Practical Aspects of Modern Cryptography

Winter 2011

Josh Benaloh
Brian LaMacchia

Some Tools We've Developed

- Homomorphic Encryption
- Secret Sharing
- Verifiable Secret Sharing
- Threshold Encryption
- Interactive Proofs

Secret Sharing Homomorphisms

Many secret sharing methods have an additional useful feature:

If two secrets are separately shared amongst the same set of people in the same way, then the sum of the individual shares constitute shares of the sum of the secrets.

Secret Sharing Homomorphisms

OR

Secret: a – Shares: $a, a, \ldots, a$

Secret: b – Shares: $b, b, \ldots, b$

Secret sum: $a + b$

Share sums: $a + b, a + b, \ldots, a + b$

Secret Sharing Homomorphisms

AND

Secret: a – Shares: $a_1, a_2, \ldots, a_n$

Secret: b – Shares: $b_1, b_2, \ldots, b_n$

Secret sum: $a + b$

Share sums: $a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n$

Secret Sharing Homomorphisms

THRESHOLD

Secret: $P_1(0)$ – Shares: $P_1(1), P_1(2), \ldots, P_1(n)$

Secret: $P_2(0)$ – Shares: $P_2(1), P_2(2), \ldots, P_2(n)$

Secret sum: $P_1(0) + P_2(0)$

Share sums: $P_1(1) + P_2(1), P_1(2) + P_2(2), \ldots, P_1(n) + P_2(n)$

Threshold Encryption

I want to encrypt a secret message M for a set of n recipients such that

- any k of the n recipients can uniquely decrypt the secret message M,
- but any set of fewer than k recipients has *no information whatsoever* about the secret message M.

Recall Diffie-Hellman

Alice

- Randomly select a large integer a and send $A = g^a \bmod p$.
- Compute the key $K = B^a \bmod p$.

Bob

- Randomly select a large integer b and send $B = g^b \bmod p$.
- Compute the key $K = A^b \bmod p$.

$$B^a = g^{ba} = g^{ab} = A^b$$

ElGamal Encryption

ElGamal Encryption

- Alice selects a large random private key a and computes an associated public key $A = g^a \bmod p$.

ElGamal Encryption

- Alice selects a large random private key a and computes an associated public key $A = g^a \bmod p$.
- To send a message M to Alice, Bob selects a random value r and computes the pair
  $$(X, Y) = (A^r M \bmod p, g^r \bmod p).$$

ElGamal Encryption

- Alice selects a large random private key a and computes an associated public key $A = g^a \bmod p$.
- To send a message M to Alice, Bob selects a random value r and computes the pair
$$(X, Y) = (A^r M \bmod p, g^r \bmod p).$$
- To decrypt, Alice computes
$$X/Y^a \bmod p = A^r M/g^{ra} \bmod p = M.$$

ElGamal Re-Encryption

If $A = g^a \bmod p$ is a public key and the pair

$$(X, Y) = (A^r M \bmod p, g^r \bmod p)$$

is an encryption of message M, then for any value c, the pair

$$(A^c X, g^c Y) = (A^{c+r} M \bmod p, g^{c+r} \bmod p)$$

is an encryption of the same message M, for any value c.

Group ElGamal Encryption

Group ElGamal Encryption

- Each recipient selects a large random private key a_i and computes an associated public key $A_i = g^{a_i} \bmod p$.

Group ElGamal Encryption

- Each recipient selects a large random private key a_i and computes an associated public key $A_i = g^{a_i} \bmod p$.
- The group key is $A = \prod A_i \bmod p = g^{\sum a_i} \bmod p$.

Group ElGamal Encryption

- Each recipient selects a large random private key a_i and computes an associated public key $A_i = g^{a_i} \bmod p$.
- The group key is $A = \prod A_i \bmod p = g^{\sum a_i} \bmod p$.
- To send a message M to the group, Bob selects a random value r and computes the pair $(X, Y) = (A^r M \bmod p, g^r \bmod p)$.

Group ElGamal Encryption

- Each recipient selects a large random private key a_i and computes an associated public key $A_i = g^{a_i} \bmod p$.
- The group key is $A = \prod A_i \bmod p = g^{\sum a_i} \bmod p$.
- To send a message M to the group, Bob selects a random value r and computes the pair $(X, Y) = (A^r M \bmod p, g^r \bmod p)$.
- To decrypt, each group member computes $Y_i = Y^{a_i} \bmod p$. The message $M = X / \prod Y_i \bmod p$.

Threshold Encryption (ElGamal)

Threshold Encryption (ElGamal)

- Each recipient selects k large random secret coefficients $a_{i,0}$, $a_{i,1}$, …, $a_{i,k-2}$, $a_{i,k-1}$ and forms the polynomial
  $$P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0}$$

Threshold Encryption (ElGamal)

- Each recipient selects k large random secret coefficients $a_{i,0}$, $a_{i,1}$, …, $a_{i,k-2}$, $a_{i,k-1}$ and forms the polynomial
  $$P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0}$$
- Each polynomial $P_i(x)$ is then verifiably shared with the other recipients by distributing each $g^{a_{i,j}}$.

Threshold Encryption (ElGamal)

- Each recipient selects k large random secret coefficients $a_{i,0}$, $a_{i,1}$, …, $a_{i,k-2}$, $a_{i,k-1}$ and forms the polynomial
  $$P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0}$$
- Each polynomial $P_i(x)$ is then verifiably shared with the other recipients by distributing each $g^{a_{i,j}}$.
- The joint (threshold) public key is $\prod g^{a_{i,0}}$.

Threshold Encryption (ElGamal)

- Each recipient selects k large random secret coefficients $a_{i,0}, a_{i,1}, \ldots, a_{i,k-2}, a_{i,k-1}$ and forms the polynomial
  $$P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0}$$
- Each polynomial $P_i(x)$ is then verifiably shared with the other recipients by distributing each $g^{a_{i,j}}$.
- The joint (threshold) public key is $\prod g^{a_{i,0}}$.
- Any set of k recipients can form the secret key $\sum a_{i,0}$ to decrypt.

An Application

Verifiable

Elections

Verifiable Election Technologies

As a voter, you can check that

- your vote is correctly recorded
- all recorded votes are correctly counted

…even in the presence of malicious software, hardware, and election officials.


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?


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


Where is my
Vote ...?
موج سبز
رای من کجاست؟
WHERISMY VOTE?


رأی من کجاست ؟
WHERE
IS MY
VOTE ?


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?

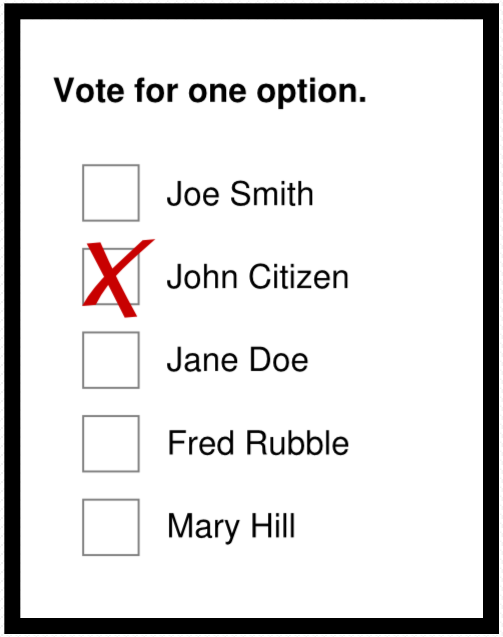

WHERE
IS MY
VOTE?


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

Traditional Voting Methods

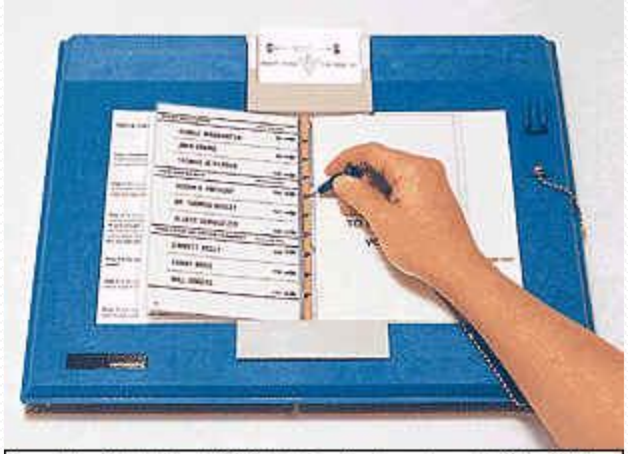
Traditional Voting Methods

- Hand-Counted Paper



Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards



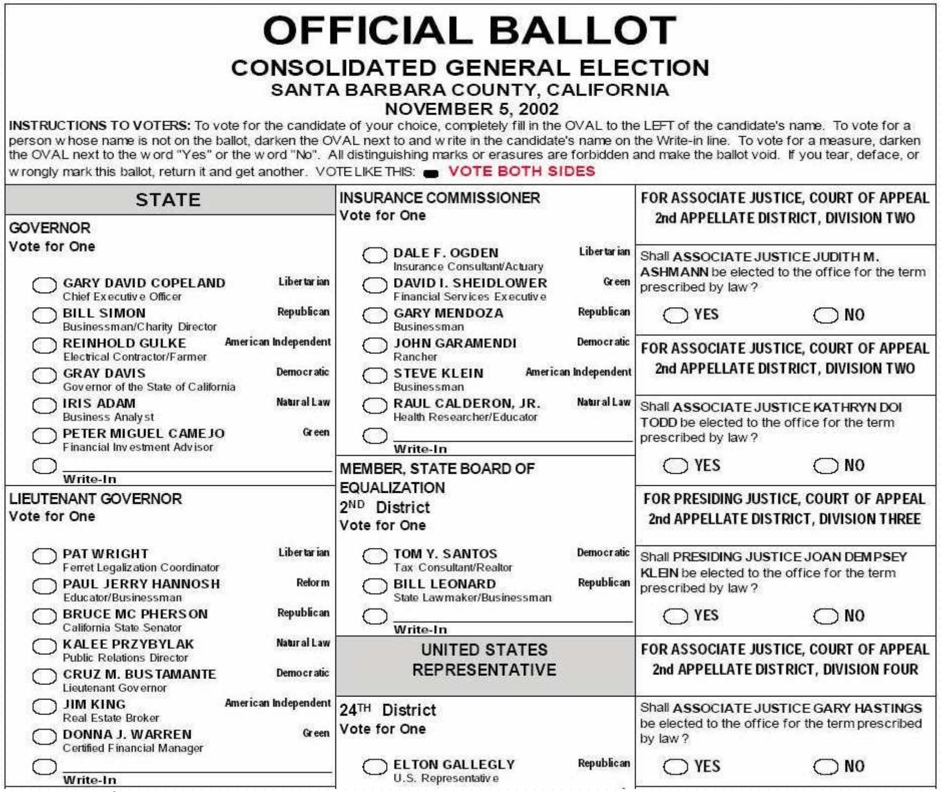
From The World Book (TM) Multimedia Encyclopedia (c) 1998 World Book, Inc., 525 W. Monroe, Chicago, IL 60661. All rights reserved. Larry Korb, Business Records Corporation

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
2ND District
Vote for One

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

UNITED STATES REPRESENTATIVE

24TH 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

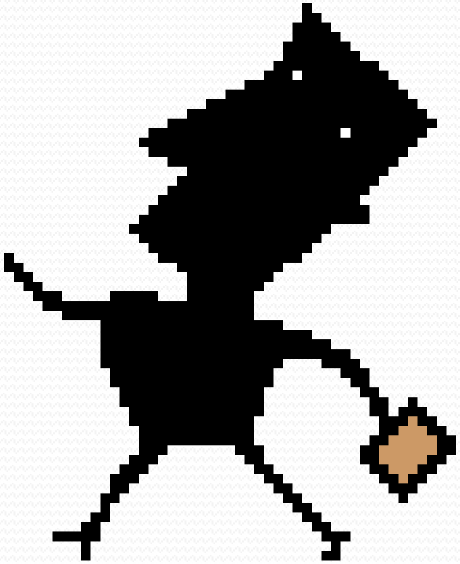
Vulnerabilities and Trust

- *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?

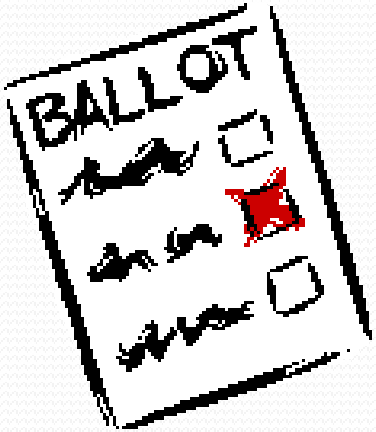
The Voter's Perspective

The Voter's Perspective

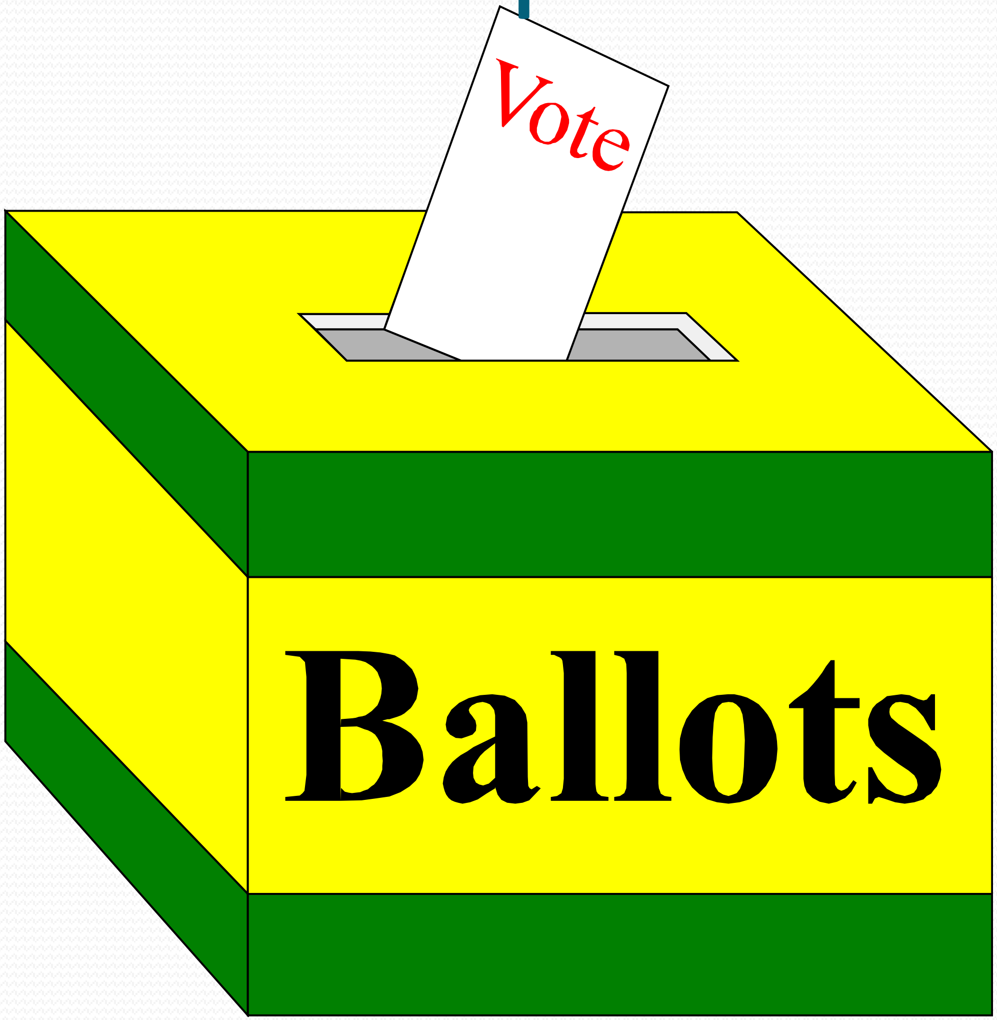


The Voter's Perspective

The Voter's Perspective

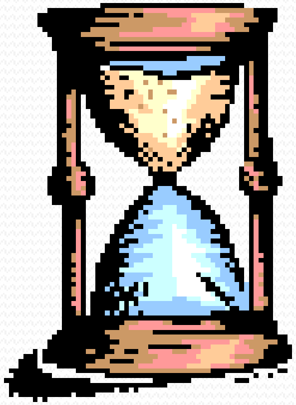


The Voter's Perspective

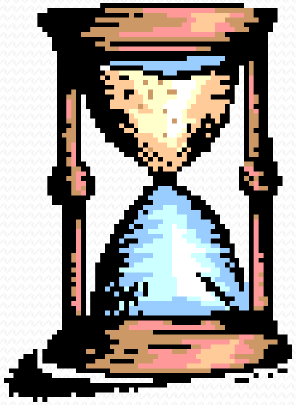


The Voter's Perspective

The Voter’s Perspective



The Voter's Perspective



The Voter's Perspective

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.

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.

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)

Fully-Verifiable Election Technologies (End-to-End Verifiable)

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

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 …

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 …

Voters can check …

… that their (sealed) votes have been properly recorded

Voters can check …

… that their (sealed) votes have been properly recorded

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

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 …

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 Verifiability

End-to-End Verifiability

As a voter, I can be sure that

End-to-End Verifiability

As a voter, I can be sure that

- My vote is

End-to-End Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended

End-to-End Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
  - Counted as cast

End-to-End Verifiability

As a voter, I can be sure that

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

End-to-End 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.*

One Thing Missing …

One Thing Missing …

… that pesky little *secret-ballot* requirement.

One Thing Missing …

… that pesky little *secret-ballot* requirement.

Elections would be sooooooo… much easier without it.

Full Voter-Verifiability *is* Possible

Full Voter-Verifiability *is* Possible

Even though this “toy” public election is not secret-ballot, it’s enough to show that voter-verifiability is possible

Full Voter-Verifiability *is* Possible

Even though this "toy" public election is not secret-ballot, it's enough to show that voter-verifiability is possible

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

Privacy

Privacy

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

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.

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

Bob Ramirez, 79 Oak

Carol Wilson, 821 Market

Where is *My* Vote?

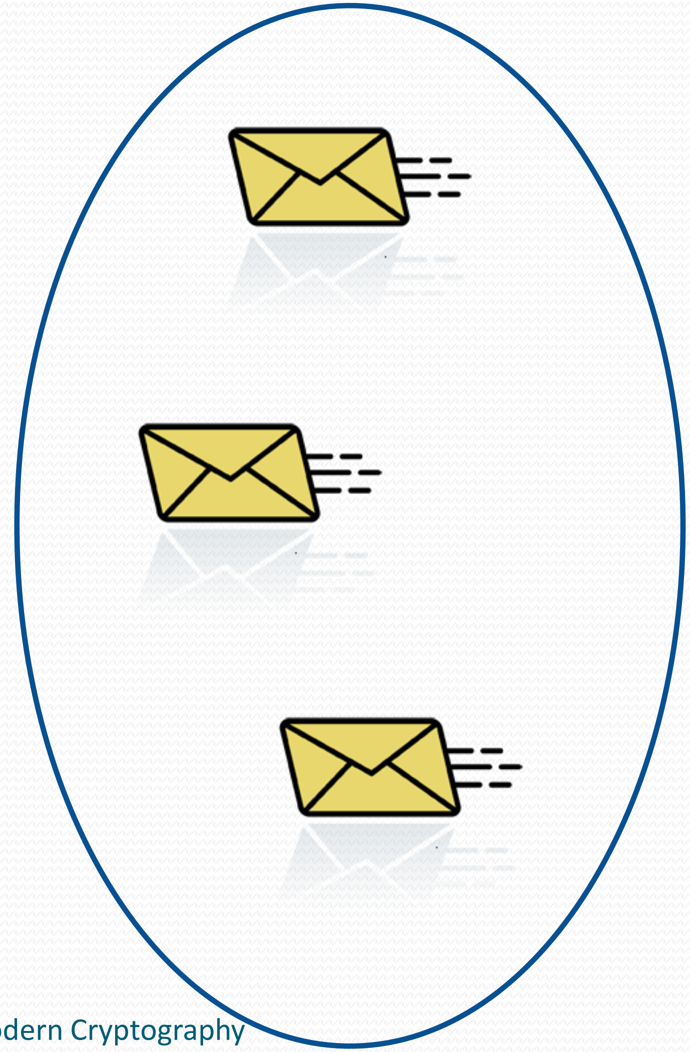
Alice Johnson, 123 Main

Bob Ramirez, 79 Oak

Carol Wilson, 821 Market

Where is *My* Vote?

Where is *My* Vote?

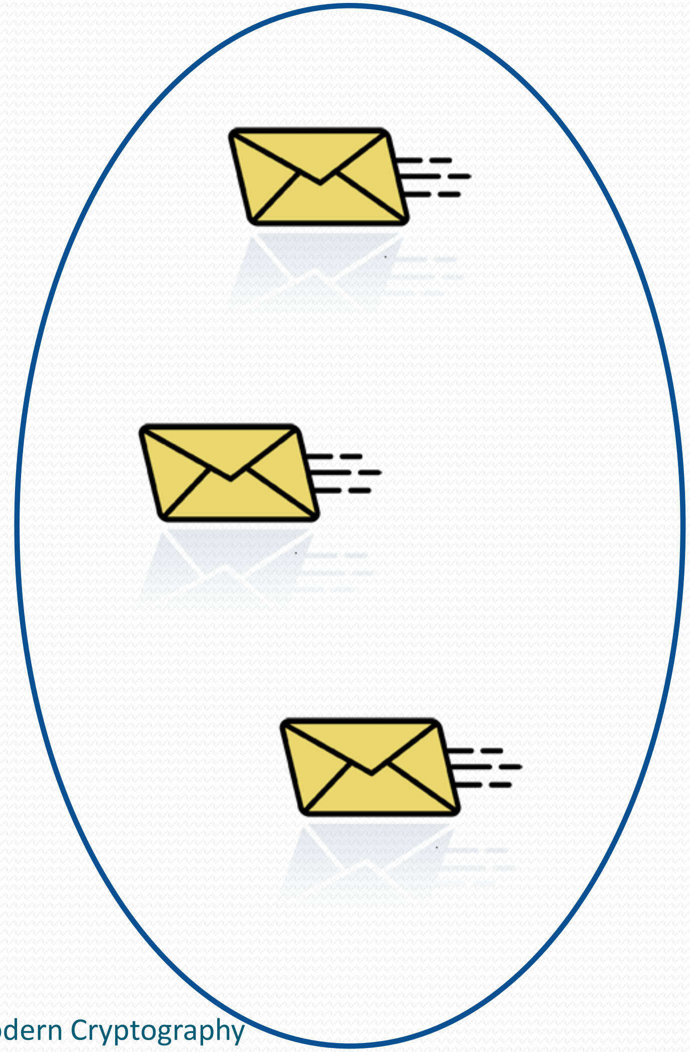


Where is *My* Vote?

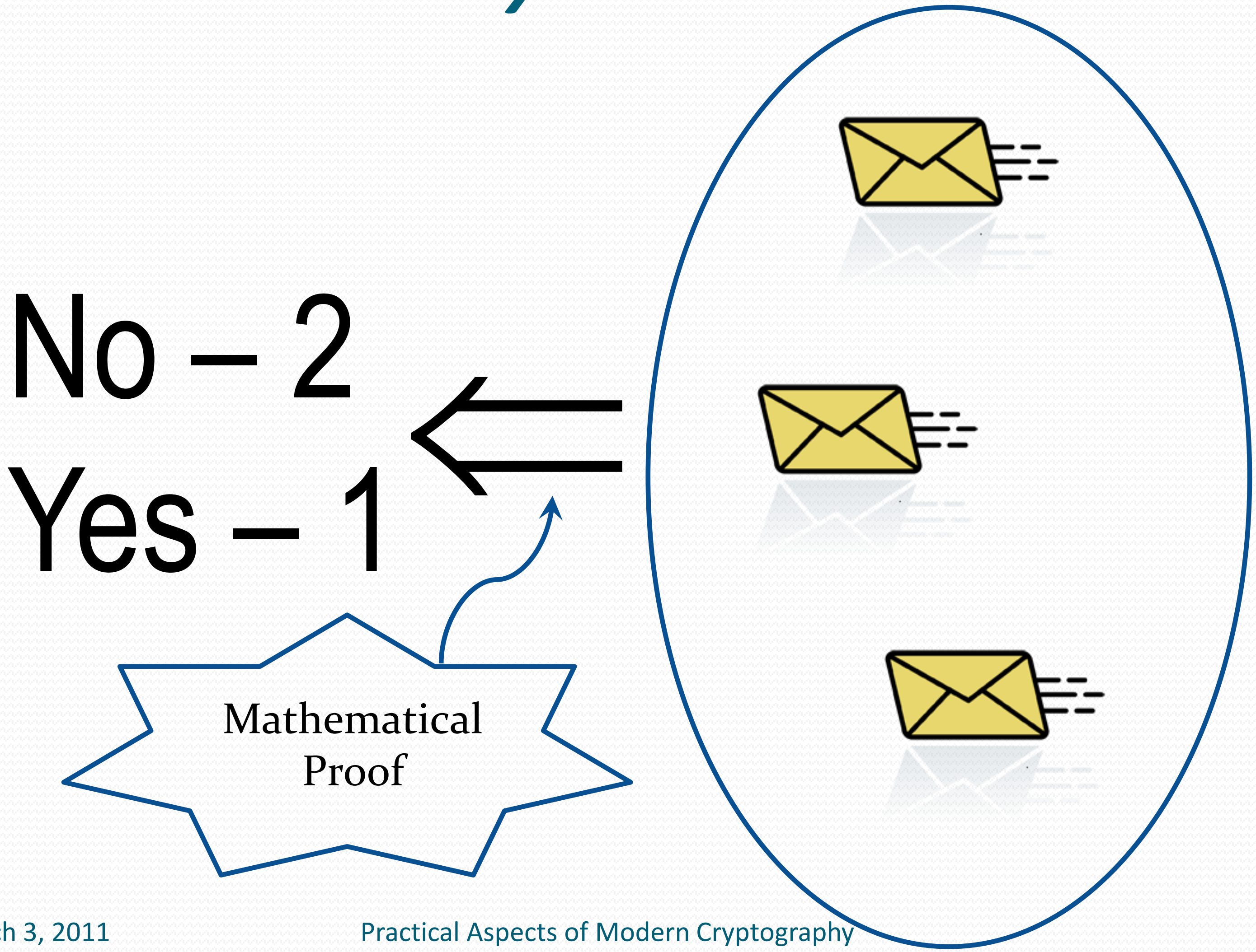
No – 2

Yes – 1

$\Longleftarrow$



Where is *My* Vote?



The Voter's Perspective

The Voter's Perspective

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

The Voter's Perspective

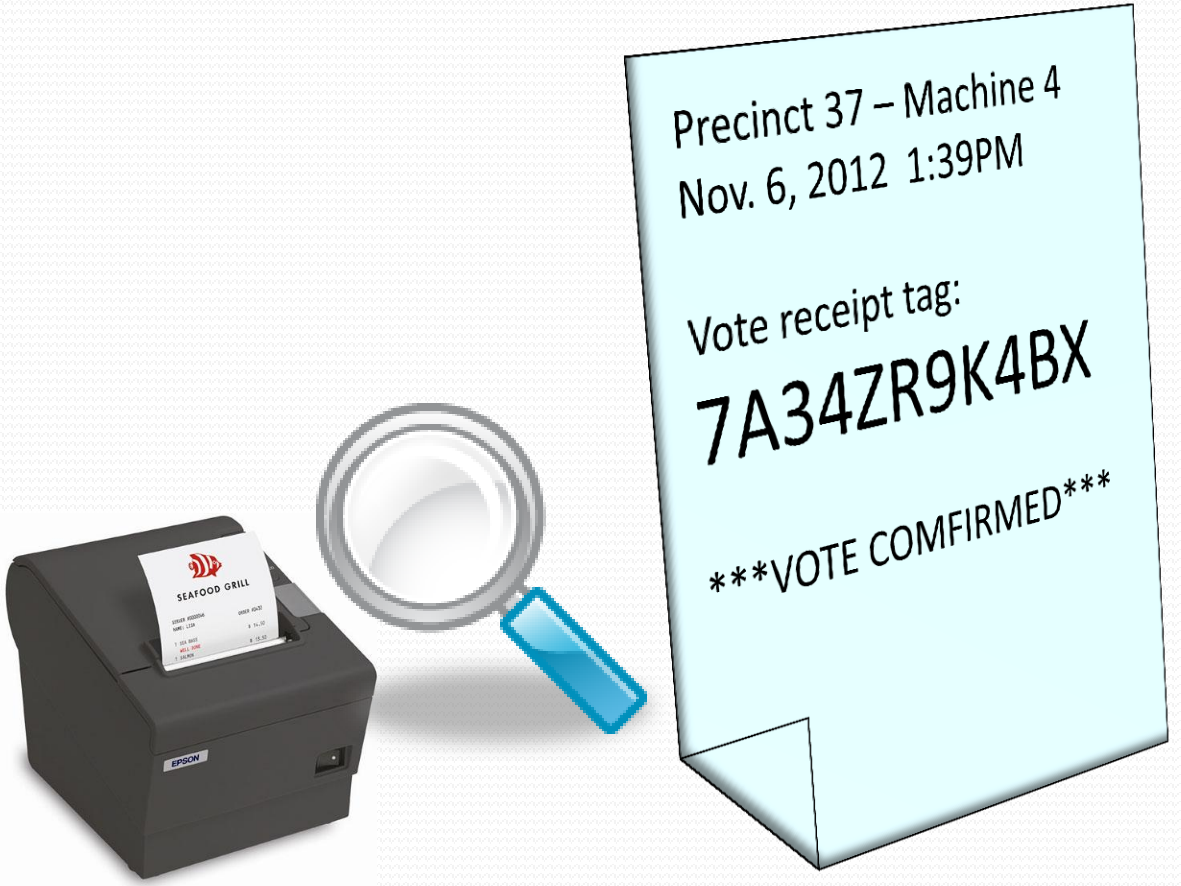
Verifiable election systems can be built to look exactly like current systems …

… with one addition …

A Verifiable Receipt

A Verifiable Receipt

A Verifiable Receipt



The Voter’s Perspective

The Voter's Perspective

Voters can …

The Voter’s Perspective

Voters can …

- Use receipts to check their results are properly recorded on a public web site.

The Voter's Perspective

Voters can …

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

The Voter’s Perspective

Voters can …

The Voter’s Perspective

Voters can …

- Write their own applications to verify the mathematical proof of the tally.

The Voter’s Perspective

Voters can …

- Write their own applications to verify the mathematical proof of the tally.
- Download verification apps from sources of their choice.

The Voter's Perspective

Voters can …

- Write their own applications to verify the mathematical proof of the tally.
- Download verification apps from sources of their choice.
- Believe verifications done by their political parties, LWV, ACLU, etc.

The Voter’s Perspective

Voters can …

- Write their own applications to verify the mathematical proof of the tally.
- Download verification apps from sources of their choice.
- Believe verifications done by their political parties, LWV, ACLU, etc.
- Accept the results without question.

So How Does It Work?

Secure MPC is *not* Enough

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.

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 …

End-to-End Verifiable Elections

Two principle phases …

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

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.

End-to-End Verifiable Elections

Two questions must be answered …

End-to-End Verifiable Elections

Two questions must be answered …

- How do voters turn their preferences into encrypted votes?

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?

Is it *Really* This Easy?

Yes …

Is it *Really* This Easy?

Yes …

… but there are lots of details to get right.

Fundamental Tallying Decision

Fundamental Tallying Decision

There are essentially two paradigms to choose from …

Fundamental Tallying Decision

There are essentially two paradigms to choose from …

- Anonymized Ballots

Fundamental Tallying Decision

There are essentially two paradigms to choose from …

- Anonymized Ballots

  (Mix Networks)

Fundamental Tallying Decision

There are essentially two paradigms to choose from …

- Anonymized Ballots

  (Mix Networks)

- Ballotless Tallying

Fundamental Tallying Decision

There are essentially two paradigms to choose from …

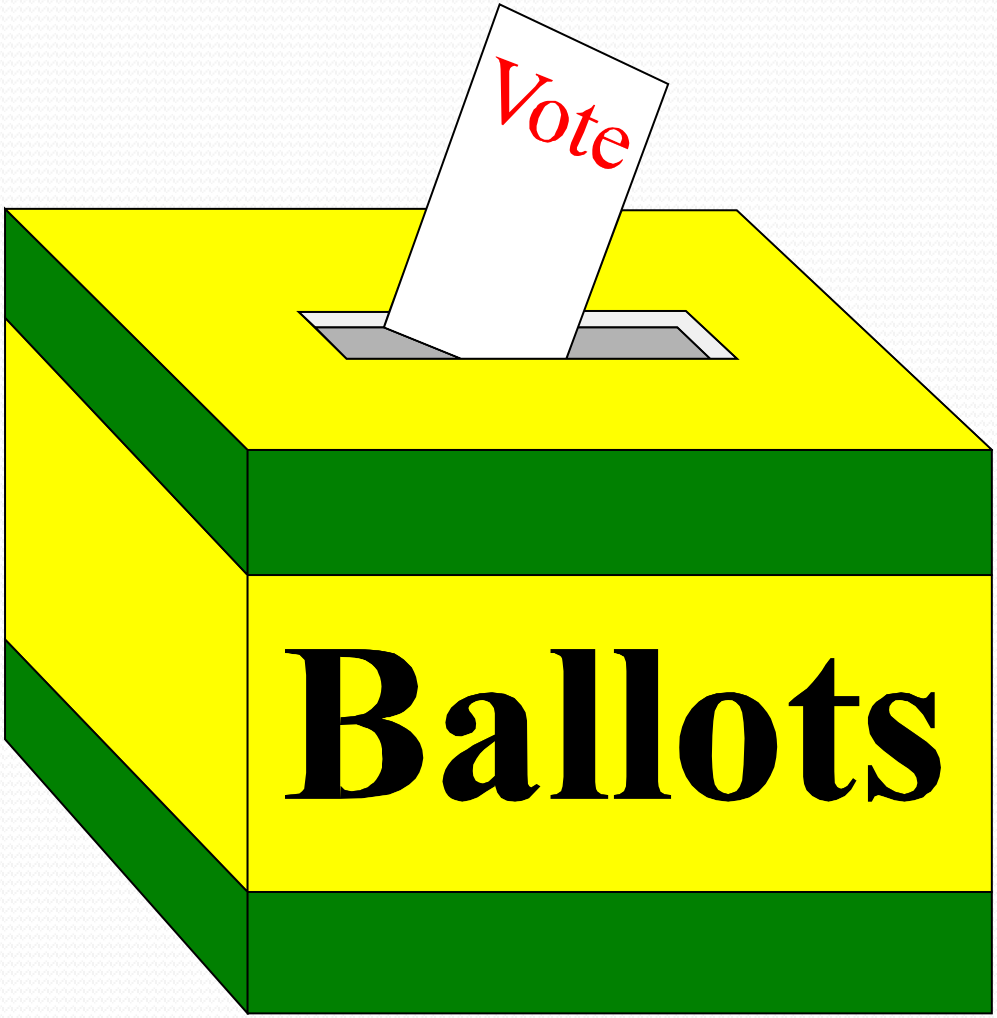
- Anonymized Ballots

  (Mix Networks)

- Ballotless Tallying

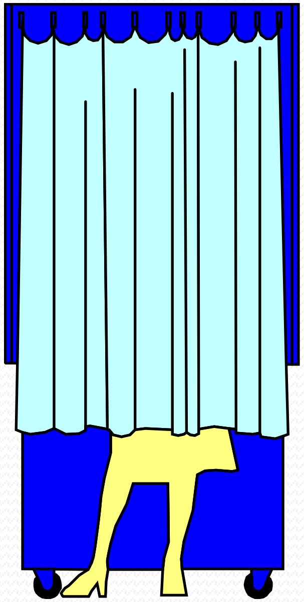
  (Homomorphic Encryption)

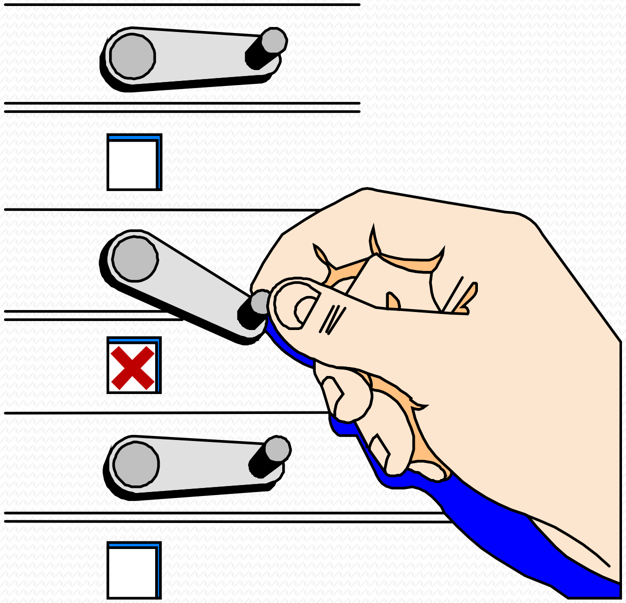
Anonymized Ballots



Ballotless Tallying

Homomorphic Tallying





Homomorphic Encryption

Some Homomorphic Functions

- RSA: $E(m) = me \bmod n$
- ElGamal: $E(m, r) = (g^r, mhr) \bmod p$
- 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

Homomorphic Encryption

The *product* of the *encryptions* of the votes constitutes an *encryption* of the *sum* of the votes.

Multiple Authorities

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

Multiple Authorities

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

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

Double Commutivity

The *product* of the *encryptions* of the *shares* of the votes constitute an *encryption* of a *share* the *sum* of the votes.

Robust Sharing

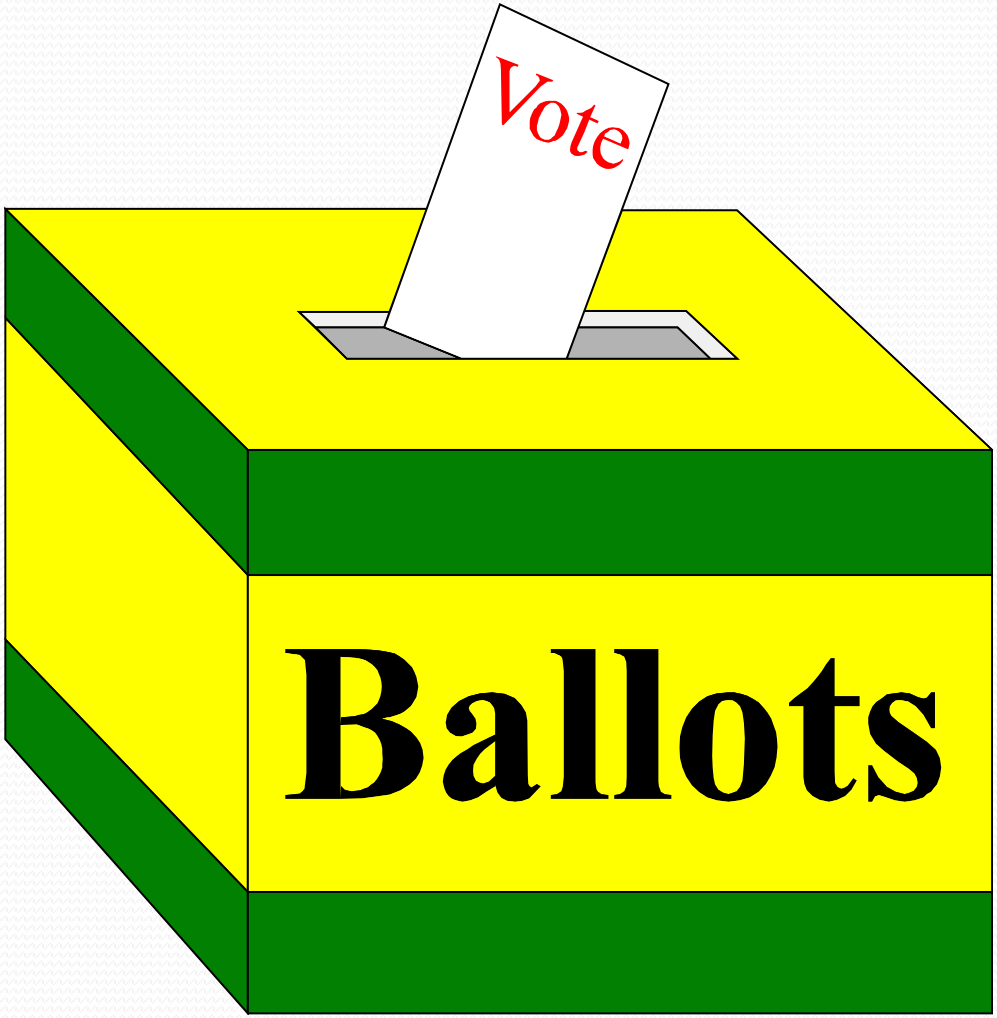
Robust Sharing

- Note that votes can be “shared” with a polynomial threshold scheme instead of a simple sum.

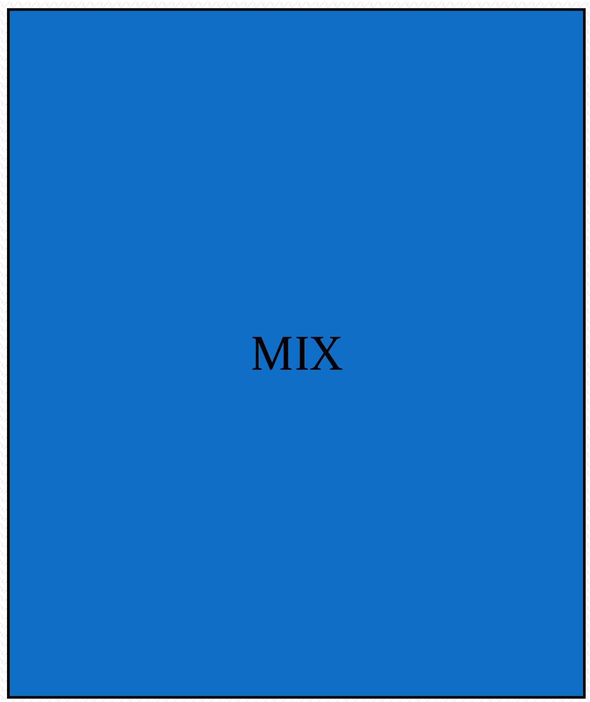
Robust Sharing

- Note that votes can be “shared” with a polynomial threshold scheme instead of a simple sum.
- This provides robustness in case one or more trustees fails to properly decrypt their shares.

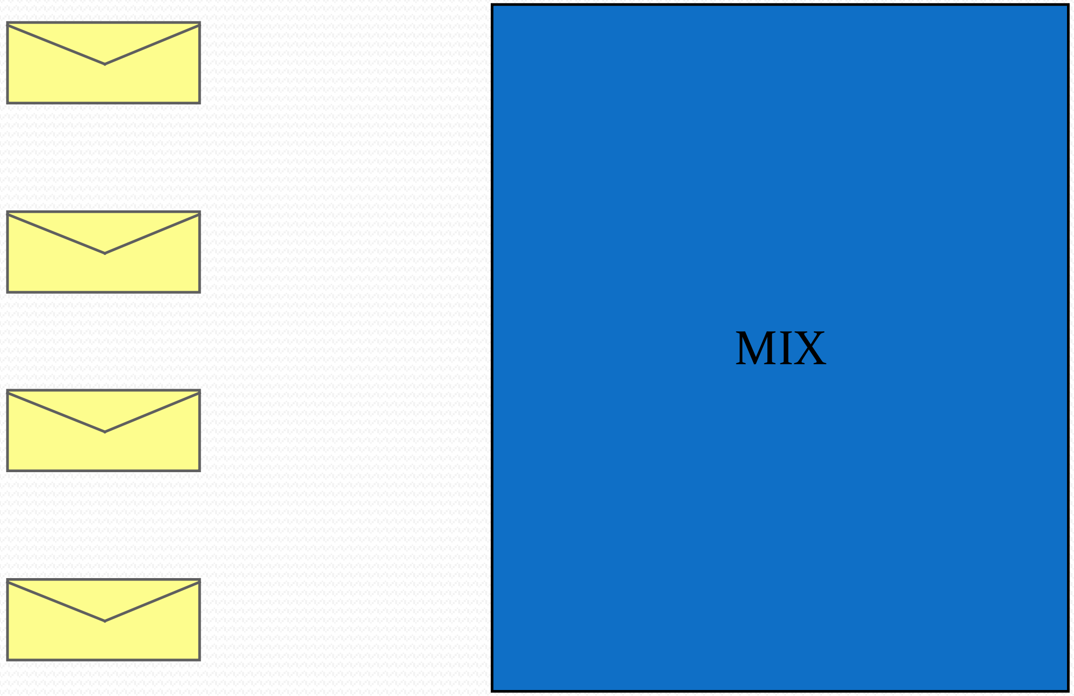
Mix-Based Elections



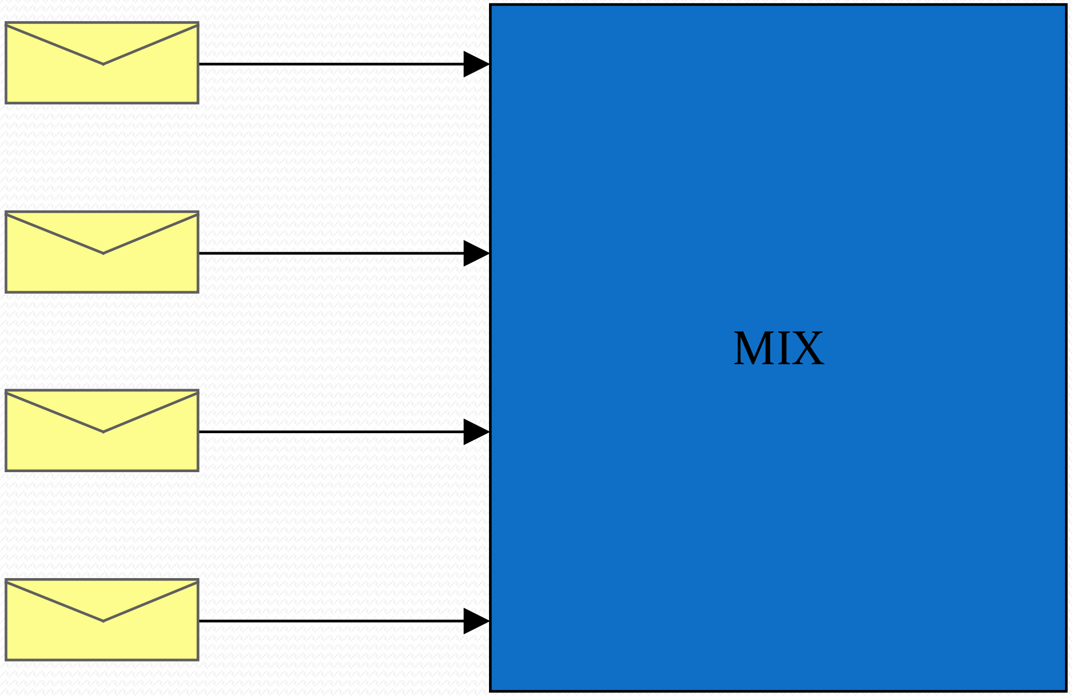
The Mix-Net Paradigm



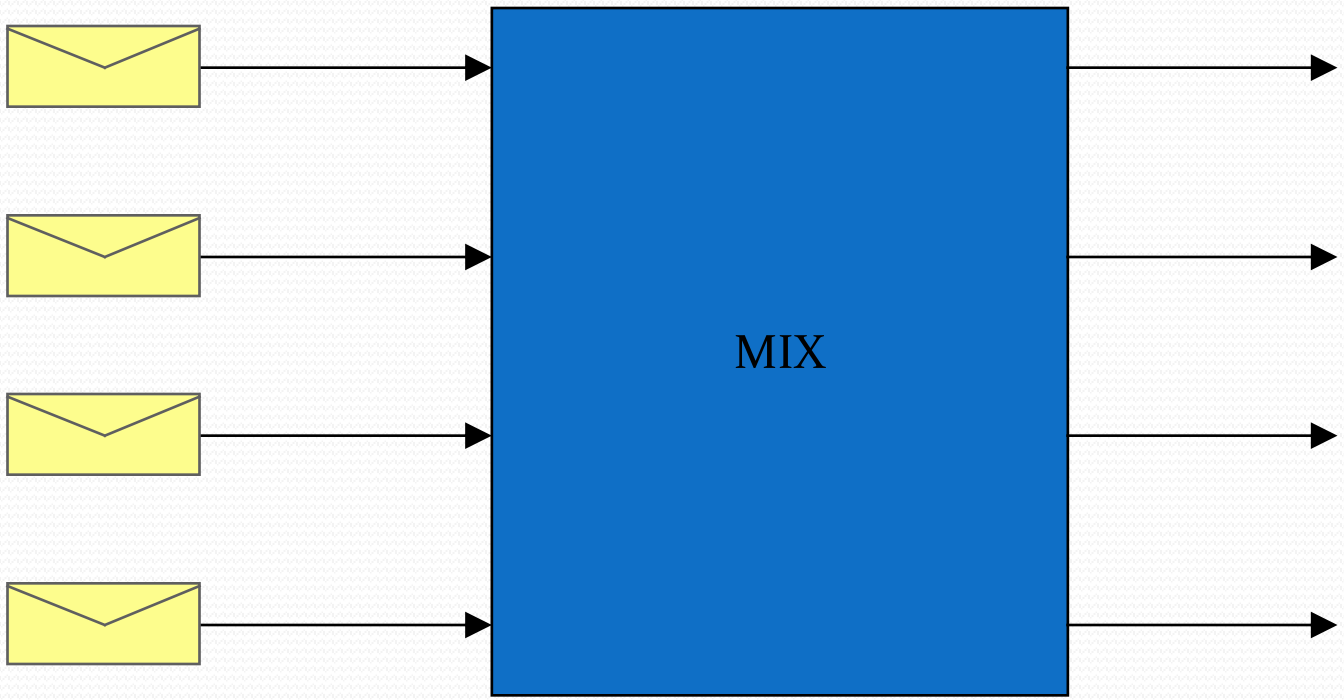
The Mix-Net Paradigm



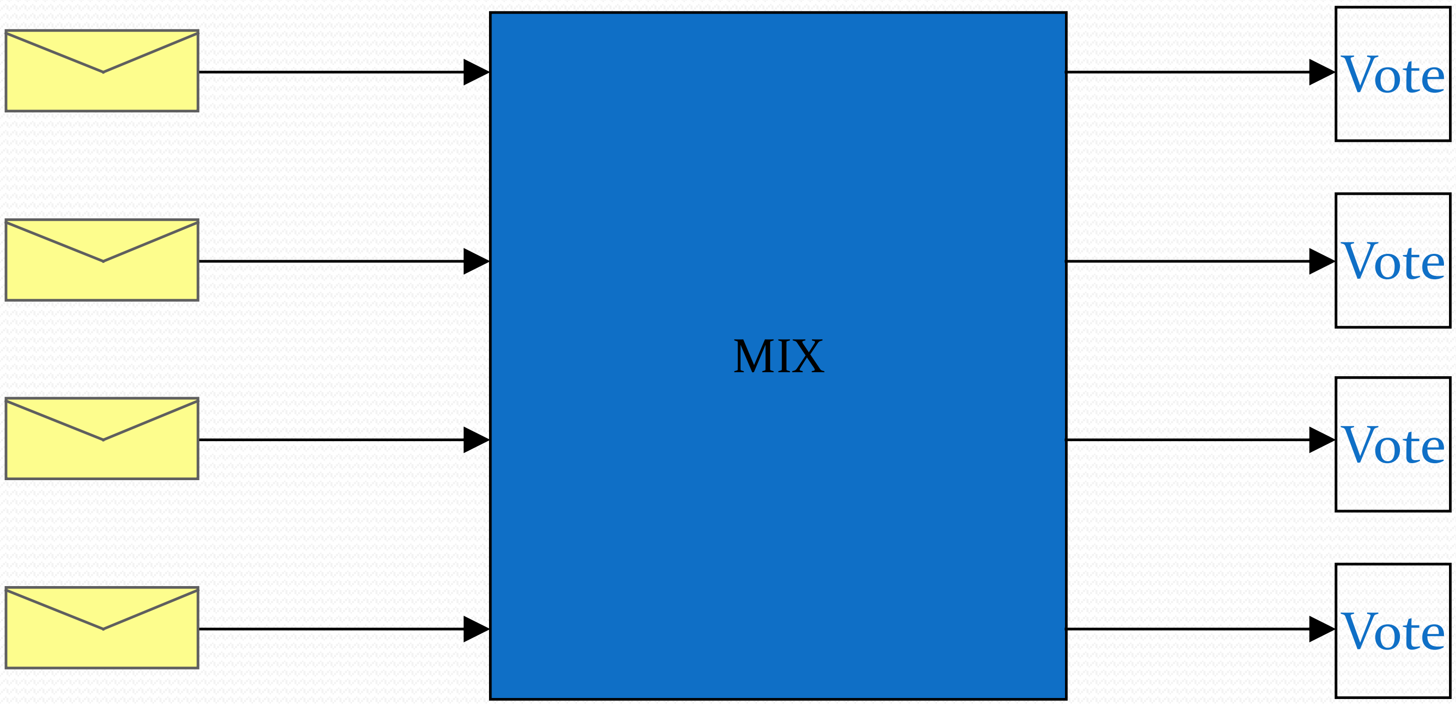
The Mix-Net Paradigm



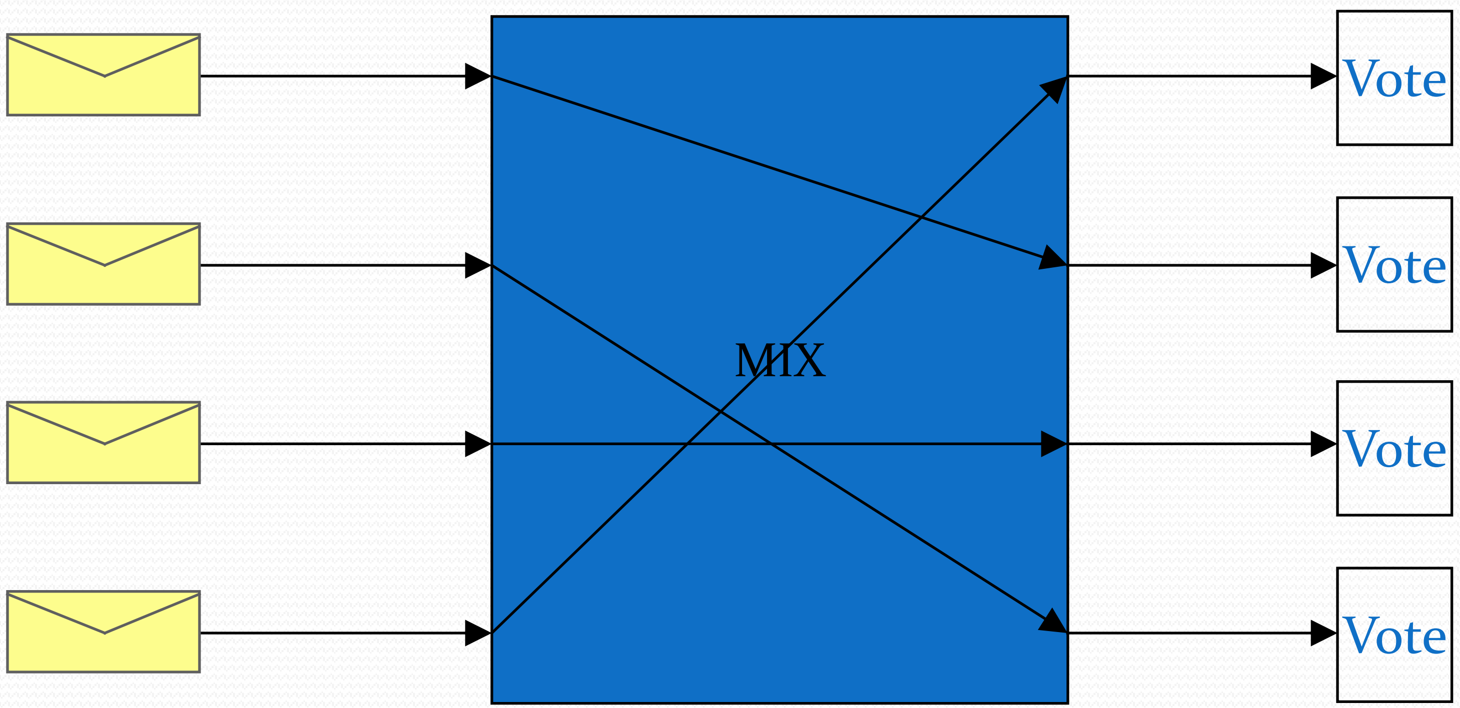
The Mix-Net Paradigm



The Mix-Net Paradigm

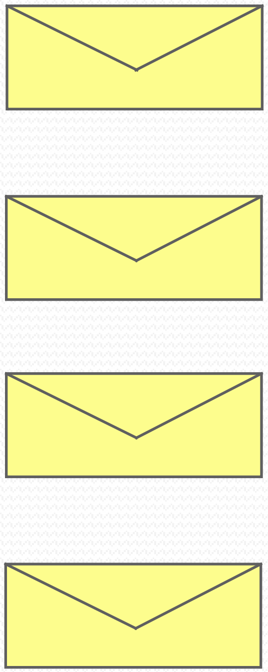


The Mix-Net Paradigm

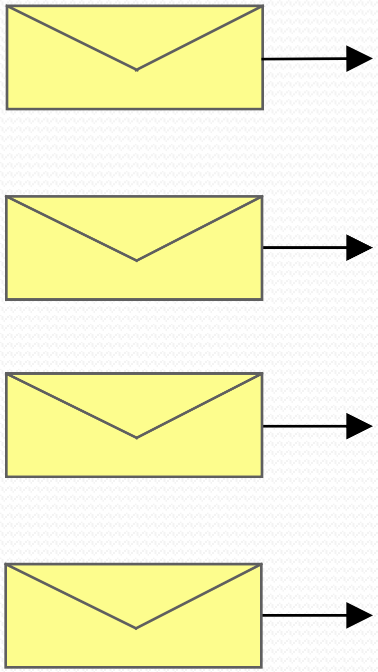


Multiple Mixes

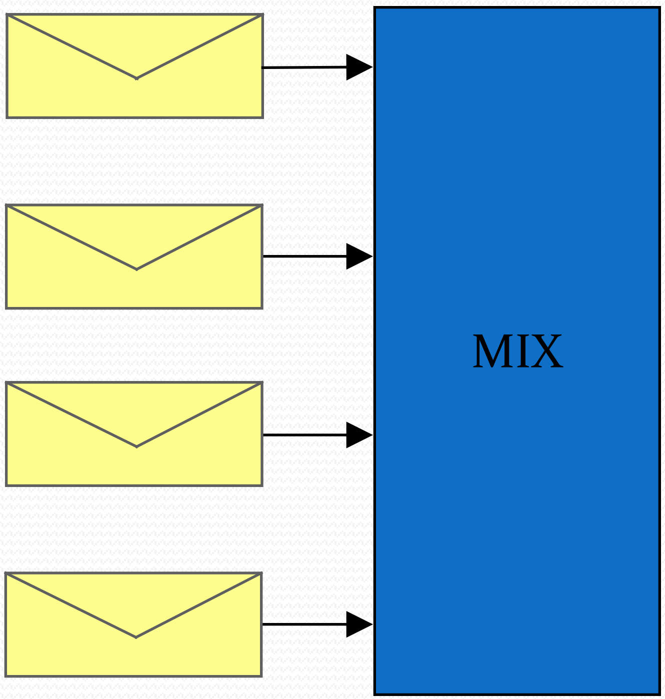
Multiple Mixes



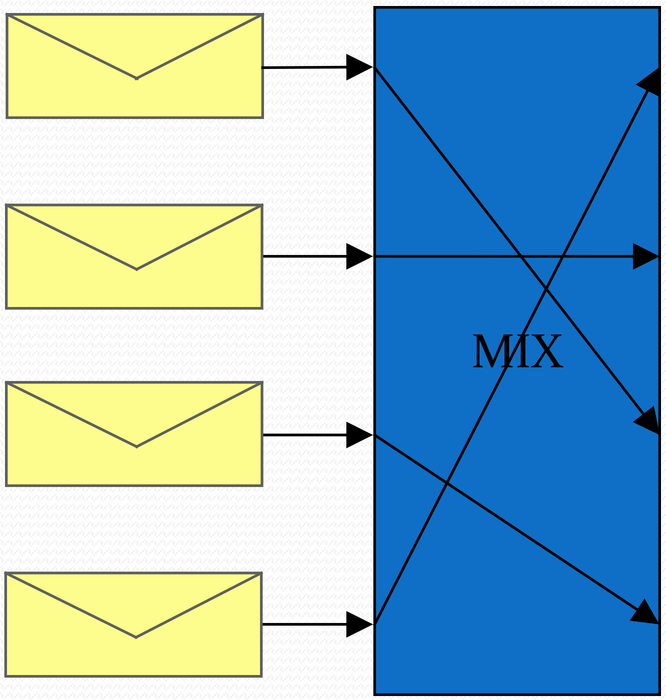
Multiple Mixes



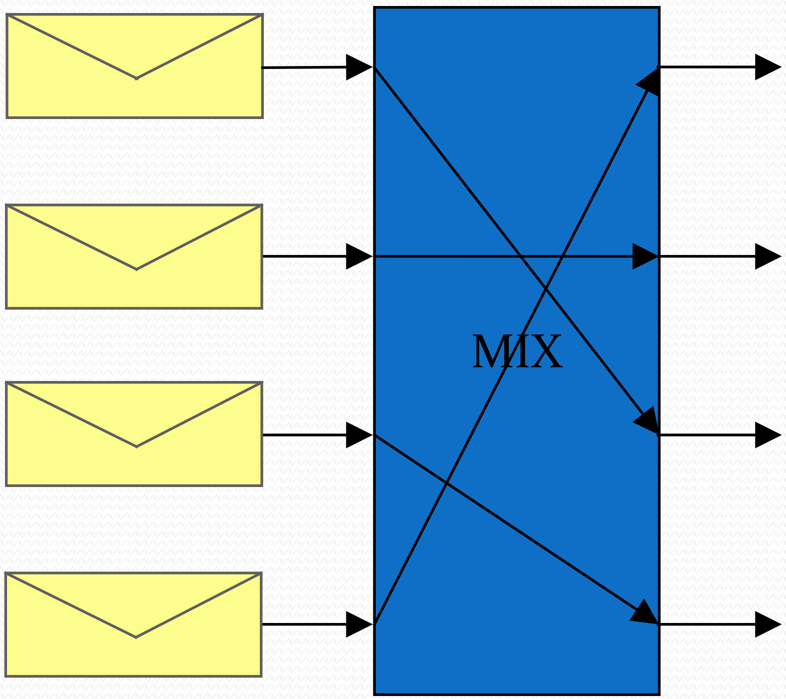
Multiple Mixes



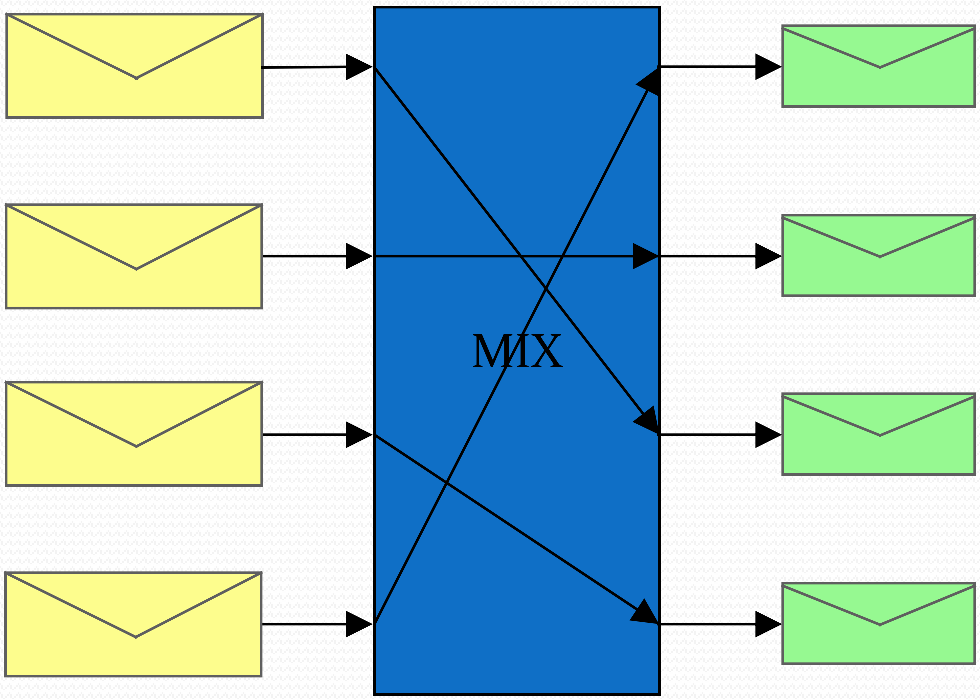
Multiple Mixes



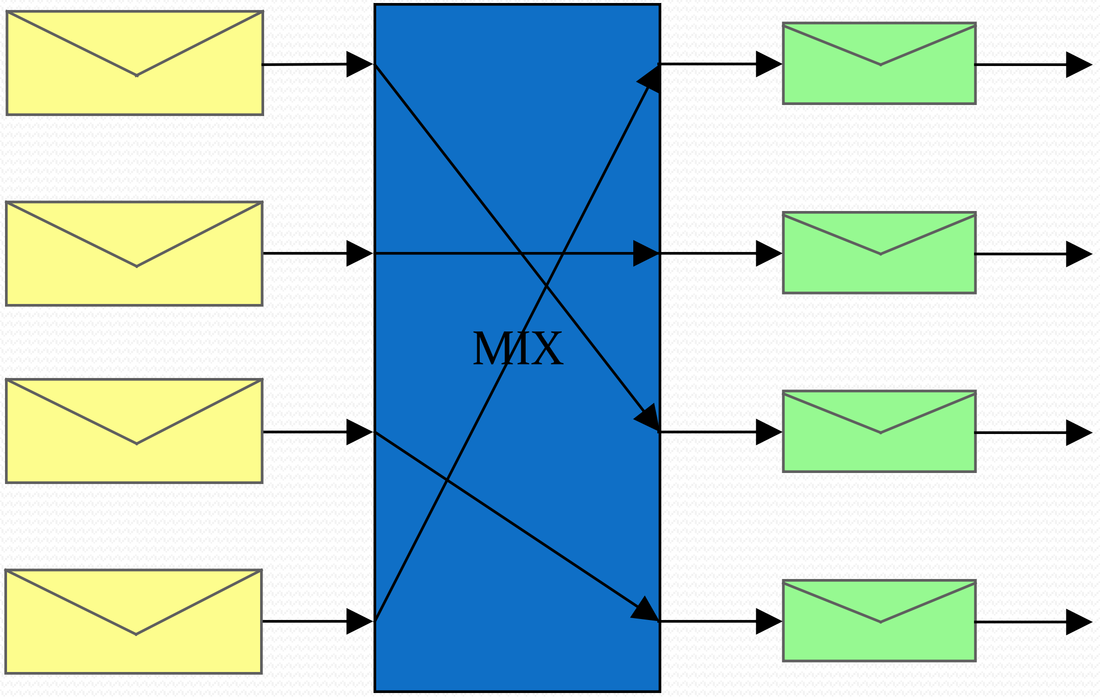
Multiple Mixes



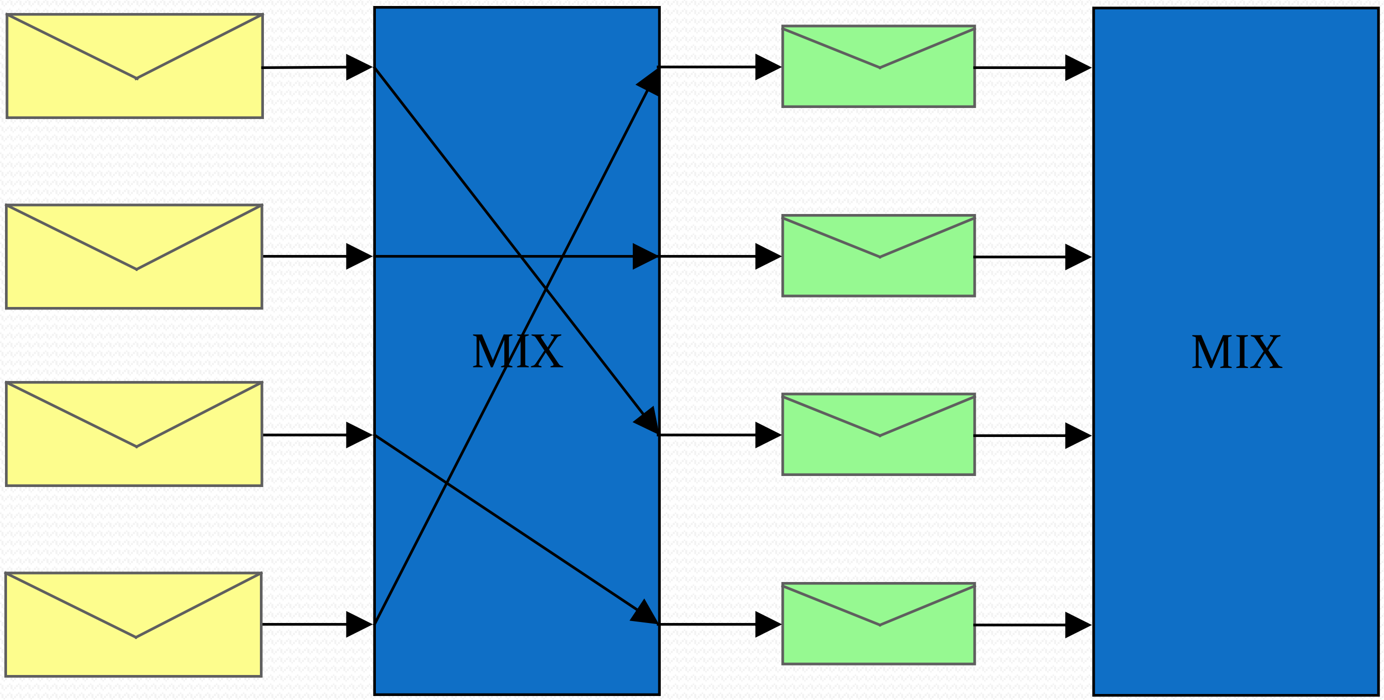
Multiple Mixes



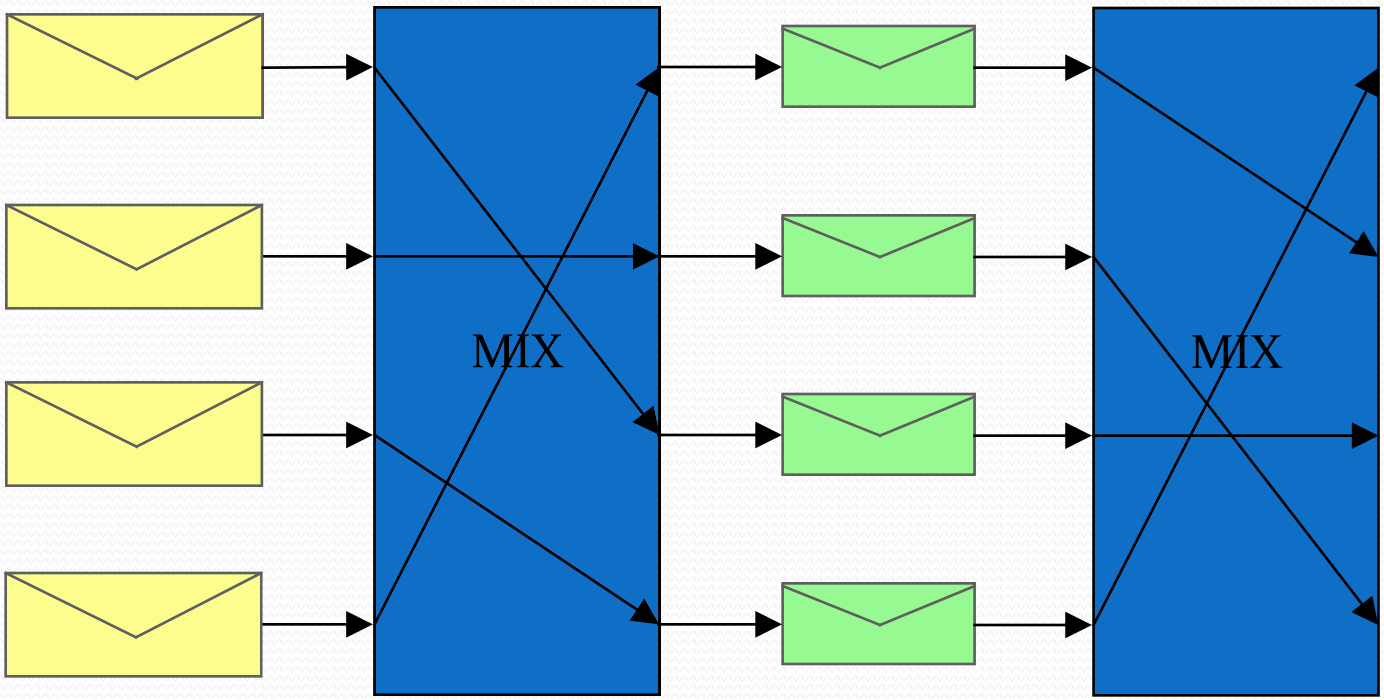
Multiple Mixes



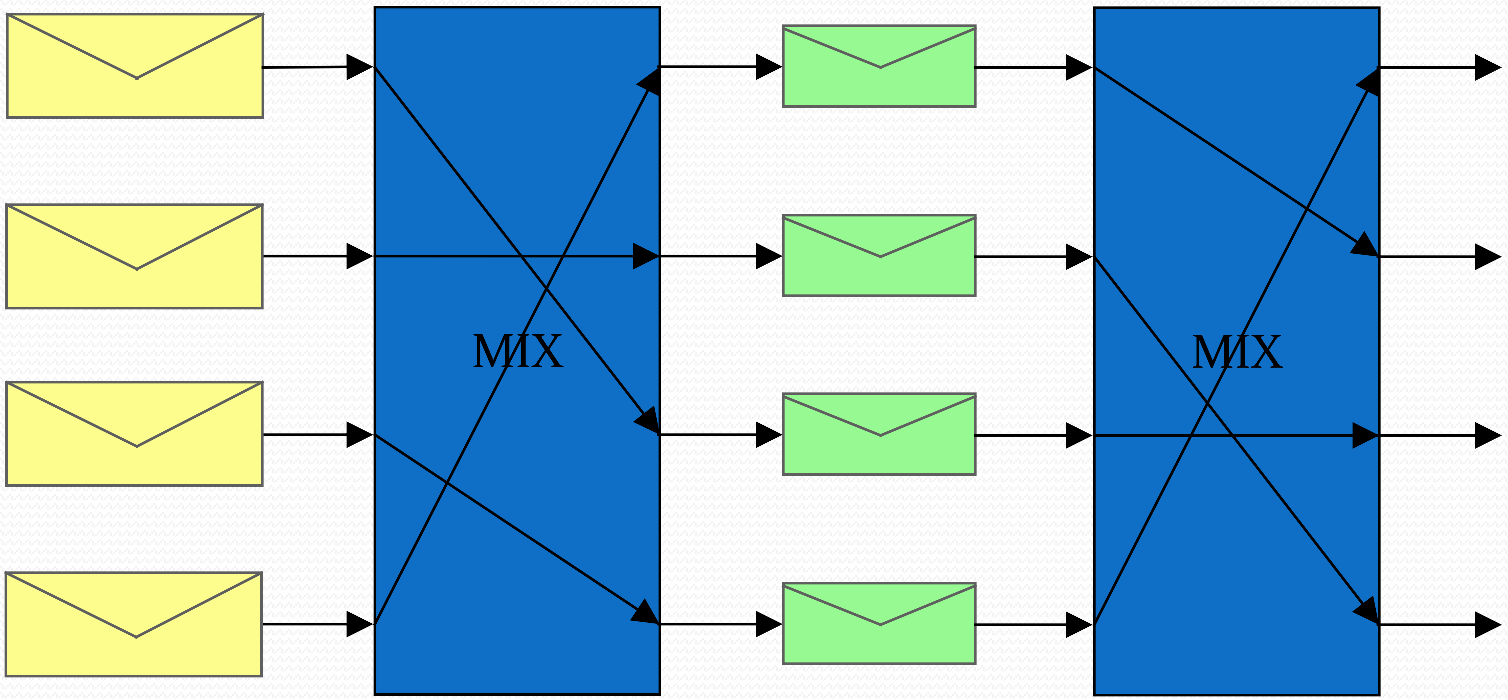
Multiple Mixes



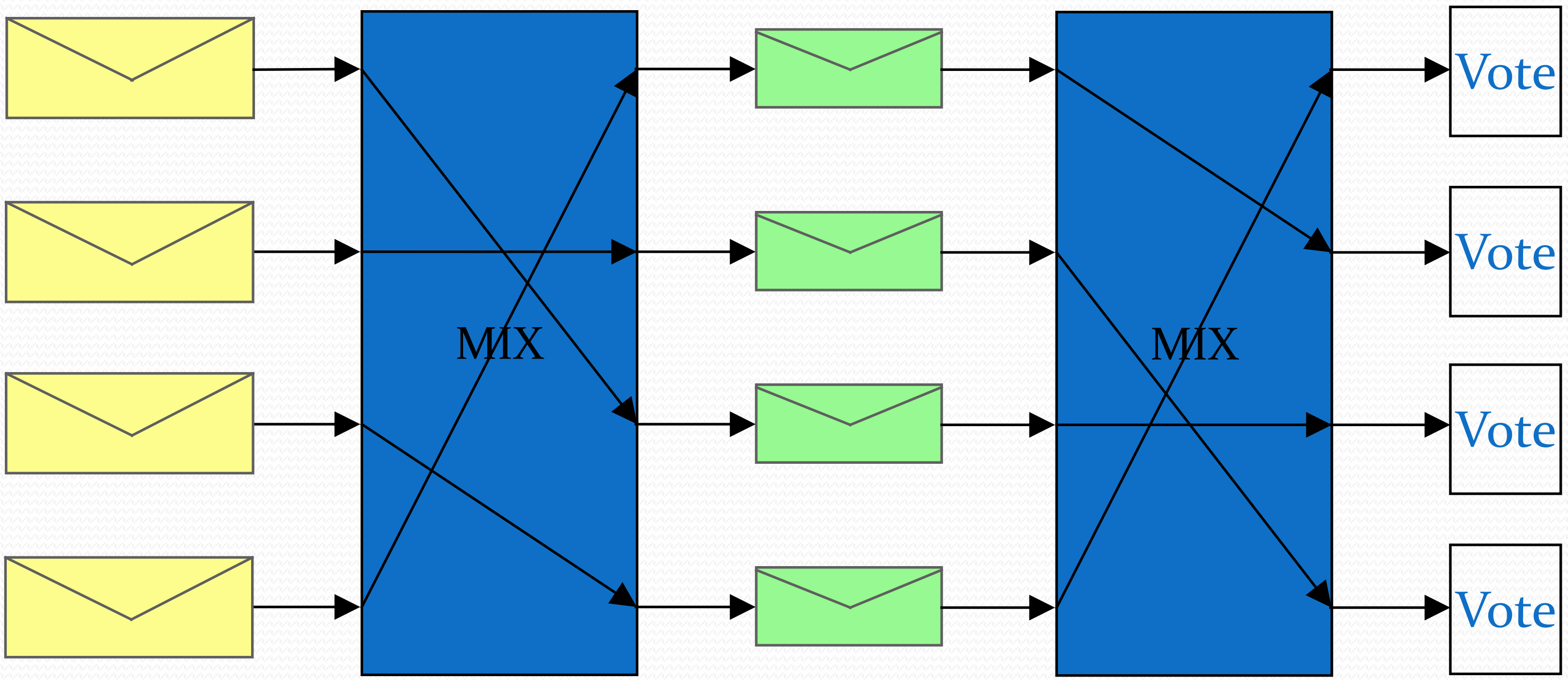
Multiple Mixes



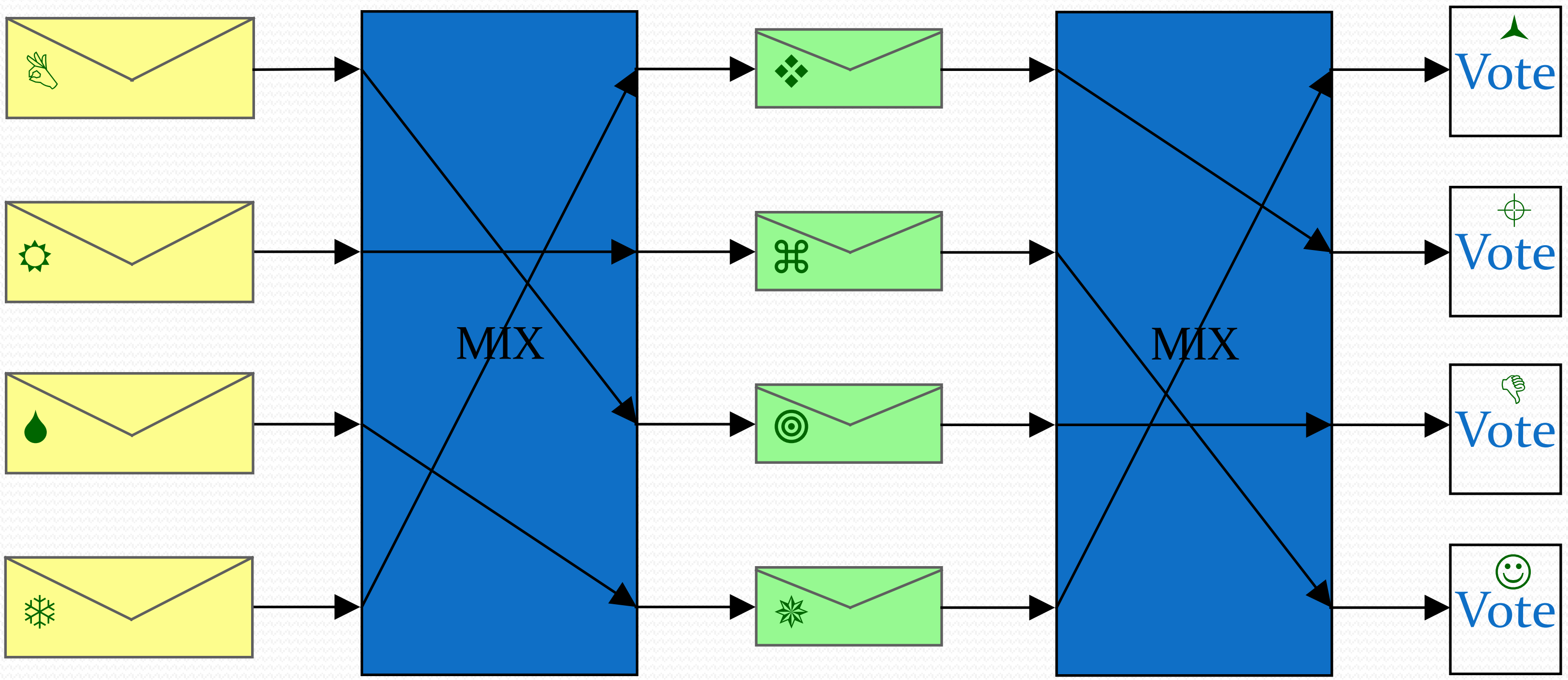
Multiple Mixes



Multiple Mixes



Multiple Mixes



Decryption Mix-net

Decryption Mix-net

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

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

Re-encryption Mix-net

The decryption and shuffling functions are decoupled.

Re-encryption Mix-net

The decryption and shuffling functions are decoupled.

Mixes can be added or removed dynamically with robustness.

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.

More 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

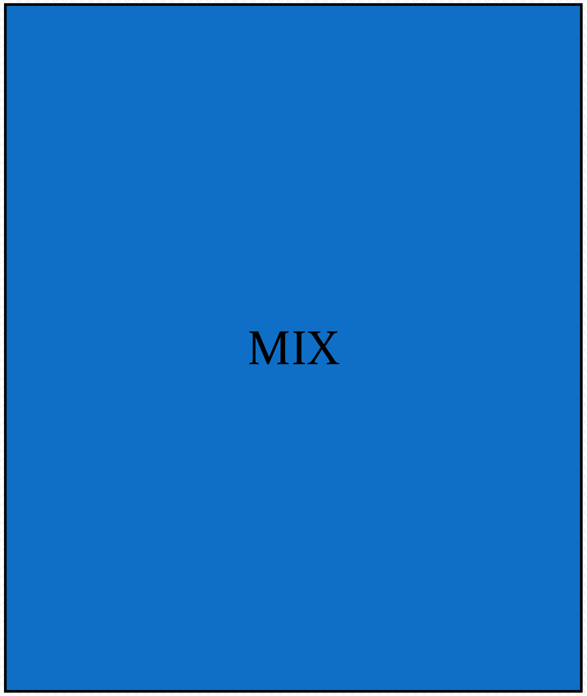
Z is *an* encryption of 0 then

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

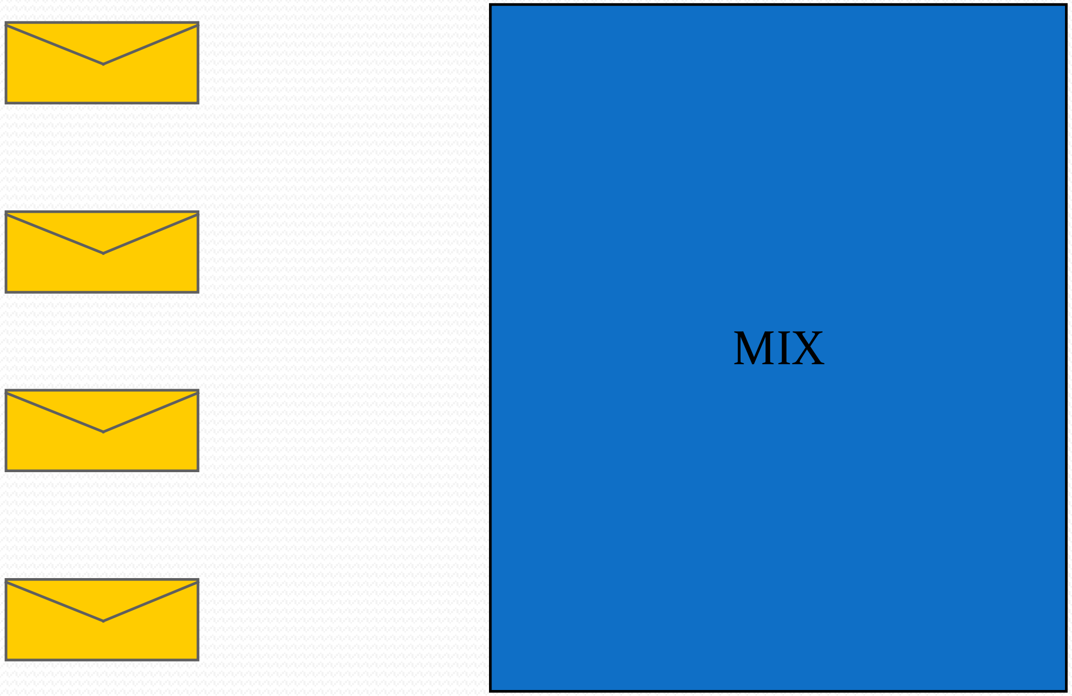
Re-encryption (multiplicative)

A is *an* encryption of a and
I is *an* encryption of 1 then
$A \otimes I$ is *another* encryption of a.

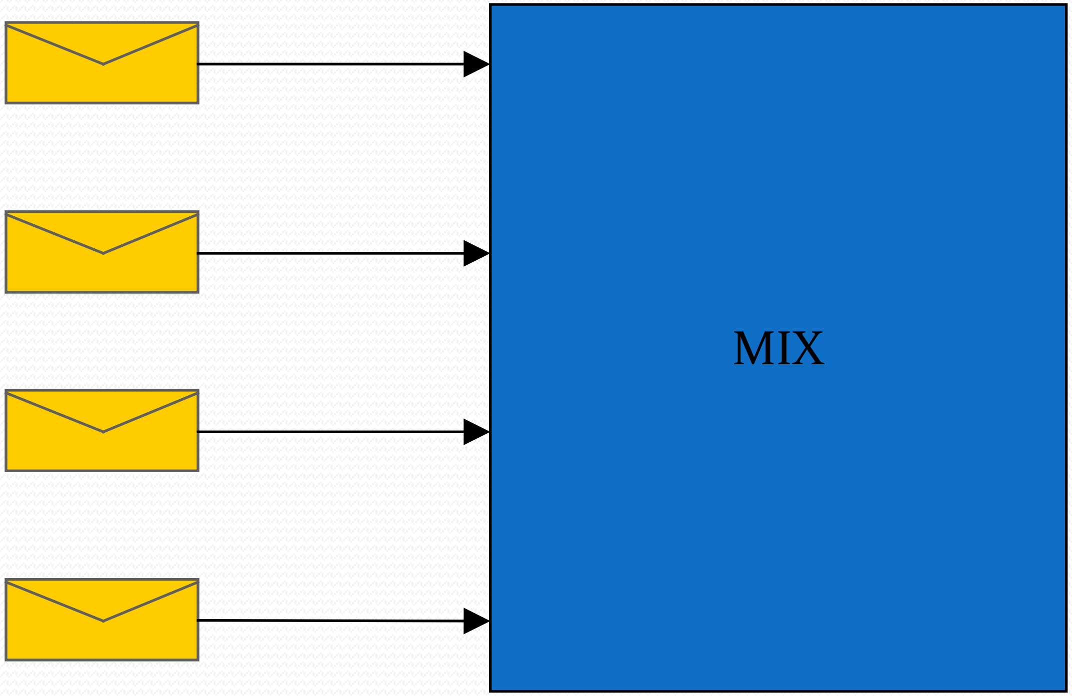
A Re-encryption Mix



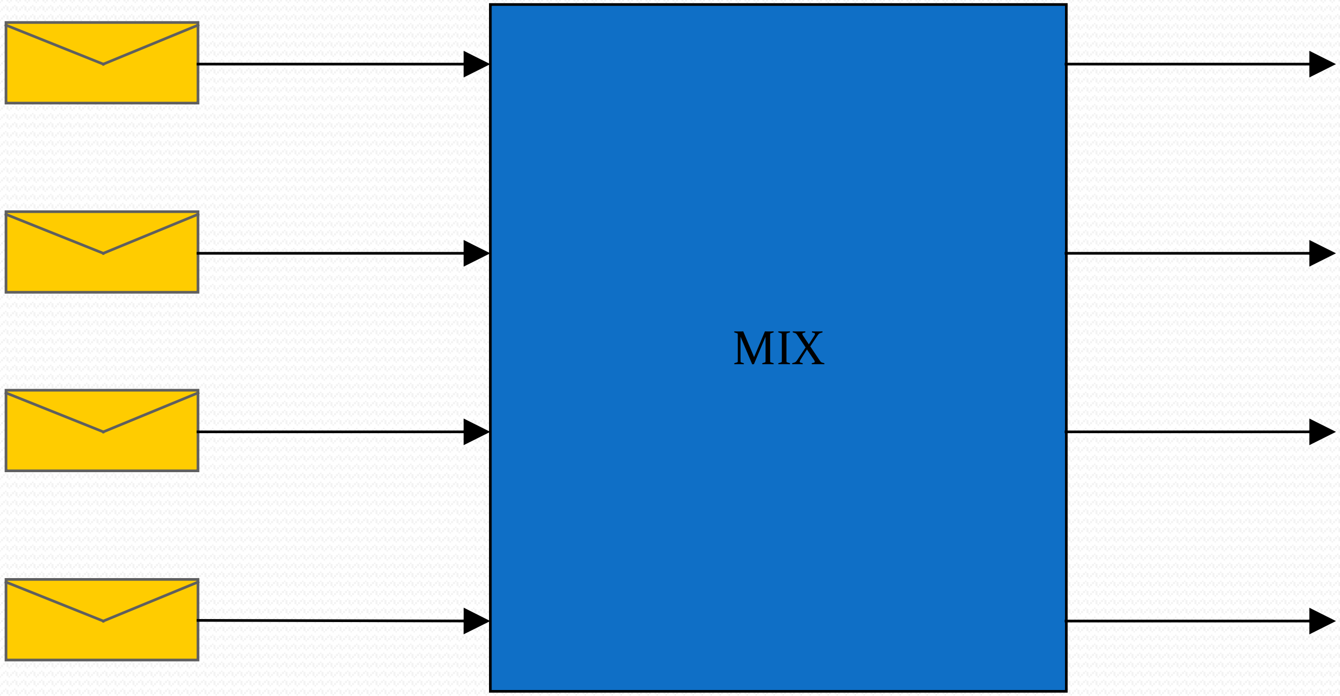
A Re-encryption Mix



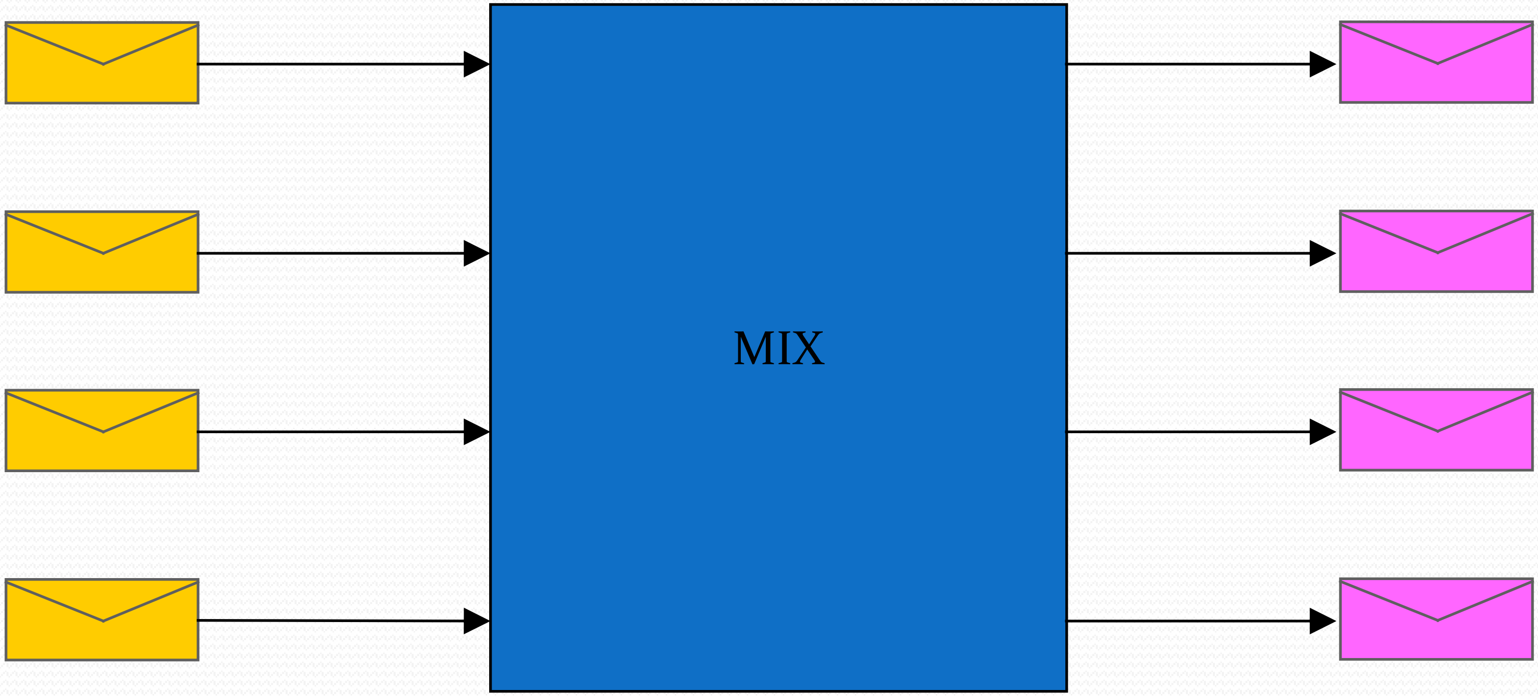
A Re-encryption Mix



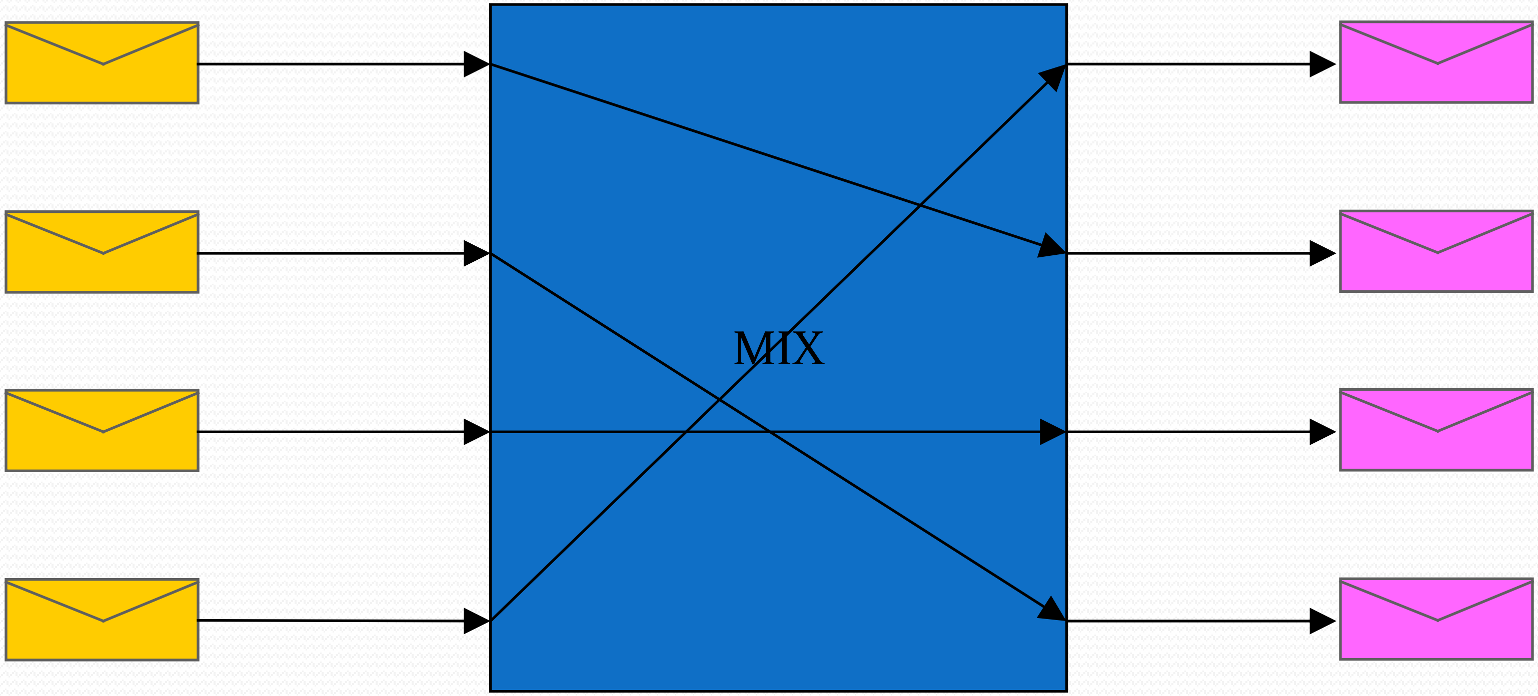
A Re-encryption Mix



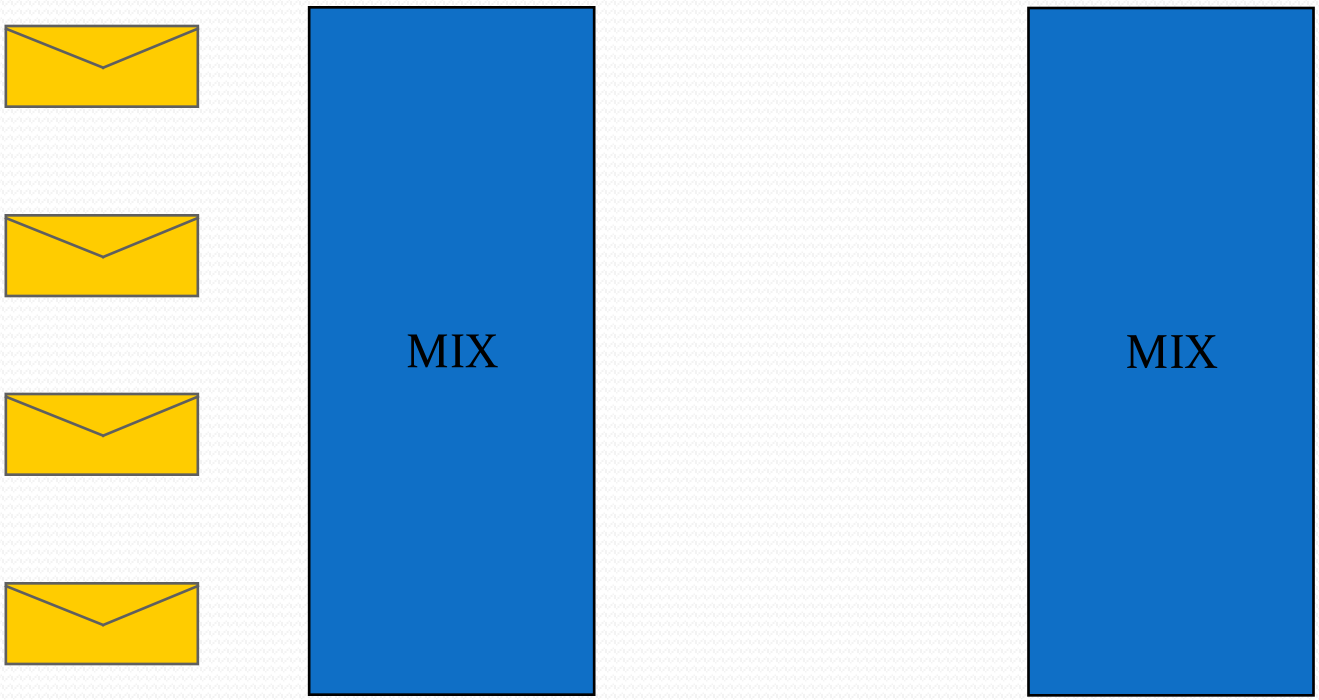
A Re-encryption Mix



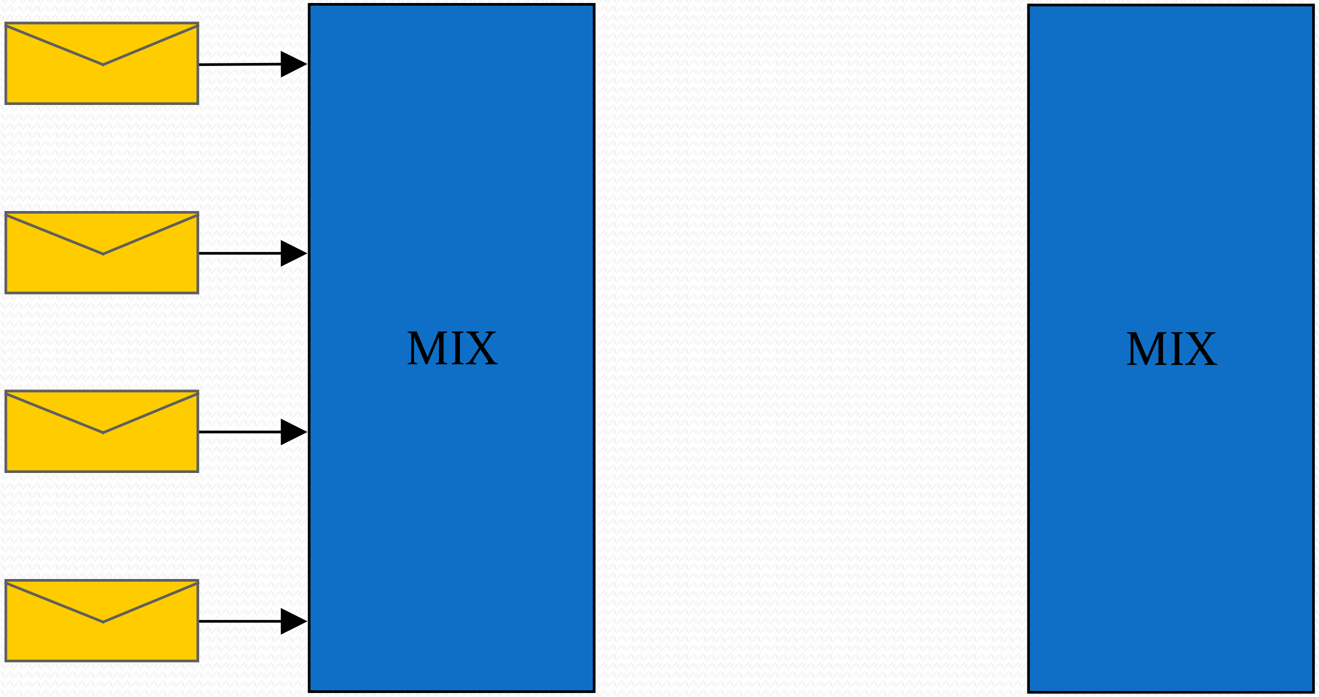
A Re-encryption Mix



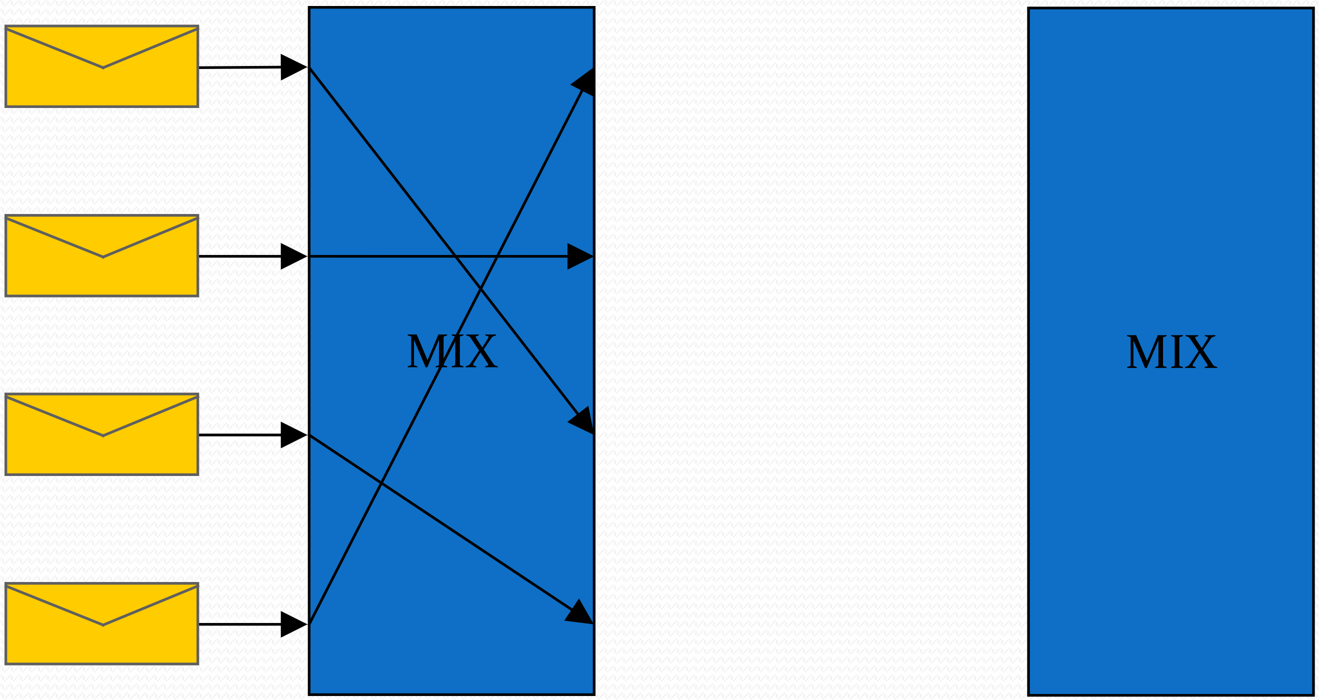
Re-encryption Mix-nets



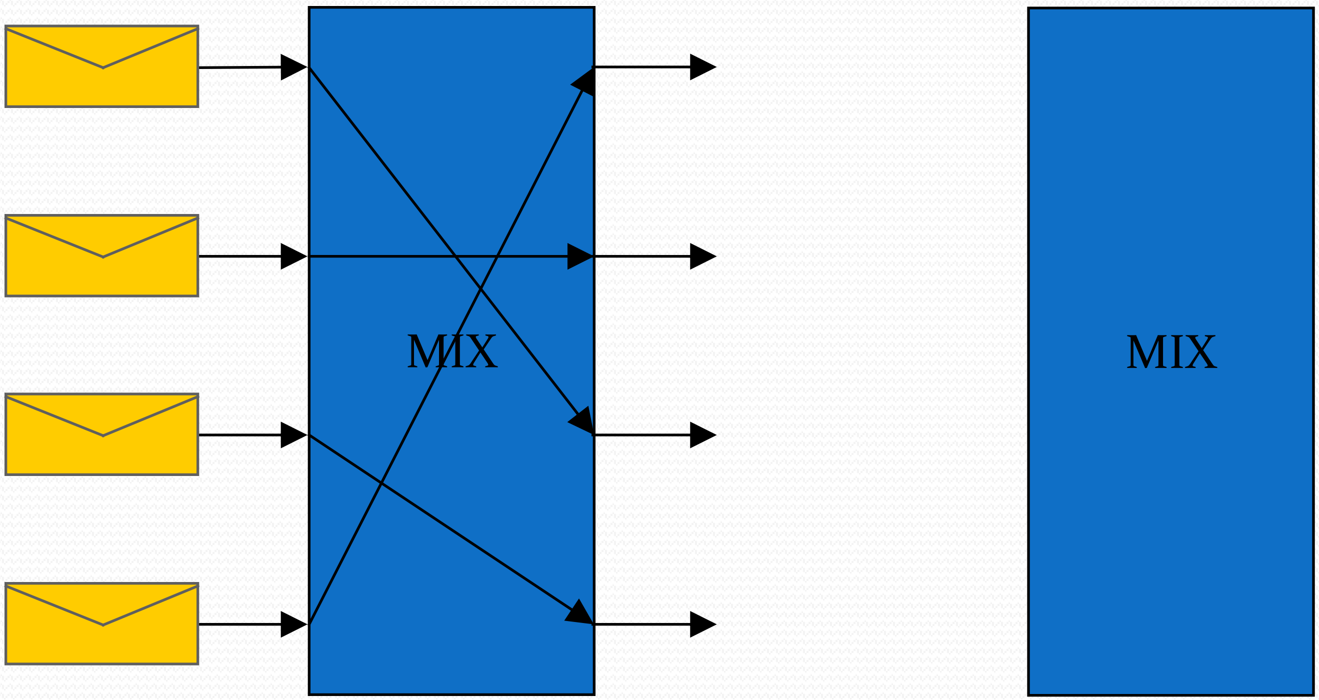
Re-encryption Mix-nets



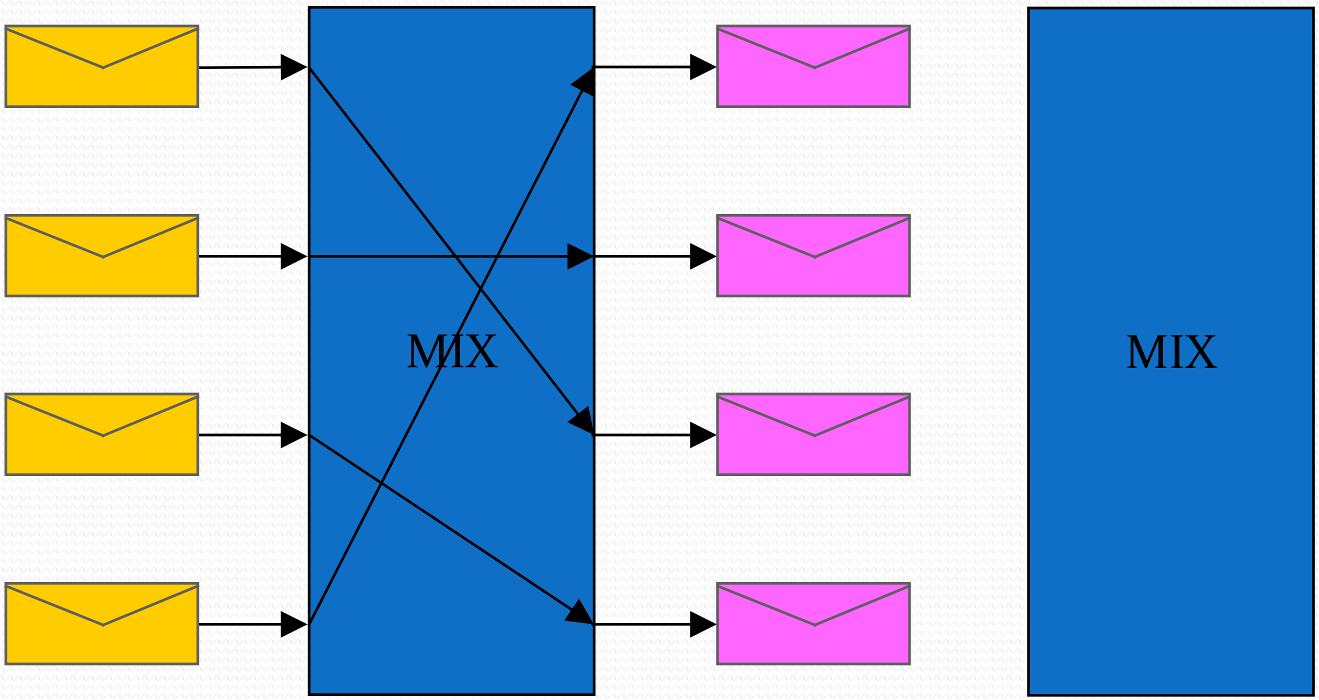
Re-encryption Mix-nets



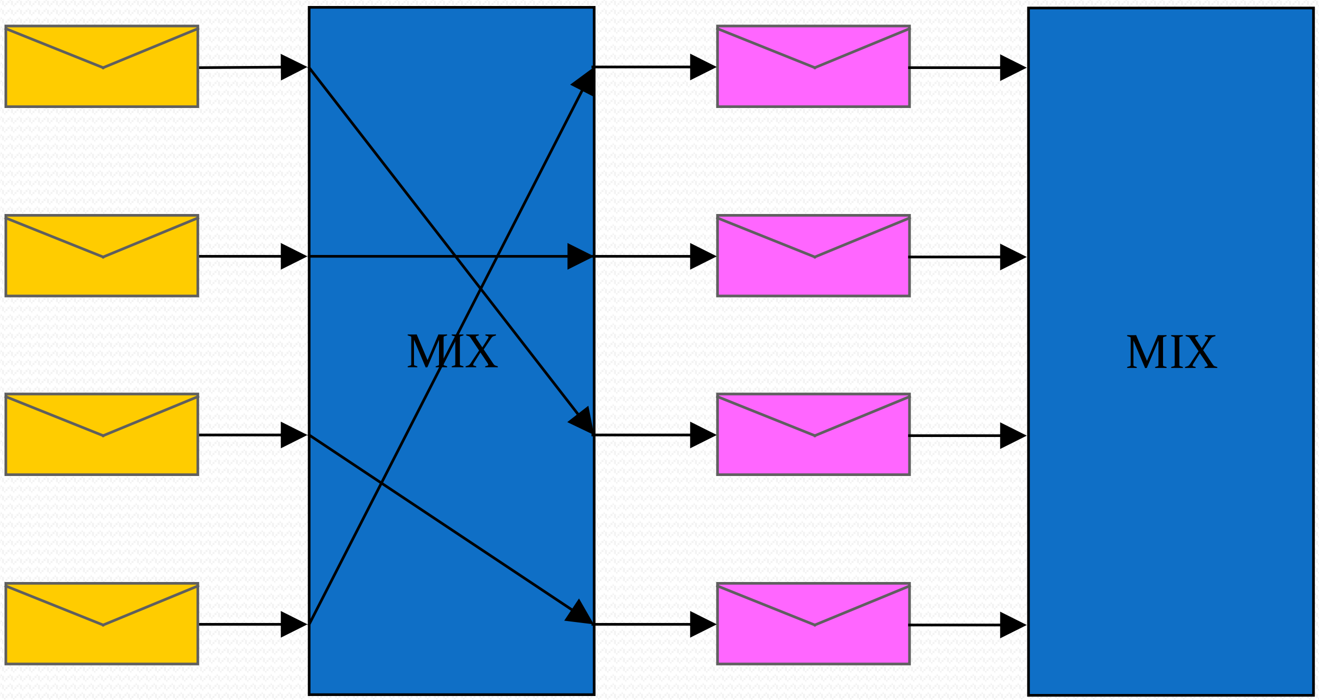
Re-encryption Mix-nets



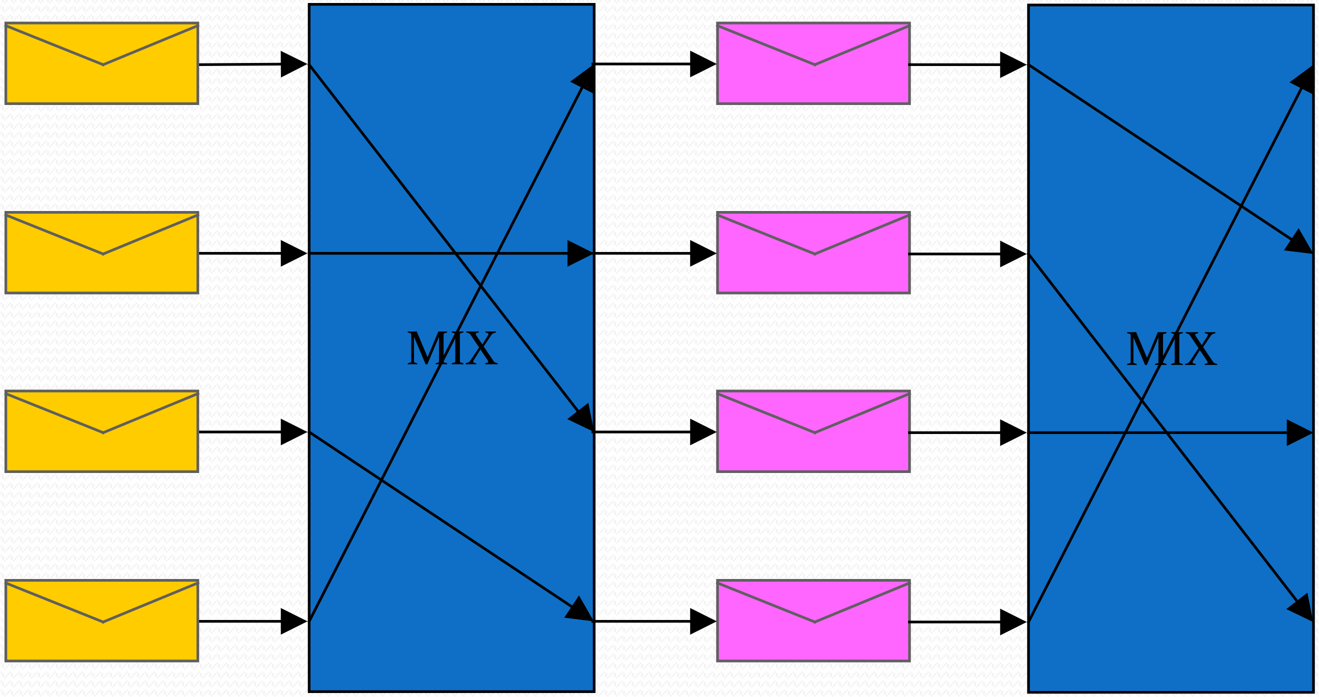
Re-encryption Mix-nets



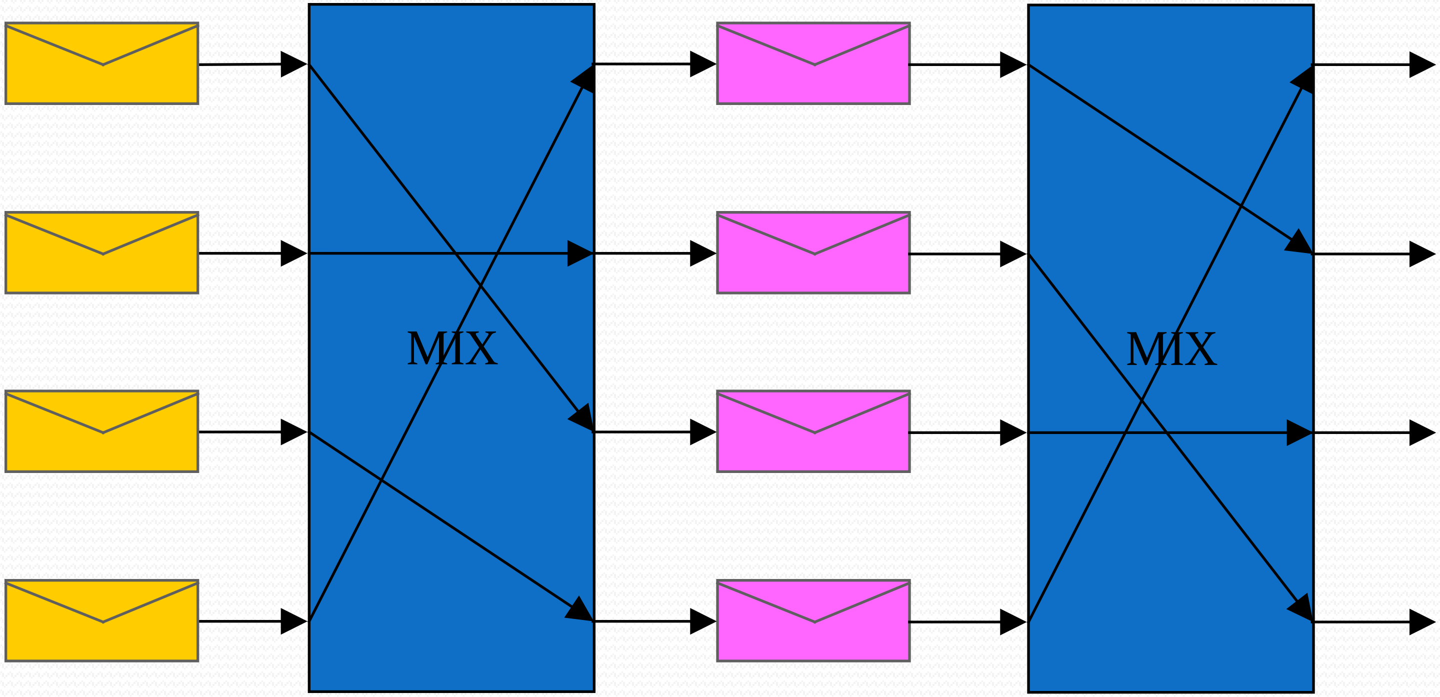
Re-encryption Mix-nets



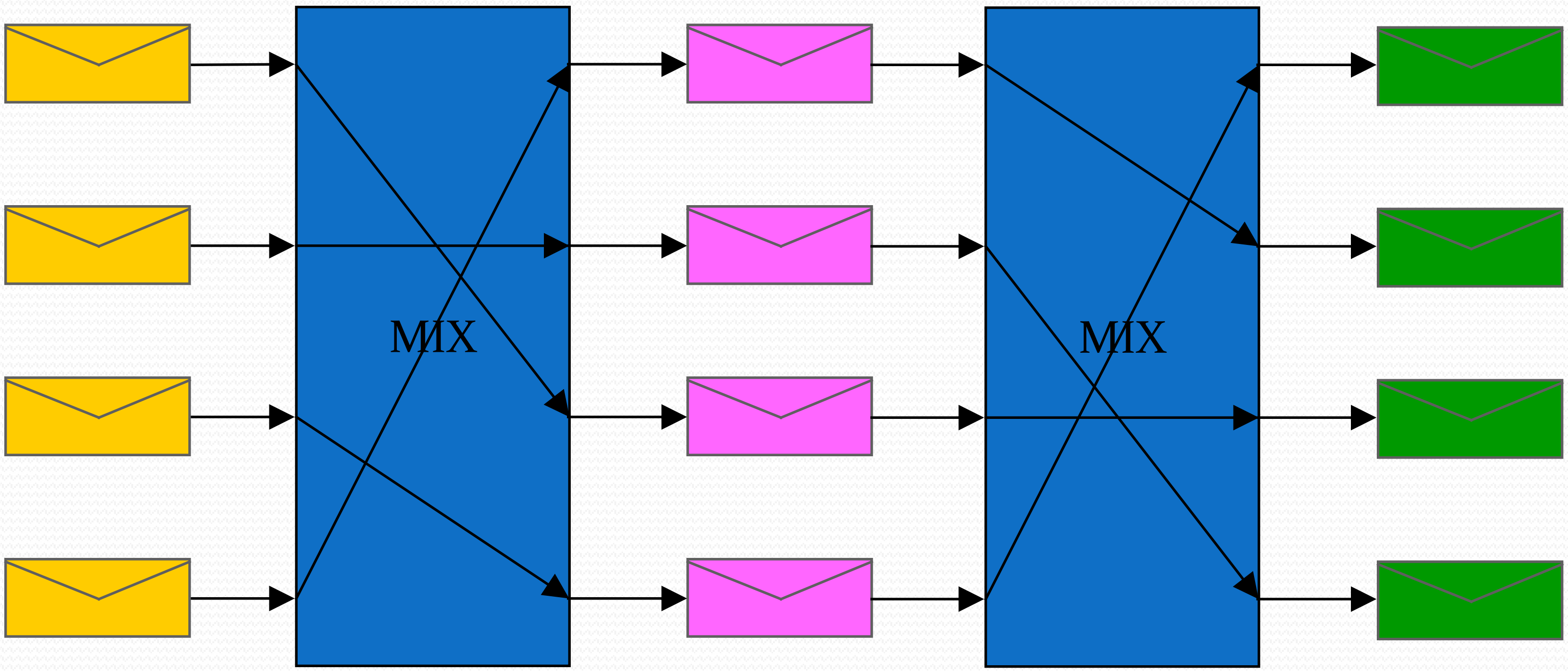
Re-encryption Mix-nets



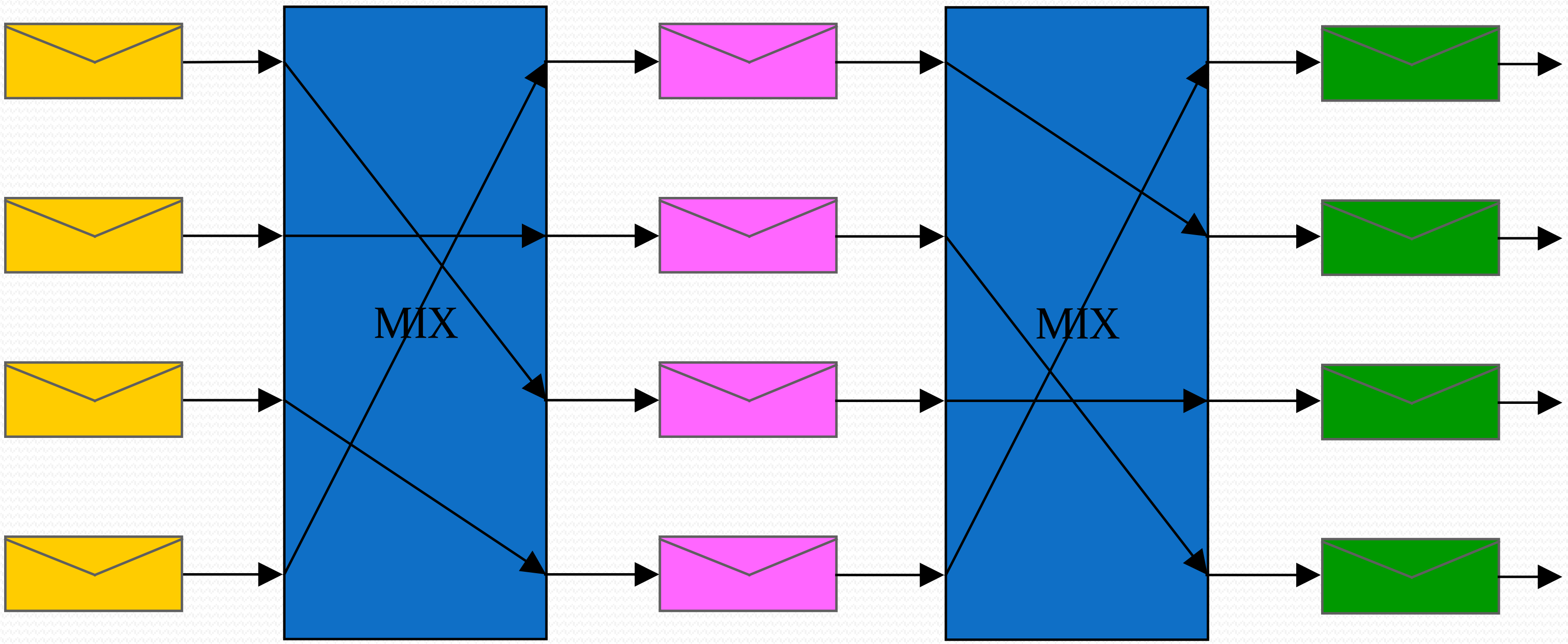
Re-encryption Mix-nets



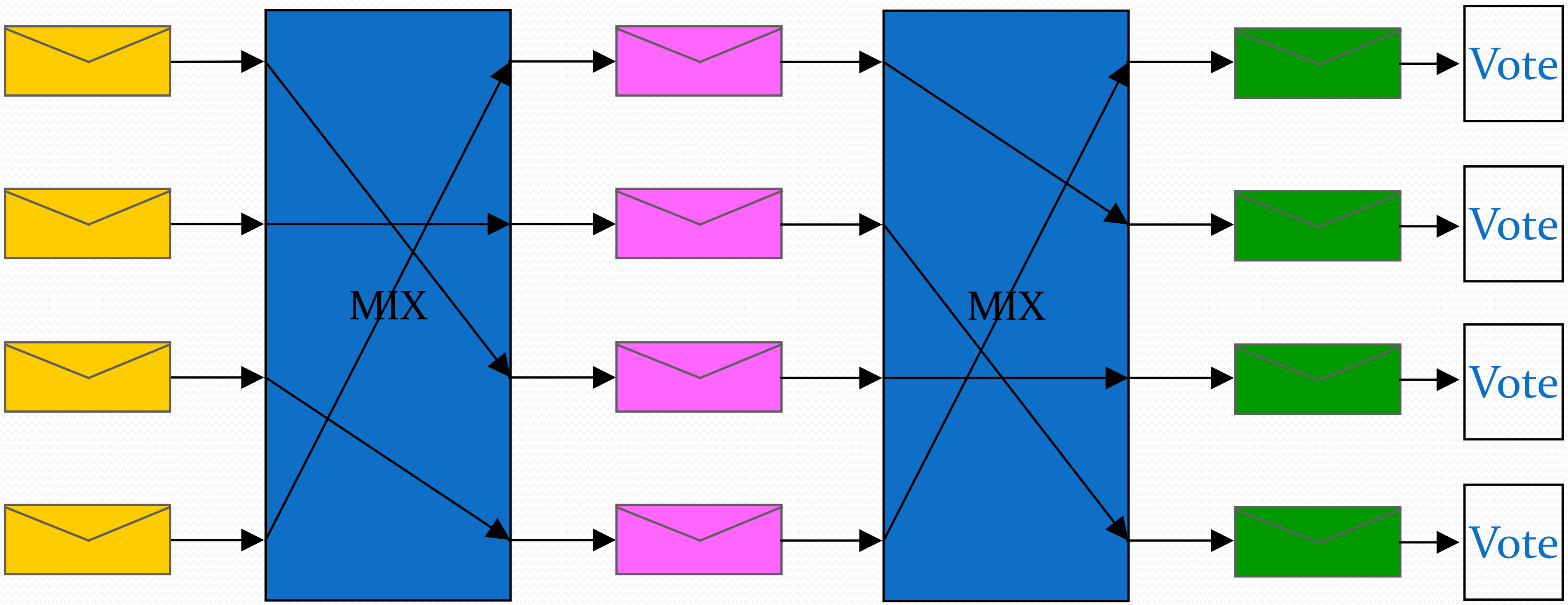
Re-encryption Mix-nets



Re-encryption Mix-nets



Re-encryption Mix-nets



Verifiability

Verifiability

Each re-encryption mix provides a mathematical proof that its output is a permutation of re-encryptions of its input.

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.

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.

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.

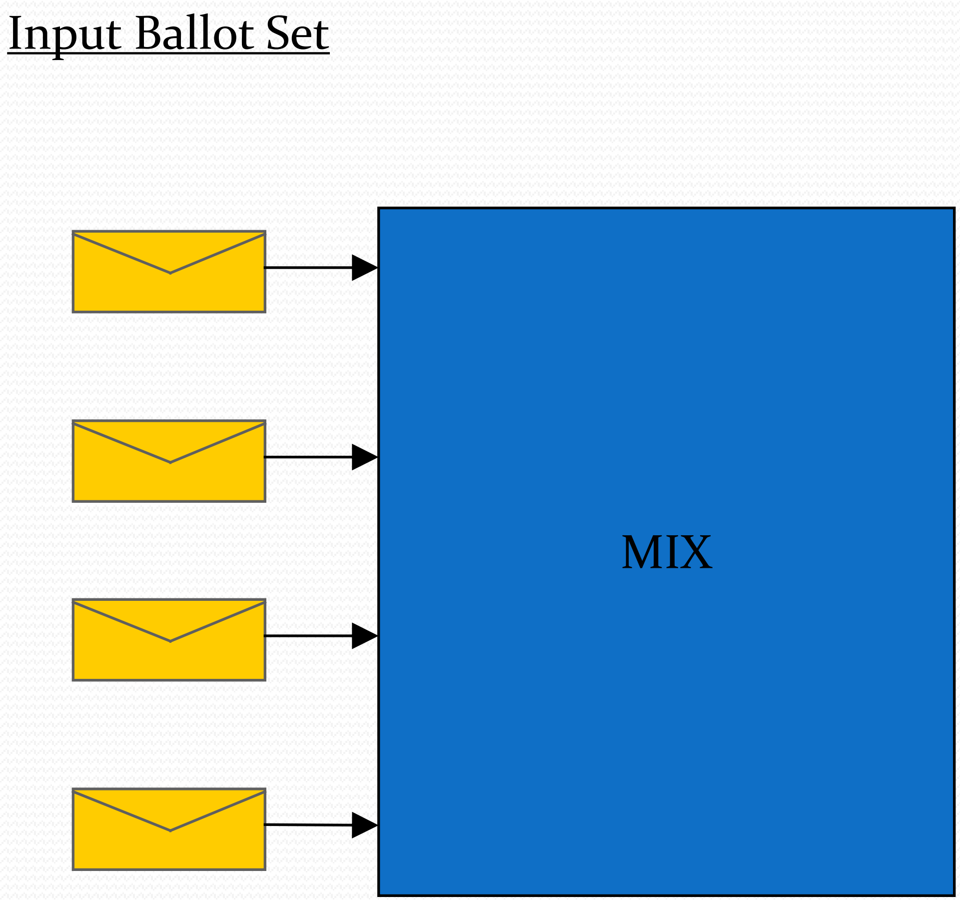
If a mix's proof is invalid, its mixing will be bypassed.

Recent Mix Work

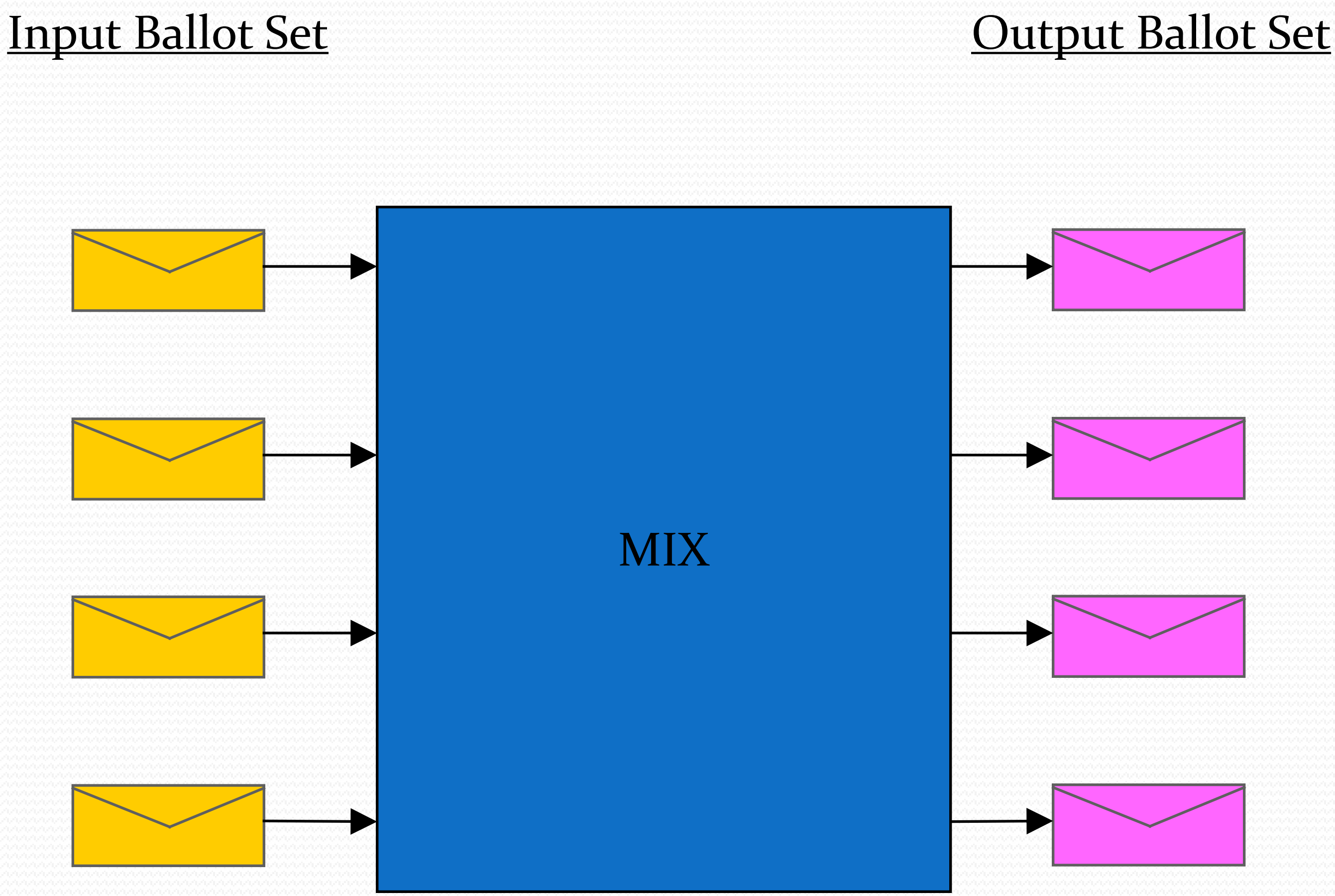
- 1993 Park, Itoh, and Kurosawa
- 1995 Sako and Kilian
- 2001 Furukawa and Sako
- 2001 Neff
- 2002 Jakobsson, Juels, and Rivest
- 2003 Groth

Re-encryption Mix Operation

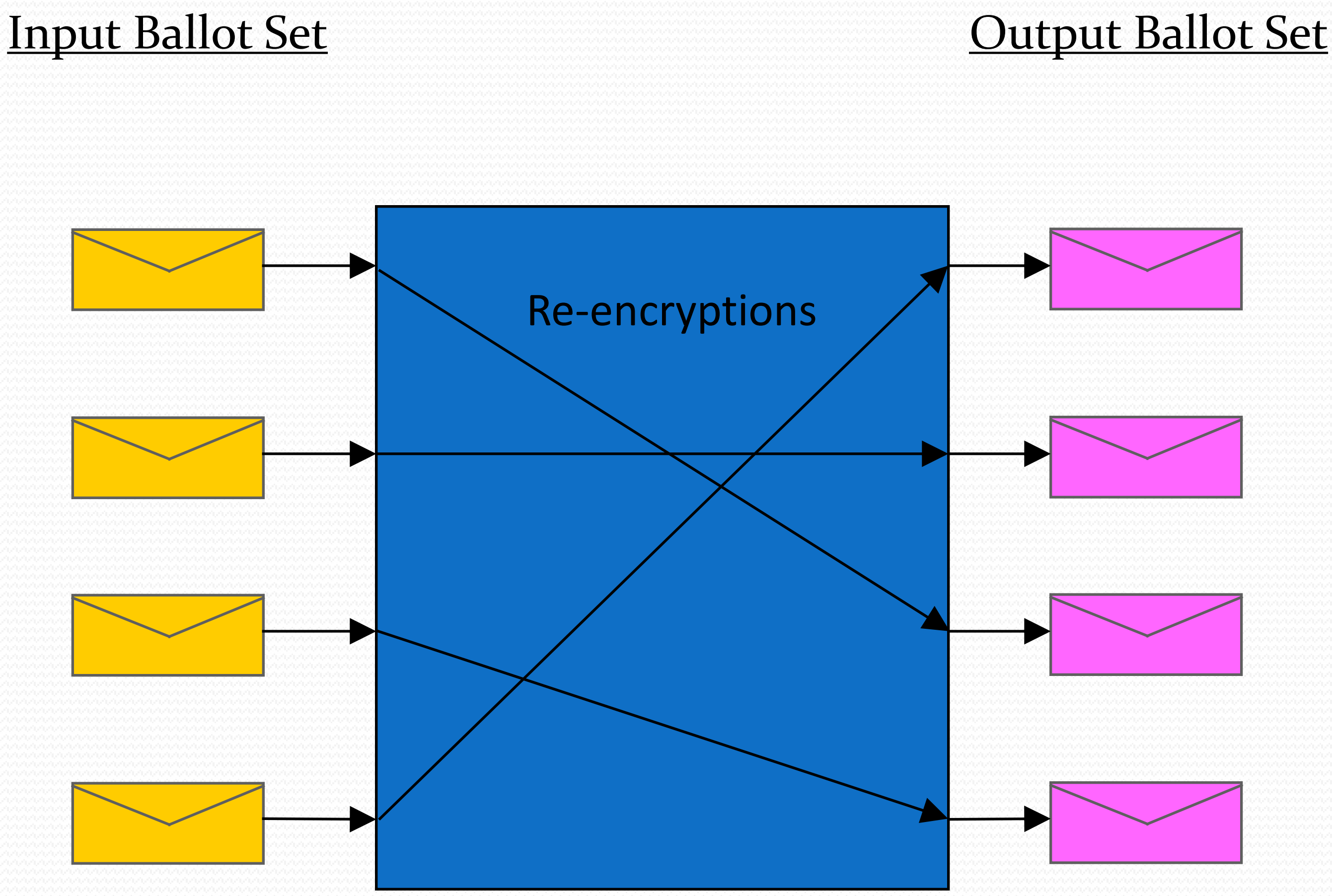
Re-encryption Mix Operation



Re-encryption Mix Operation



Re-encryption Mix Operation



Re-encryption

Re-encryption

- Each value is *re-encrypted* homomorphically.

Re-encryption

- Each value is *re-encrypted* homomorphically.

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

Verifying a Re-encryption

Verifying a Re-encryption

- A prover could simply reveal the specifics of the “blinding factors” used for re-encryption, but this would also reveal the permutation.

Verifying a Re-encryption

- A prover could simply reveal the specifics of the “blinding factors” used for re-encryption, but this would also reveal the permutation.
- Instead, an interactive proof can be performed to demonstrate the equivalence of the input and output ballot sets.

Verifying a Re-encryption

- A prover could simply reveal the specifics of the “blinding factors” used for re-encryption, but this would also reveal the permutation.
- Instead, an interactive proof can be performed to demonstrate the equivalence of the input and output ballot sets.
- The Fiat-Shamir heuristic can be used to “publish” the proof.

The Encryption

The Encryption

- Anyone with the decryption key can read all of the votes – even before mixing.

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.

Most Verifiable Election Protocols

Most Verifiable Election Protocols

[Step 1]

Most Verifiable Election Protocols

Step 1

Encrypt your vote and …

Most Verifiable Election Protocols

Step 1

Encrypt your vote and …

How?

How do Humans Encrypt?

How do Humans Encrypt?

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

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

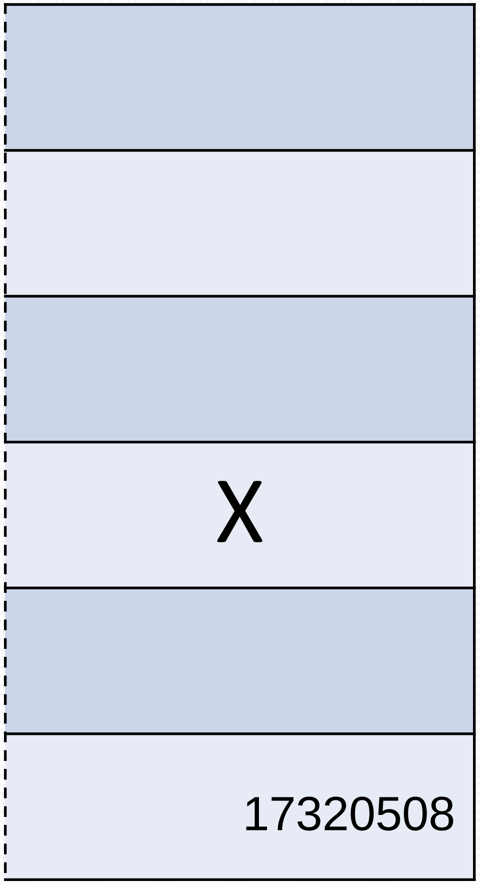
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	
David	
	17320508

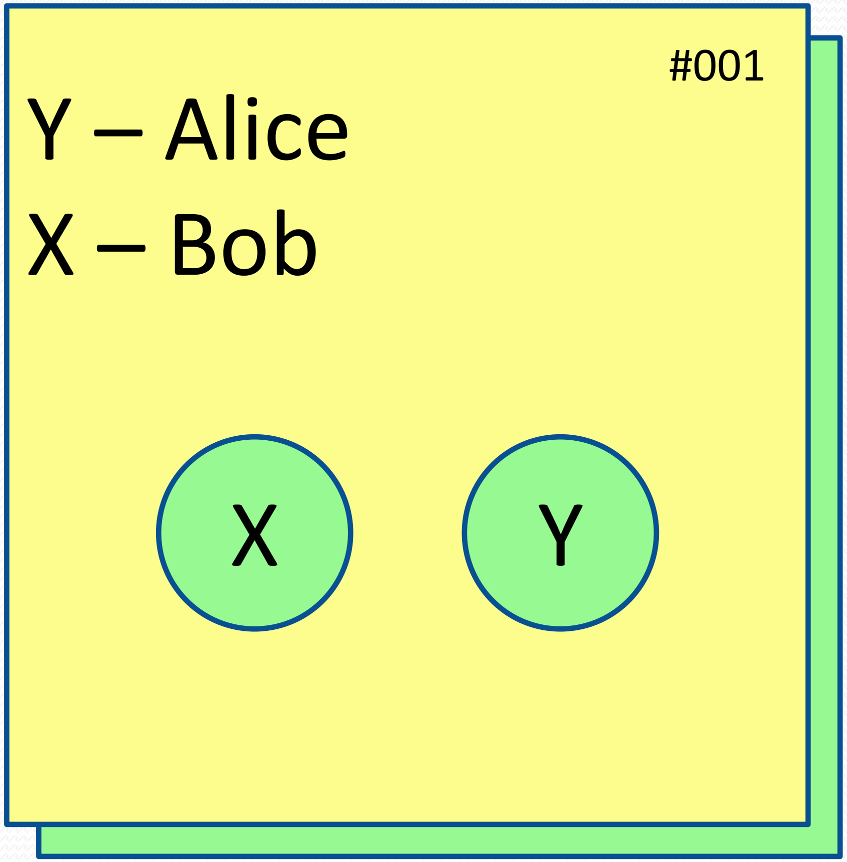
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	X
David	
	17320508

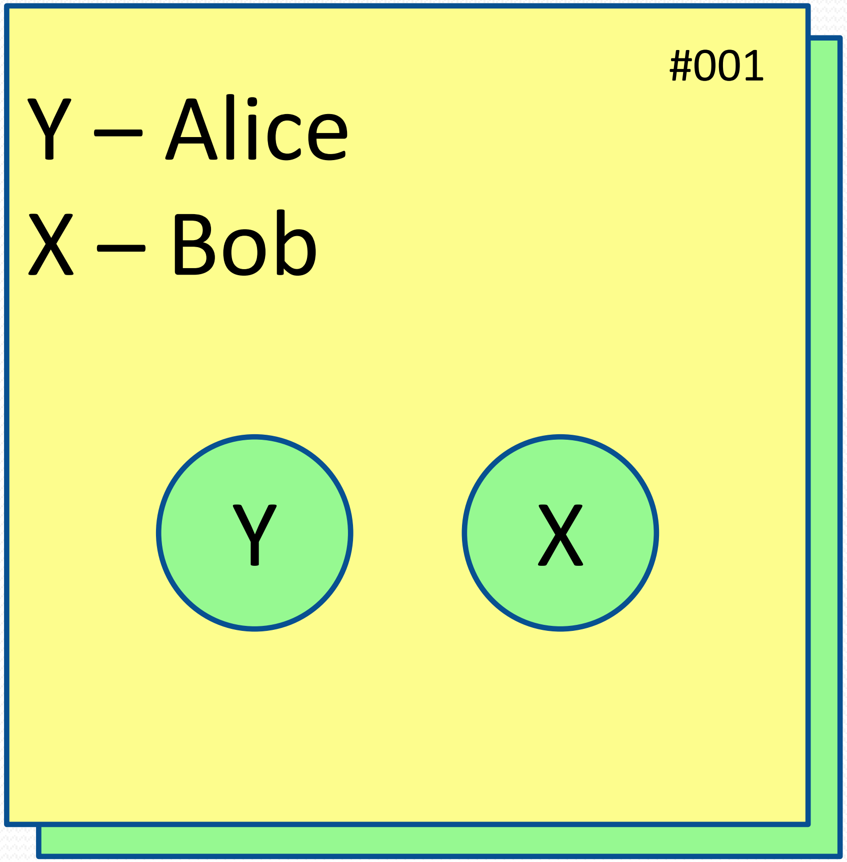
Prêt à Voter Ballot



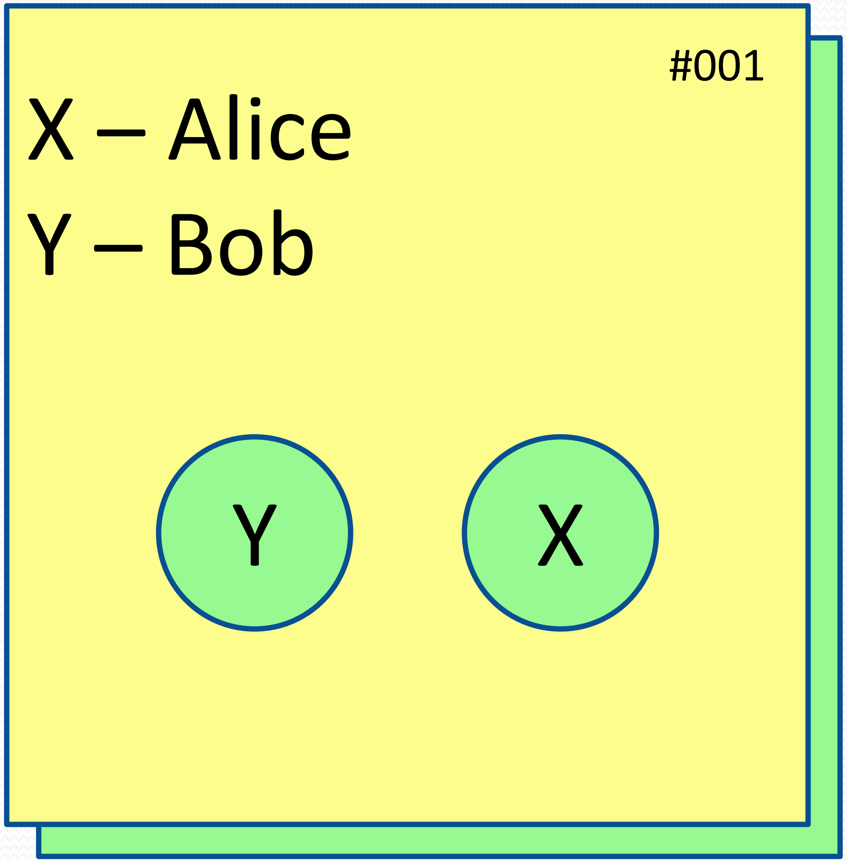
PunchScan Ballot



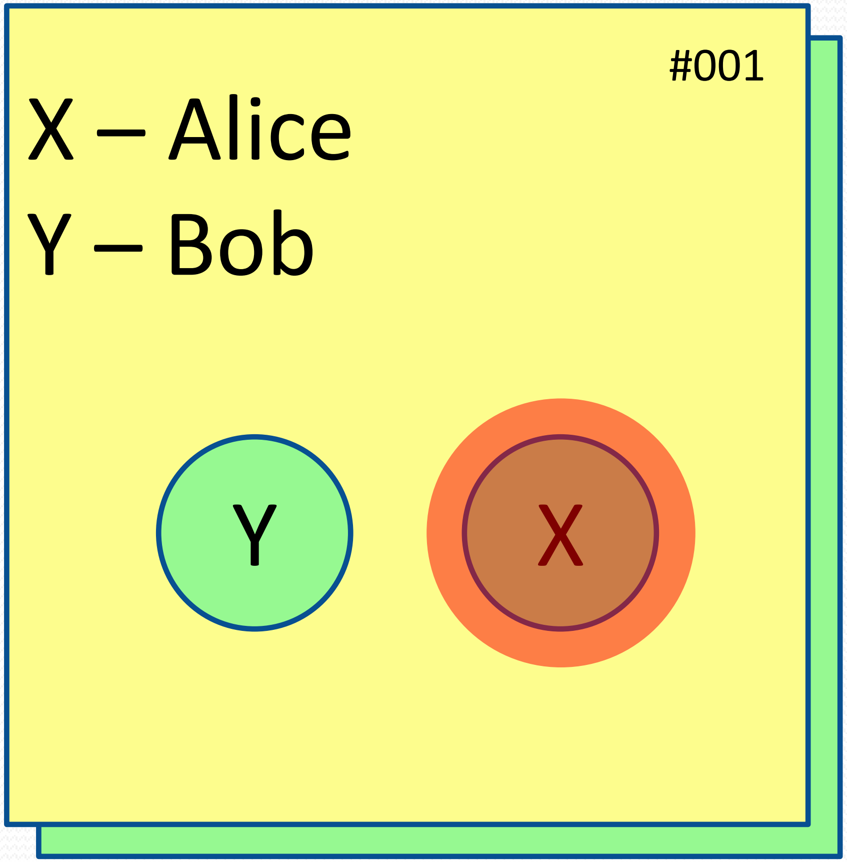
PunchScan Ballot



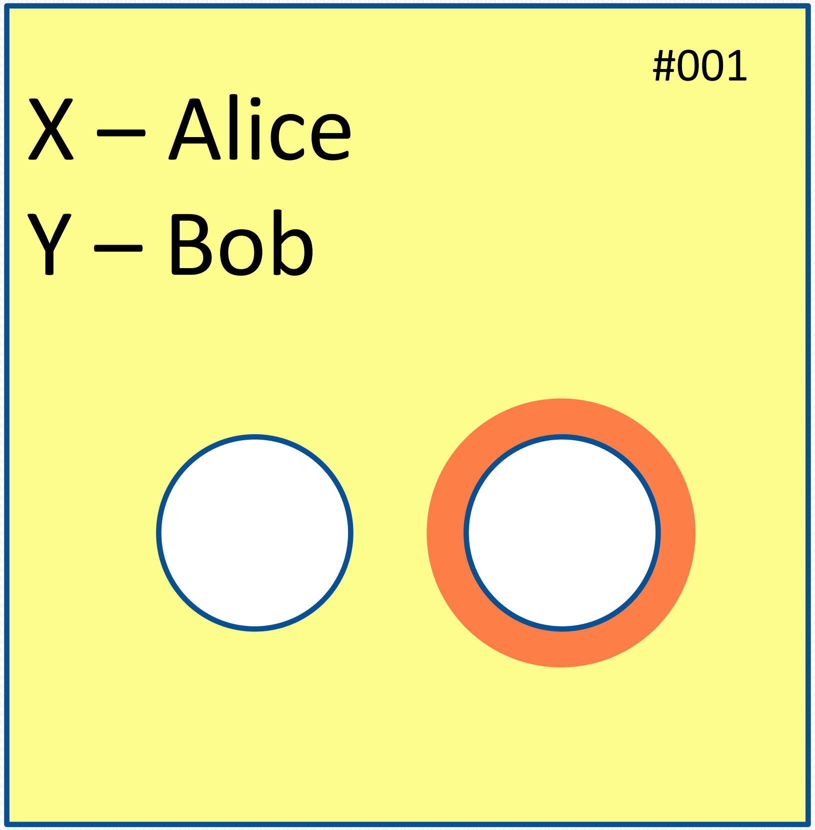
PunchScan Ballot

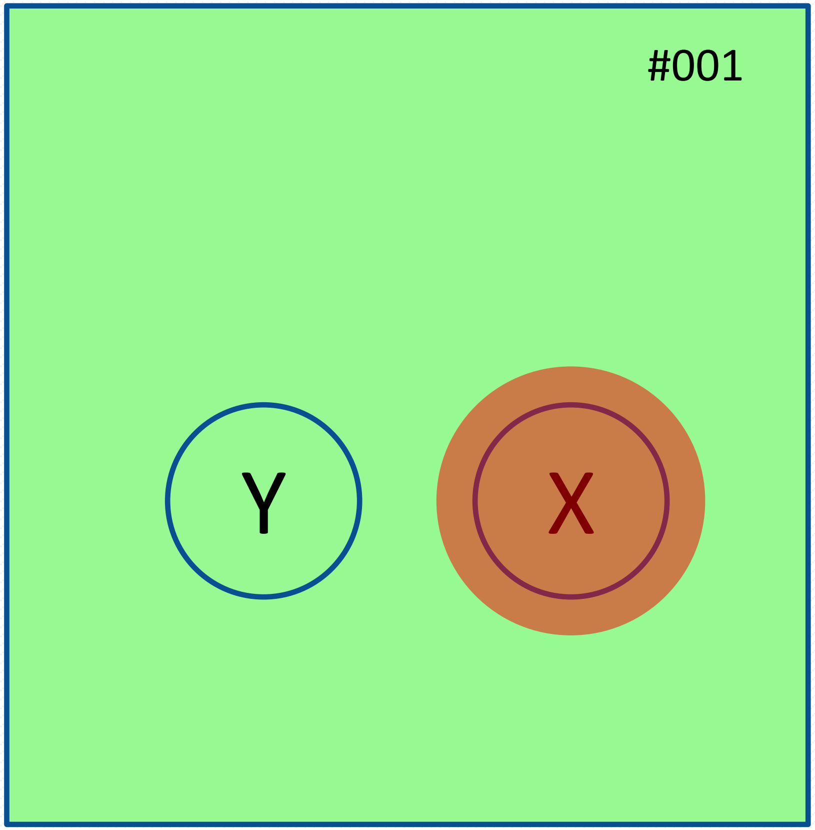


PunchScan Ballot

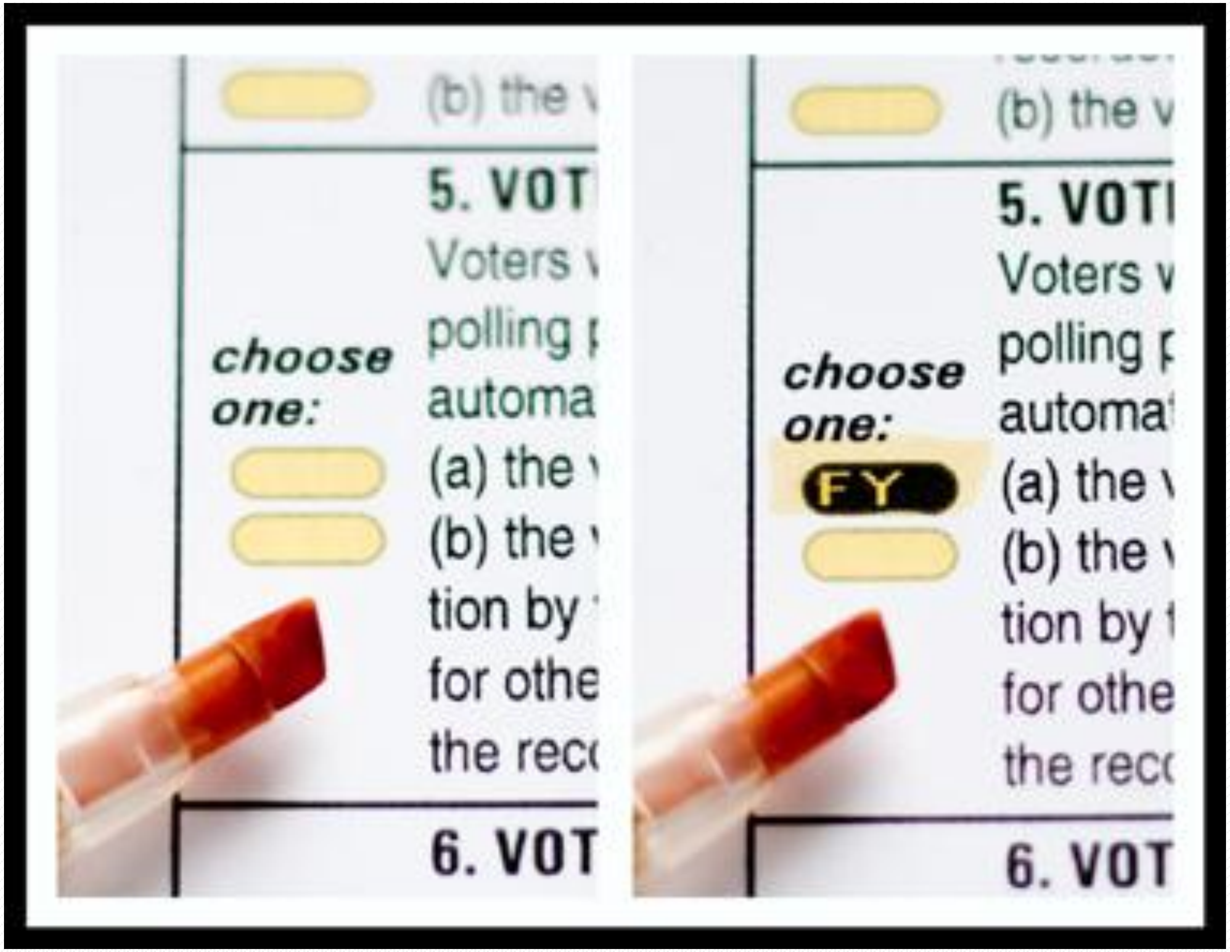


PunchScan Ballot





Scantegrity



Three-Ballot

Ballot	
President	
Alice	○
Bob	●
Charles	○
Vice President	
David	●
Erica	○
r9>k*@oe!4$%	

Ballot	
President	
Alice	●
Bob	●
Charles	○
Vice President	
David	○
Erica	●
*t3]a&;nzs^_=	

Ballot	
President	
Alice	○
Bob	○
Charles	●
Vice President	
David	●
Erica	○
u)/+8c$@.?(	

Voter-Initiated Auditing

Voter-Initiated Auditing

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

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

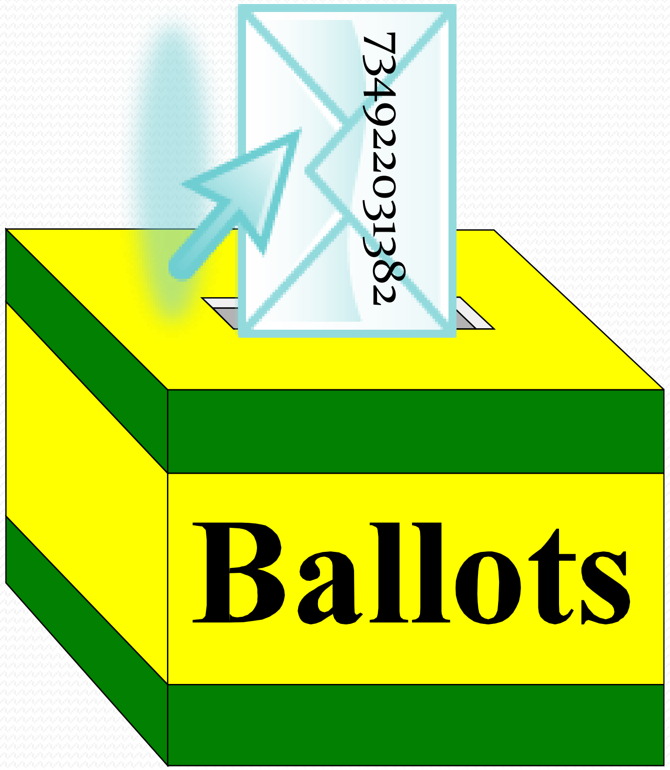
Encrypted Vote

Voter-Initiated Auditing

Voter choice: Cast or Challenge

Voter-Initiated Auditing

Cast



Voter-Initiated Auditing

<u>Challenge</u>

Voter-Initiated Auditing

Challenge

Voter-Initiated Auditing

<u>Challenge</u>

Voter-Initiated Auditing

Challenge

Vote for **Alice**
Random # is
28637582738

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.

True Verifiability

- The end-to-end verifiable election technologies described here allow individuals to *choose who to trust*.
- Individuals are not forced to trust officials with special status. They can depend on verifications from entities of their choice.
- Sufficiently paranoid individuals can check everything for themselves.

Real-World Deployments

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.

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.

End-to-End Verifiability

End-to-End Verifiability

- … is a fundamentally different paradigm,

End-to-End Verifiability

- … is a fundamentally different paradigm,
- … is not just a security enhancement,

End-to-End Verifiability

- … is a fundamentally different paradigm,
- … is not just a security enhancement,
- … democratizes the electoral process,

End-to-End Verifiability

- … is a fundamentally different paradigm,
- … is not just a security enhancement,
- … democratizes the electoral process,
- … but it is ***not*** a panacea.

End-to-End System Properties

End-to-End System Properties

- Accuracy/Integrity

End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved

End-to-End System Properties

- Accuracy/Integrity
  – *enormously* improved
- Privacy/Coercion

End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved
- Privacy/Coercion
  - not substantially changed

End-to-End System Properties

- Accuracy/Integrity
  - – *enormously* improved
- Privacy/Coercion
  - – not substantially changed
- Reliability/Survivability

End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved
- Privacy/Coercion
  - not substantially changed
- Reliability/Survivability
  - not substantially changed

End-to-End System Properties

- Accuracy/Integrity
  - – *enormously* improved
- Privacy/Coercion
  - – not substantially changed
- Reliability/Survivability
  - – not substantially changed
- Usability/Comprehensibility

End-to-End System Properties

- Accuracy/Integrity
  – *enormously* improved
- Privacy/Coercion
  – not substantially changed
- Reliability/Survivability
  – not substantially changed
- Usability/Comprehensibility
  – not substantially changed

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.
- However, a bill was recently introduced in Congress that explicitly precludes use of crypto.