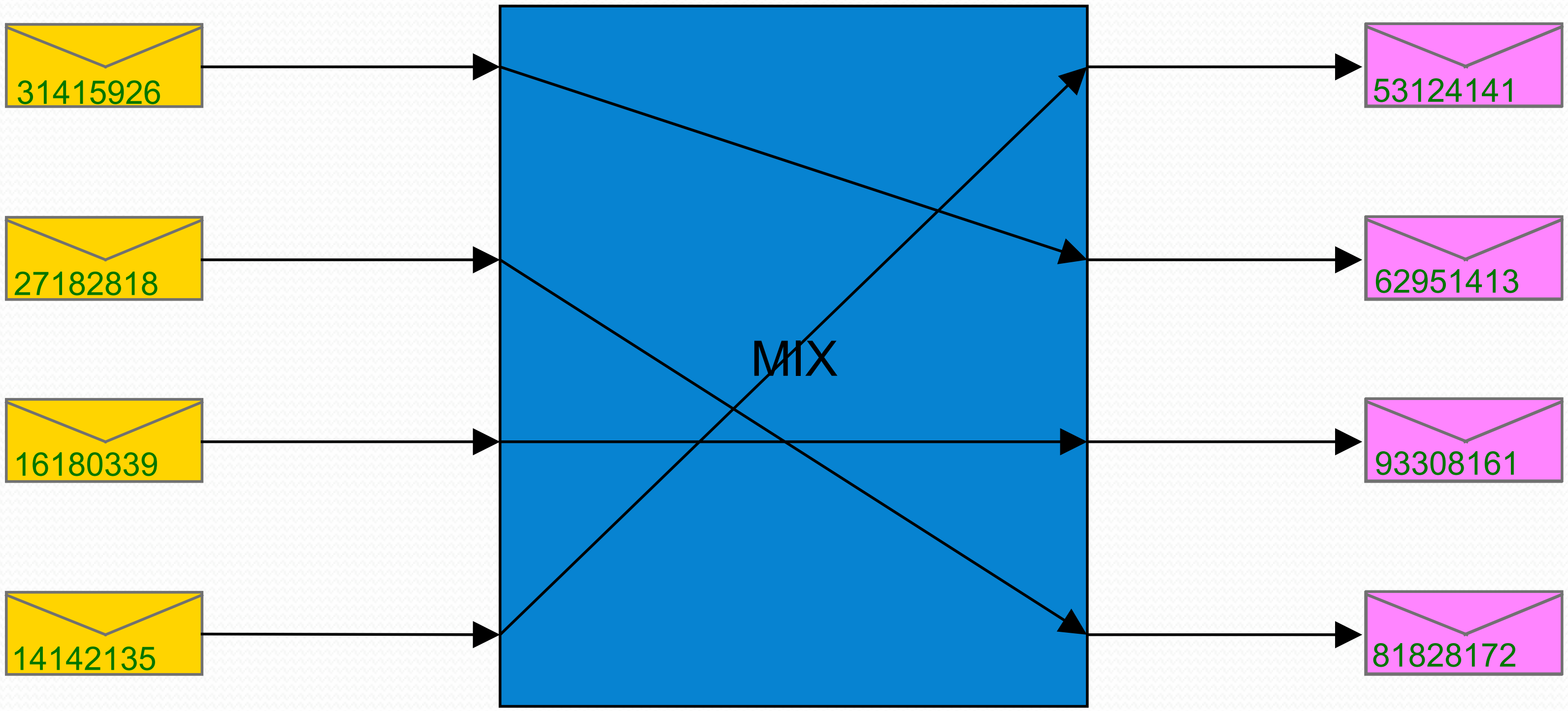


Re-encryption

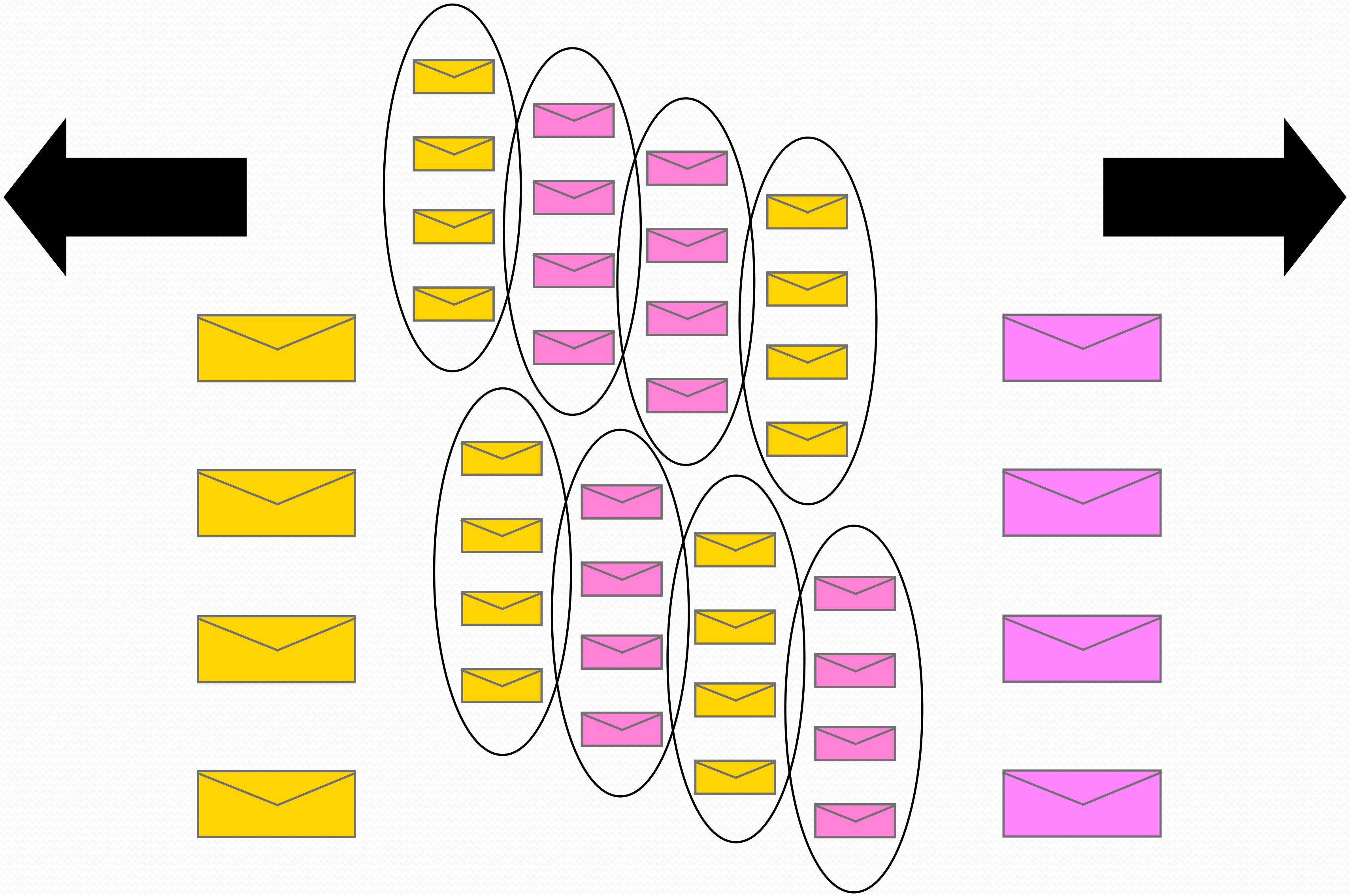
- Each value is *re-encrypted* by multiplying it by an encryption of one.

- This can be done *without* knowing the decryptions.

Verifying a Re-encryption



A Simple Verifiable Re-encryption Mix



Is This "Proof" Absolute?

- The proof can be "defeated" *if and only if* every left/right decision can be predicted by the prover in advance.
- If there are 100 intermediate ballot sets, the chance of this happening is 1 in 2^{100}.

Who Chooses?

If *you* choose, then *you* are convinced.

- But this won't convince me.

We can each make some of the choices.

- But this can be inefficient.

We can co-operate on the choices.

- But this is cumbersome.

We can agree on a random source.

- But what source?

Who Chooses?

The Fiat-Shamir Heuristic

- Prepare all of the ballot sets as above.
- Put all of the data into a one-way hash.
- Use the hash output to make the choices.

This allows a proof of equivalence to be “published” by the mix.

Assumptions

A disadvantage of using Fiat-Shamir is that election integrity now requires a computational assumption – the assumption that the hash is "secure".

Voter privacy depends upon the quality of the encryption.

The Encryption

- Anyone with the decryption key can read all of the votes – even before mixing.
- A threshold encryption scheme is used to distribute the decryption capabilities.

Randomized Partial Checking

Choose Any Two

We have techniques to make verifiable tallying …

1. Computationally Efficient
2. Conceptually Simple
3. Exact

Most Verifiable Election Protocols

Step 1

Encrypt your vote and …

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

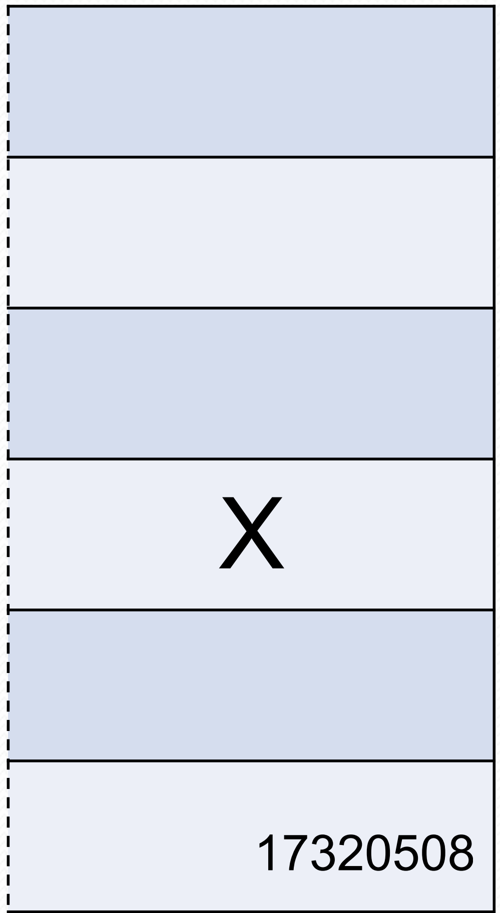
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	
David	
	17320508

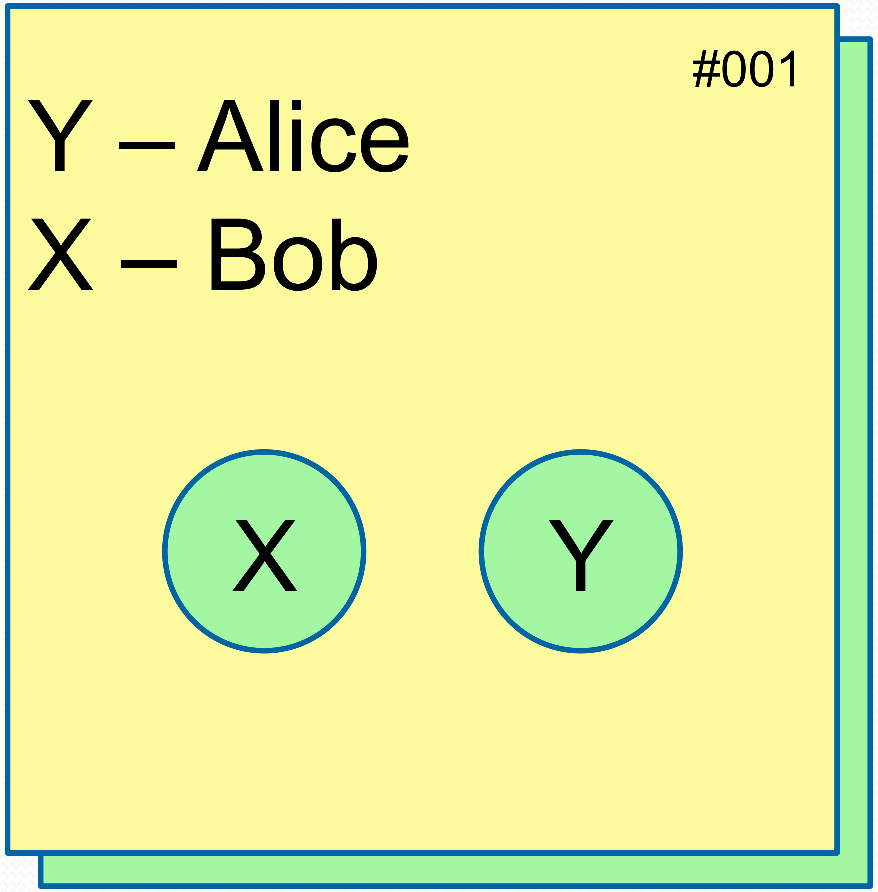
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	X
David	
	17320508

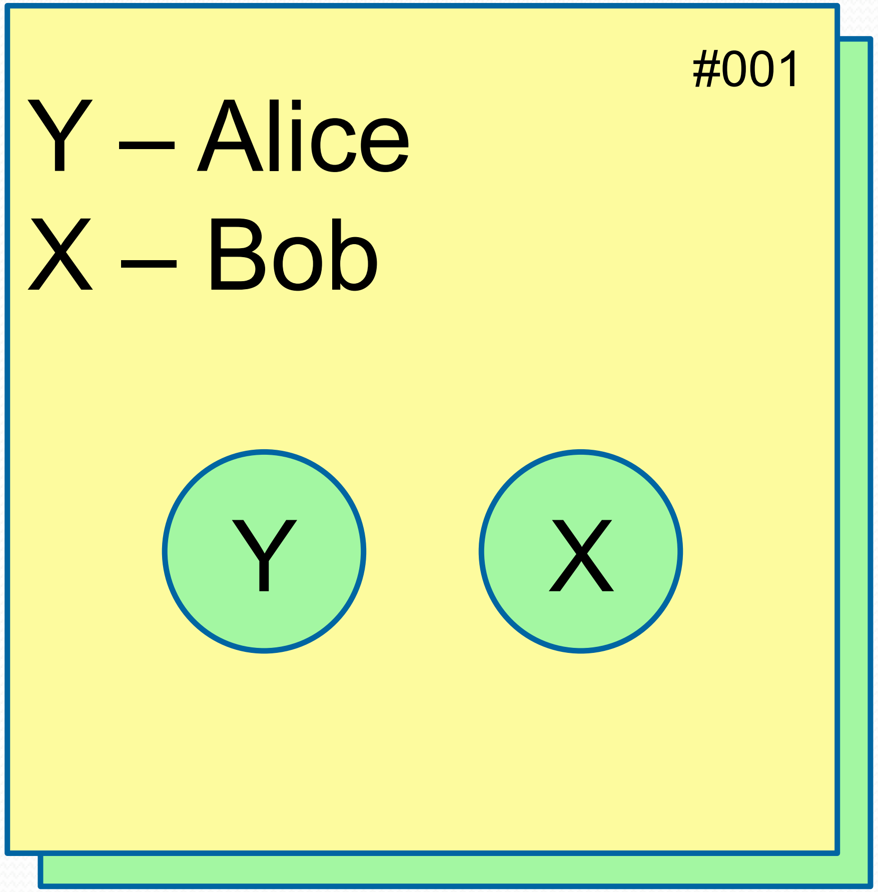
Prêt à Voter Ballot



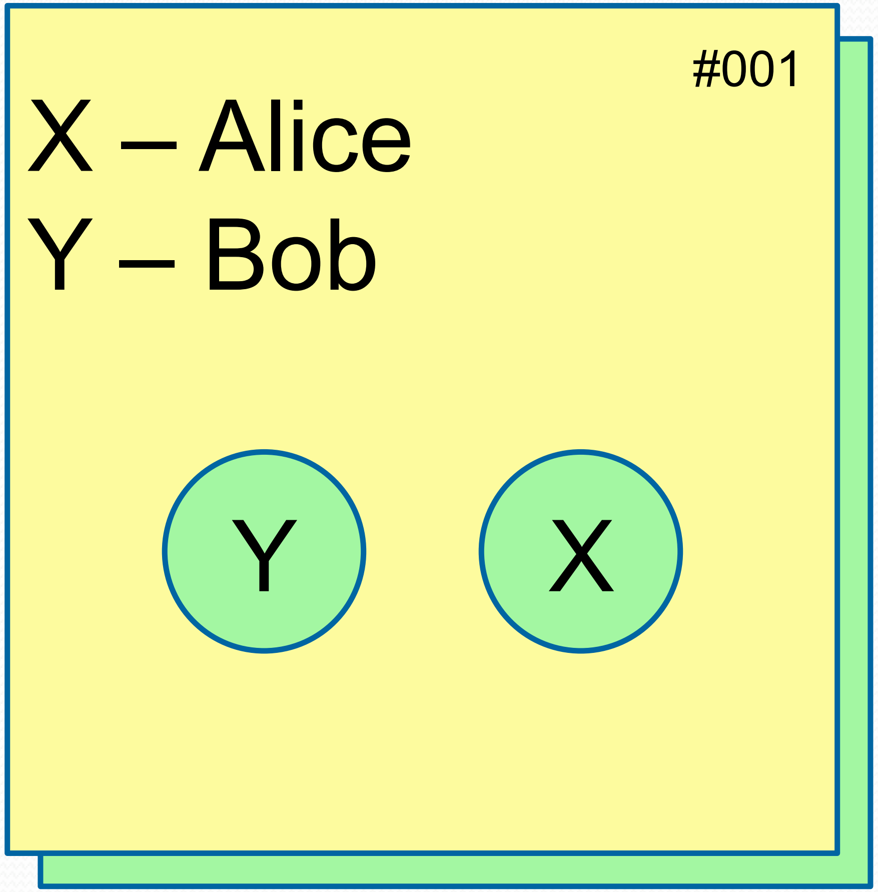
PunchScan Ballot



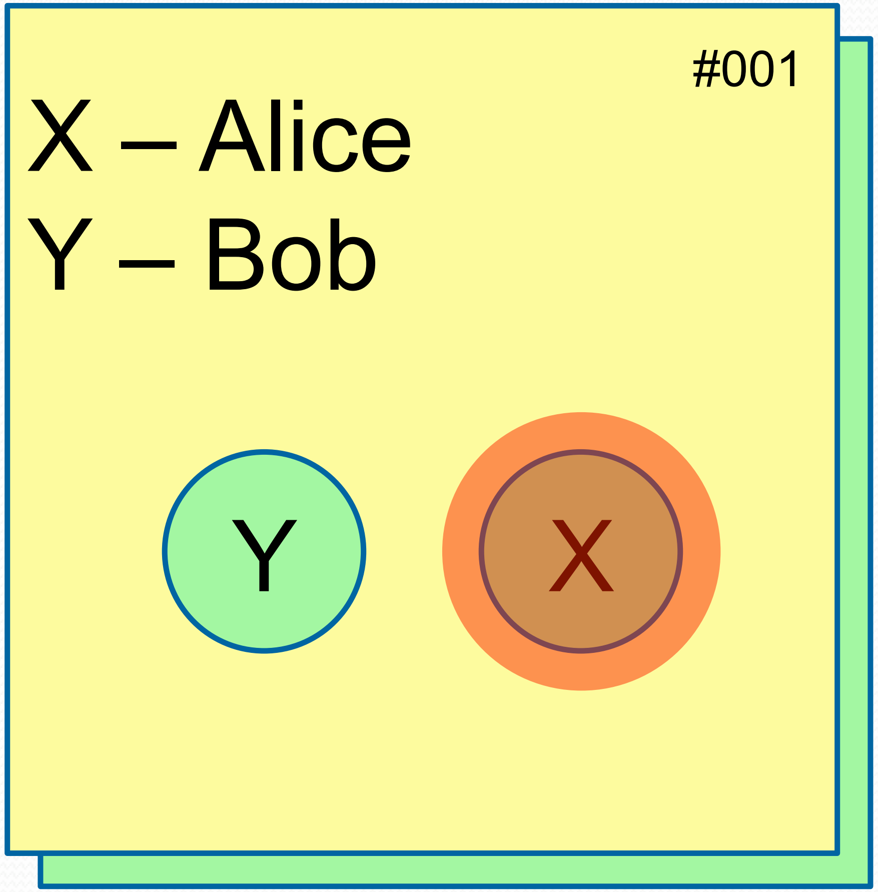
PunchScan Ballot



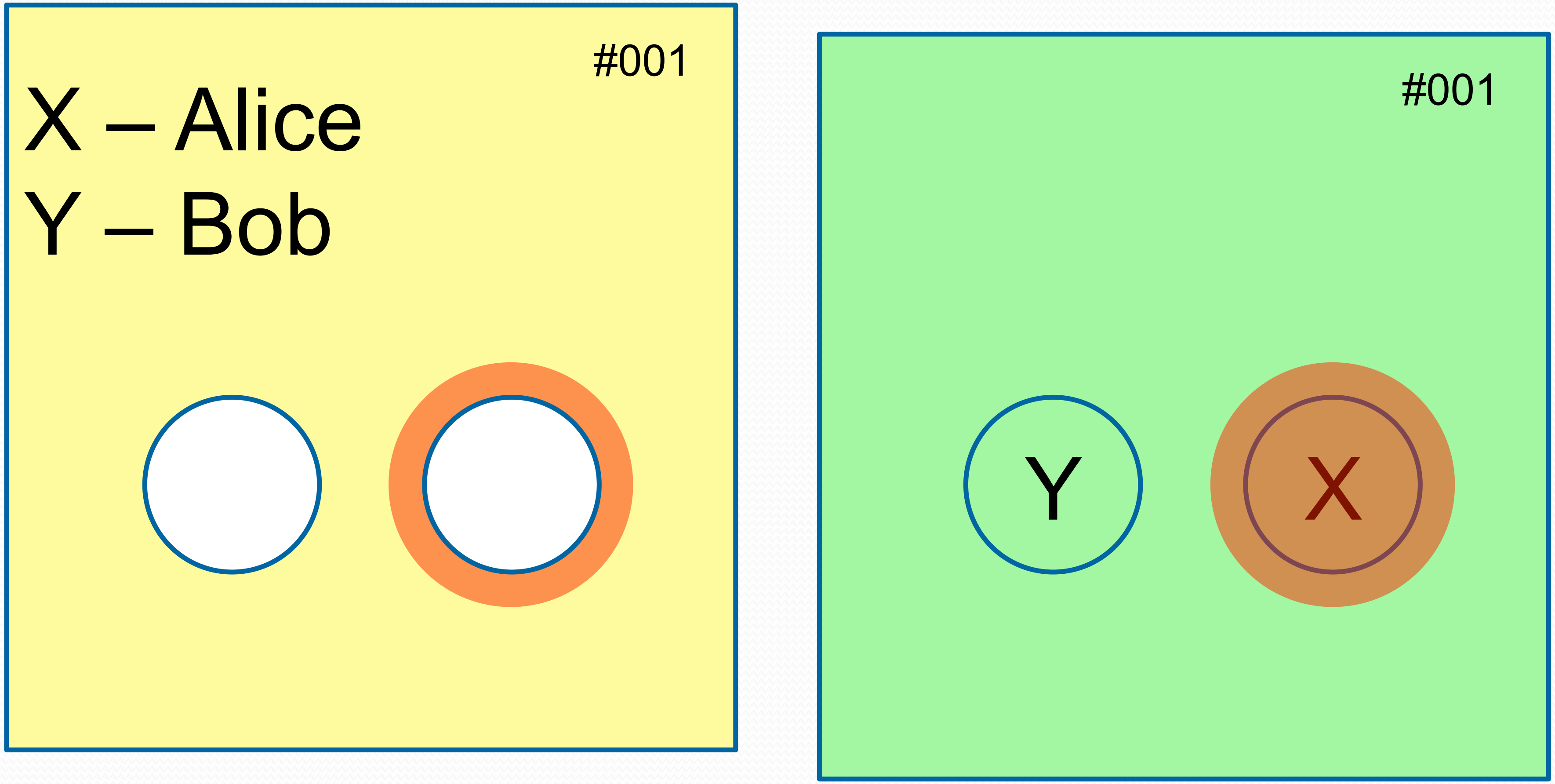
PunchScan Ballot



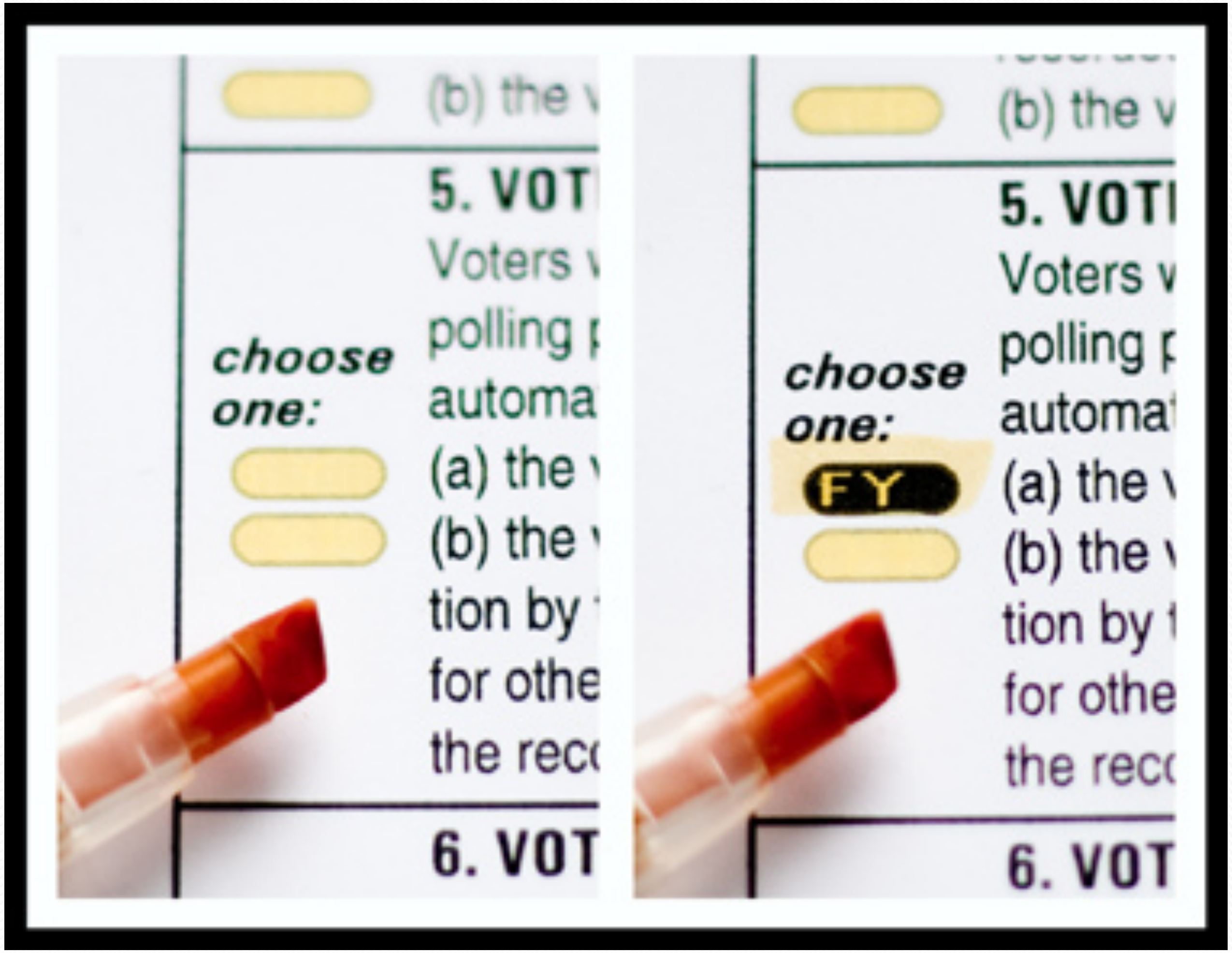
PunchScan Ballot



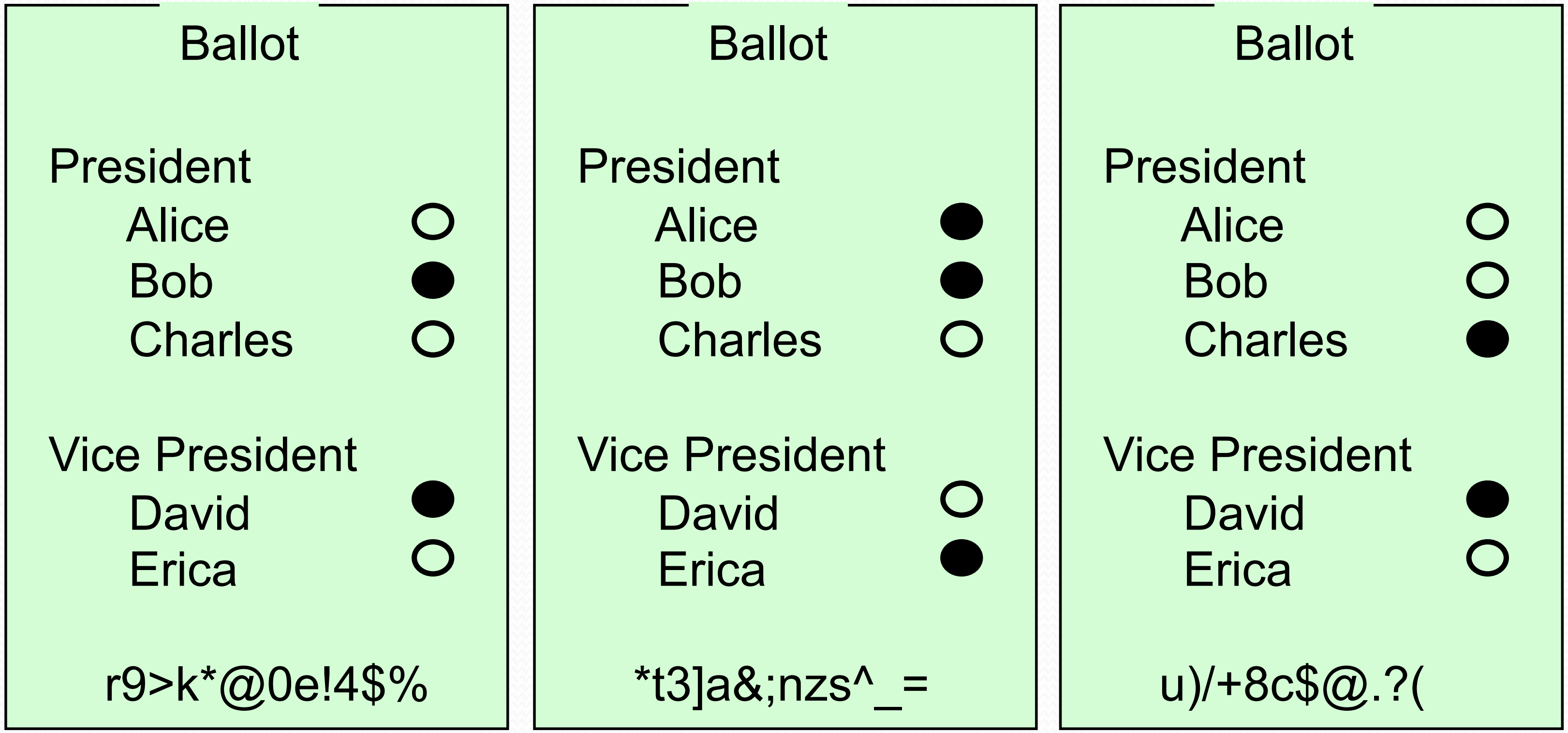
PunchScan Ballot



Scantegrity



Three-Ballot



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.

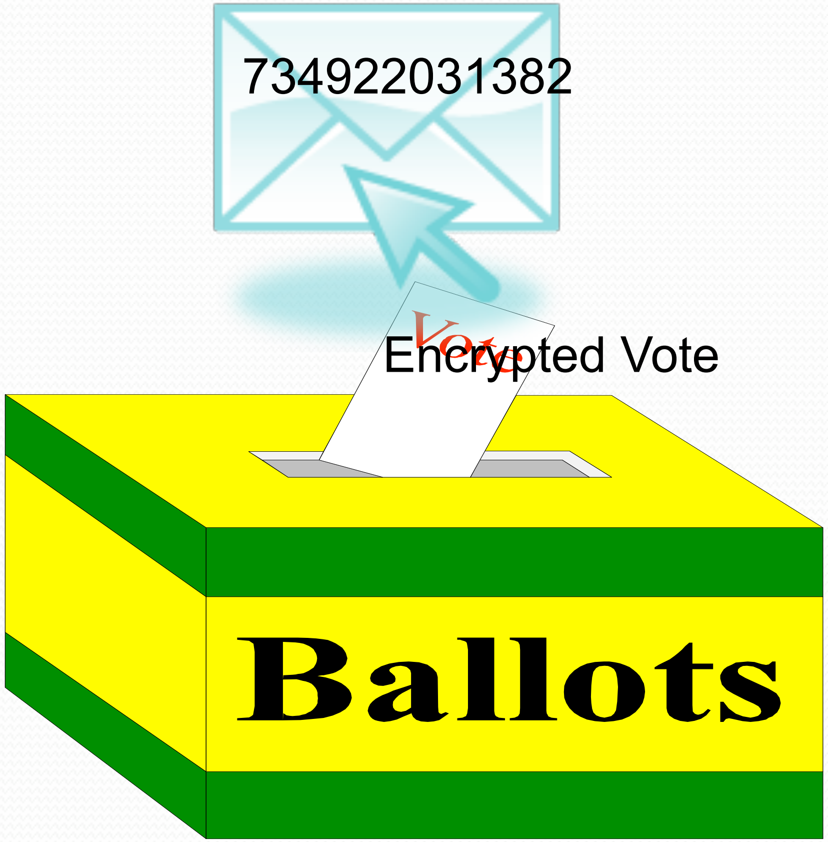
Voter-Initiated Auditing

Encrypted Vote

Voter choice: Cast or Challenge

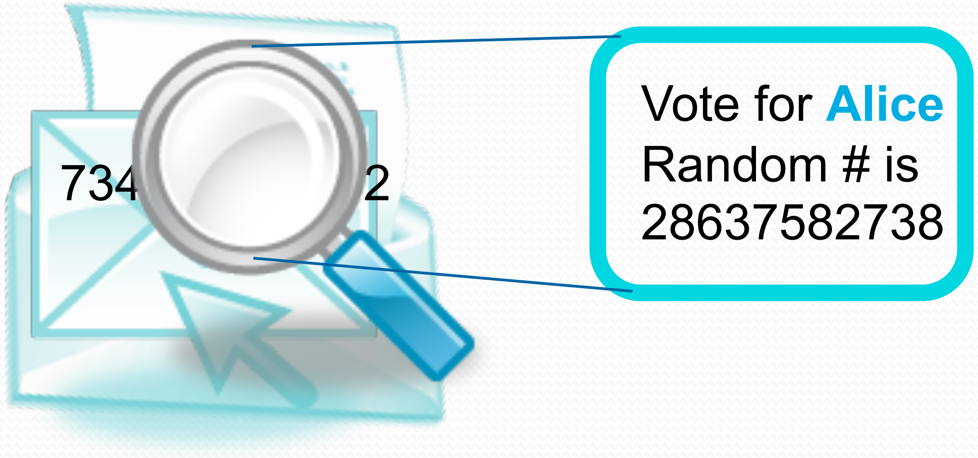
Voter-Initiated Auditing

Cast



Voter-Initiated Auditing

Challenge



Voter-Initiated Auditing

- When instantiated on an electronic voting device (DRE), it looks like Helios.

- When instantiated on an optical scanner, you get Verified Optical Scan.

Verified Optical Scan

Ballot format is identical to current optical scan.

- No special marks
- Identical ballots are fine

Verified Optical Scan

An Enhanced Ballot Scanner

- Capable of reading a ballot's contents and conditionally returning it
- Equipped with
  - Receipt Printer
  - Small Display
  - At Least Two "Choice" Buttons

Verified Optical Scan

The Ideal Ballot Scanner

- It is desirable (although not required) that the ballot scanner have the ability to print directly onto the ballot paper.
- This enables the scanner to print its interpretation of the ballot contents directly onto the ballot.

The Verified OpScan Voting Process

1. Voter prepares an optical scan ballot in a conventional manner.
2. Voter inserts the marked ballot into an optical scanner.
3. Scanner encrypts ballot contents and prints signed copy of encryption together with time, scanner ID, seq #.

Voter Options

4. Voter is given the following options.
   A. Cast this ballot.
   B. Modify this ballot.
   C. Cancel this ballot.

The "Cast" Option

If the voter chooses to cast the ballot

- The scanner's interpretation of the ballot's contents are printed onto ballot.
- The scanner adds an additional signature and hash fingerprint to the paper receipt indicating that the ballot has been cast.
- Voter takes receipt home.

The "Modify" Option

If the voter chooses to modify this ballot

- The ballot is returned to the voter without any additional marks.
- The voter is allowed to take the receipt, but it will serve no value.

The “Cancel” Option

If the voter chooses to cancel this ballot

- The scanner’s interpretation of the ballot’s contents are printed onto ballot.
- An additional mark is printed onto the ballot to indicate it is VOID for casting.
- A signed verifiable decryption and hash fingerprint are added to printed receipt.

Verification

- Voters can check that their encrypted ballots are properly posted.
- Voters and others can check that the back-end tallying is properly performed.
- Voters and others can check that cancelled ballots are properly decrypted.

Benefits

- Addition of an Independent Audit Path
- Blocking of Conspiratorial Threats
- Detection of Inadvertent Scanner Errors

Threats

- Cryptographic Compromise
- Covert Channels
- Coercion
- Ballot Addition/Deletion/Substitution
- Encrypted Ballot Duplication

Reduced Functionality

- No receipt printer
  - Hash codes can be displayed instead
- No display
  - Two marked buttons (Cast or Cancel) suffice
- No ability to print onto ballots
  - Voters must be prevented from casting previously cancelled ballots

Partial Implementation

Implementing this front end system without a cryptographic back-end still catches many faulty scanners and allows voters to check that their votes have been properly recorded.

Incremental Improvements

Many of these measures are simple improvements that offer benefits even if not used with truly “end to end” publically verifiable systems.

The Greater Whole …

When enough of these improvements are implemented, we can obtain the benefits of public verifiability without sacrificing the comfort we often have in good administrative verifiability.

Ballot Casting Assurance

The voter front ends shown here differ in both their human factors qualities and the level of assurance that they offer.

All are feasible and provide greater integrity than current methods.

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.

What’s Left?

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

What's Left?

Back End

Simple counting methods are well-understood with effective techniques.

More complex counting methods create substantial challenges –

- Maintaining strong privacy
- Keeping computations efficient

Is There any Deployment Hope?

- The U.S. Election Assistance Commission is considering new guidelines.
- These guidelines explicitly include an “innovation class” which could be satisfied by truly verifiable election systems.
- Election supervisors must choose to take this opportunity to change the paradigm.

Questions?