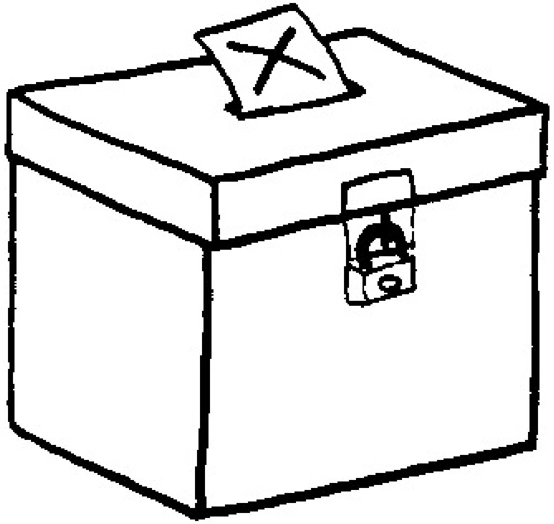
CRCS Center for Research on Computation and Society

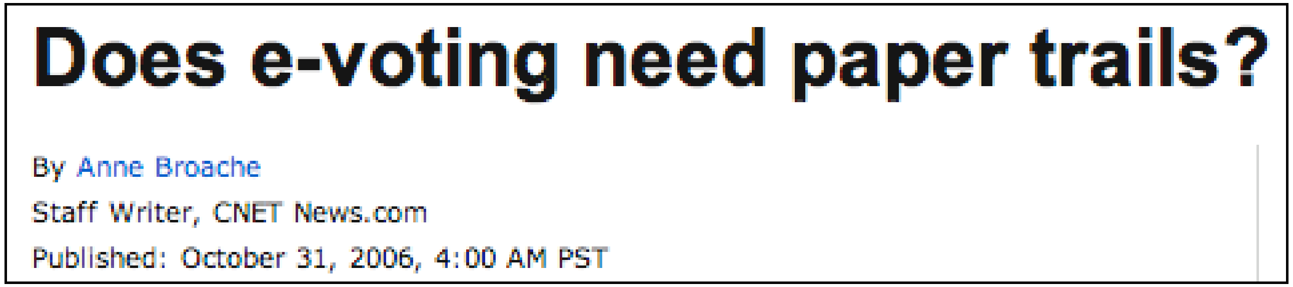
chip Children's Hospital Informatics Program



Verifying Elections with Cryptography

Ben Adida
Harvard

Google – *December 19th, 2007*



Does e-voting need paper trails?

By Anne Broache

Staff Writer, CNET News.com

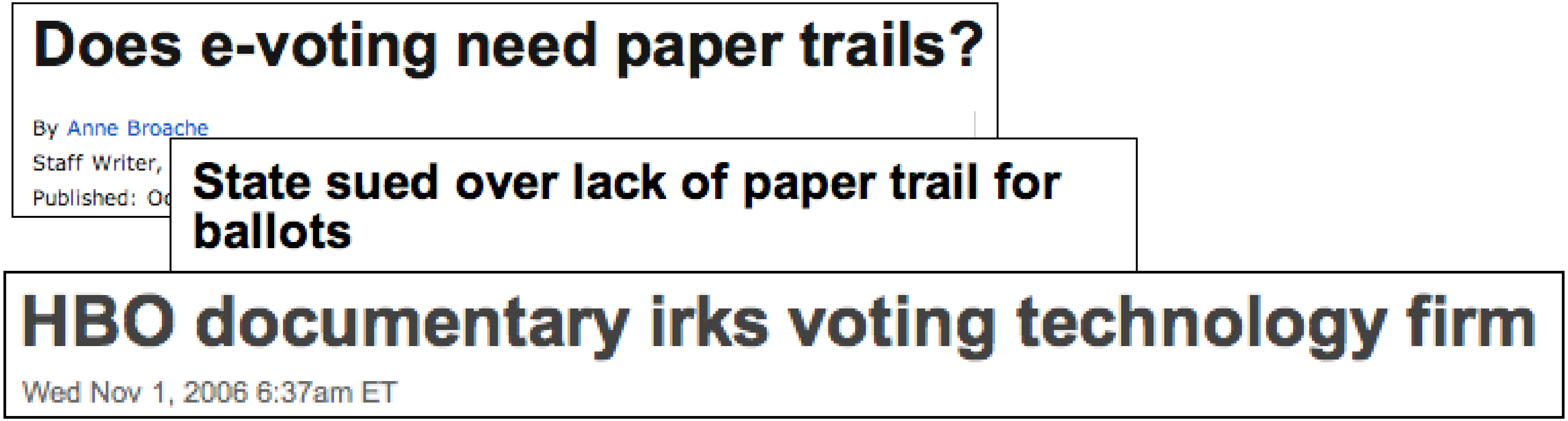
Published: October 31, 2006, 4:00 AM PST

Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: Oc

State sued over lack of paper trail for ballots

By AMAN BATHEJA
STAR-TELEGRAM STAFF WRITER



Does e-voting need paper trails?

By Anne Broache

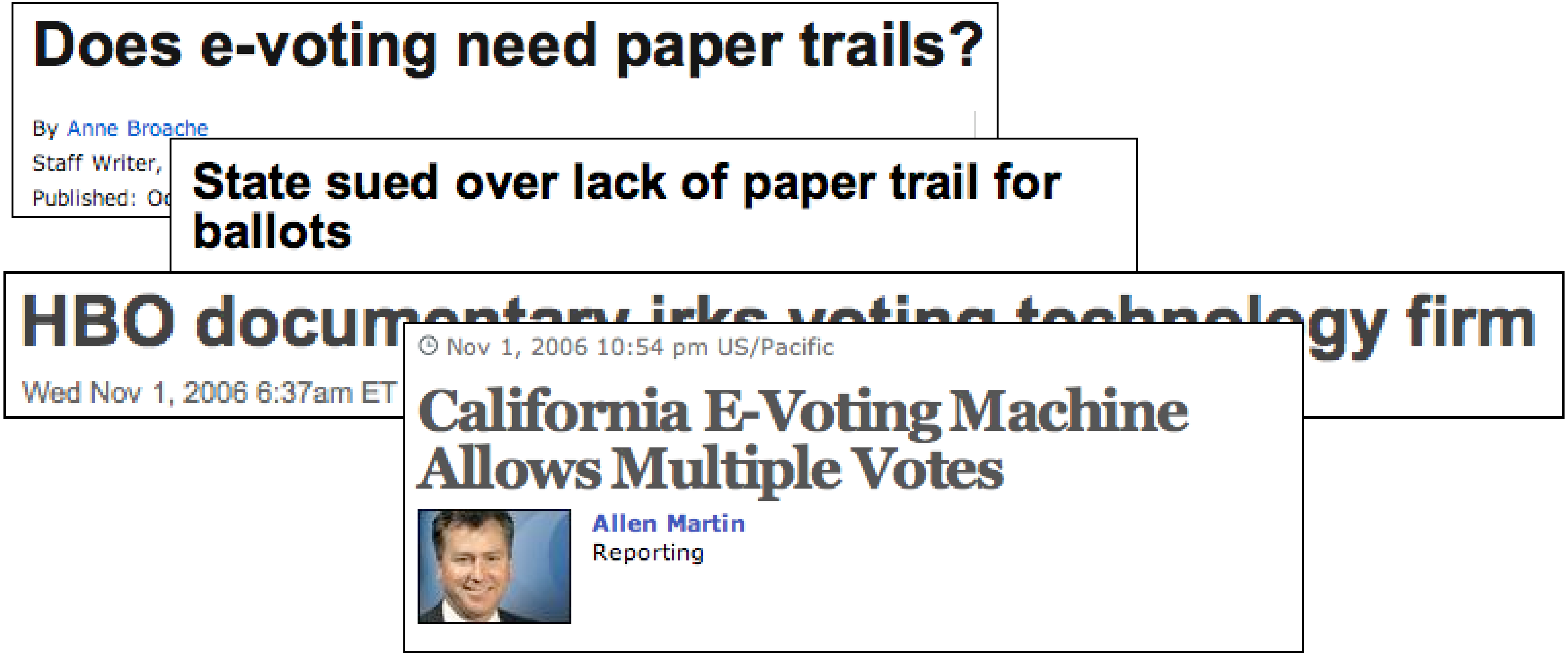
Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET



Does e-voting need paper trails?

By Anne Broache

Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

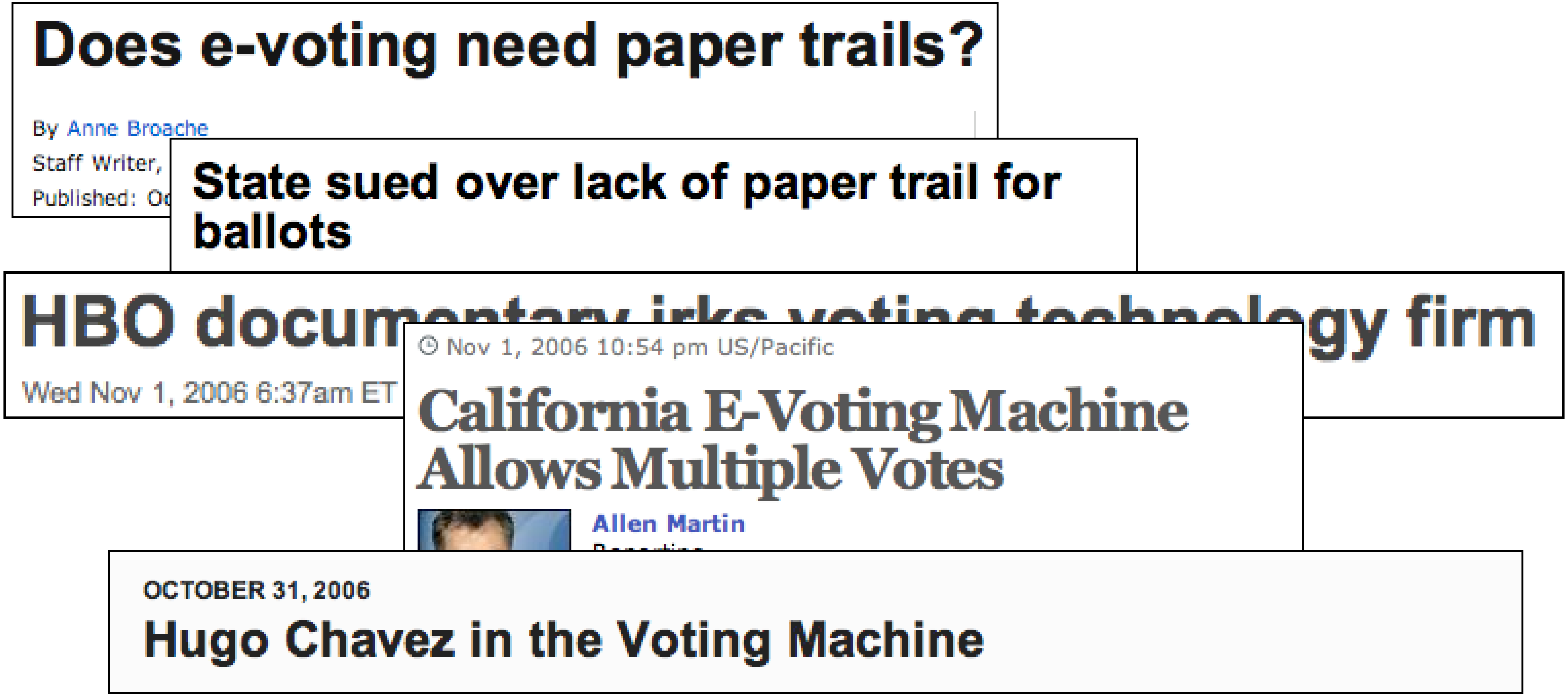
Wed Nov 1, 2006 6:37am ET

Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin

Reporting



Does e-voting need paper trails?

By Anne Broache

Staff Writer,

Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET

Nov 1, 2006 10:54 pm US/Pacific

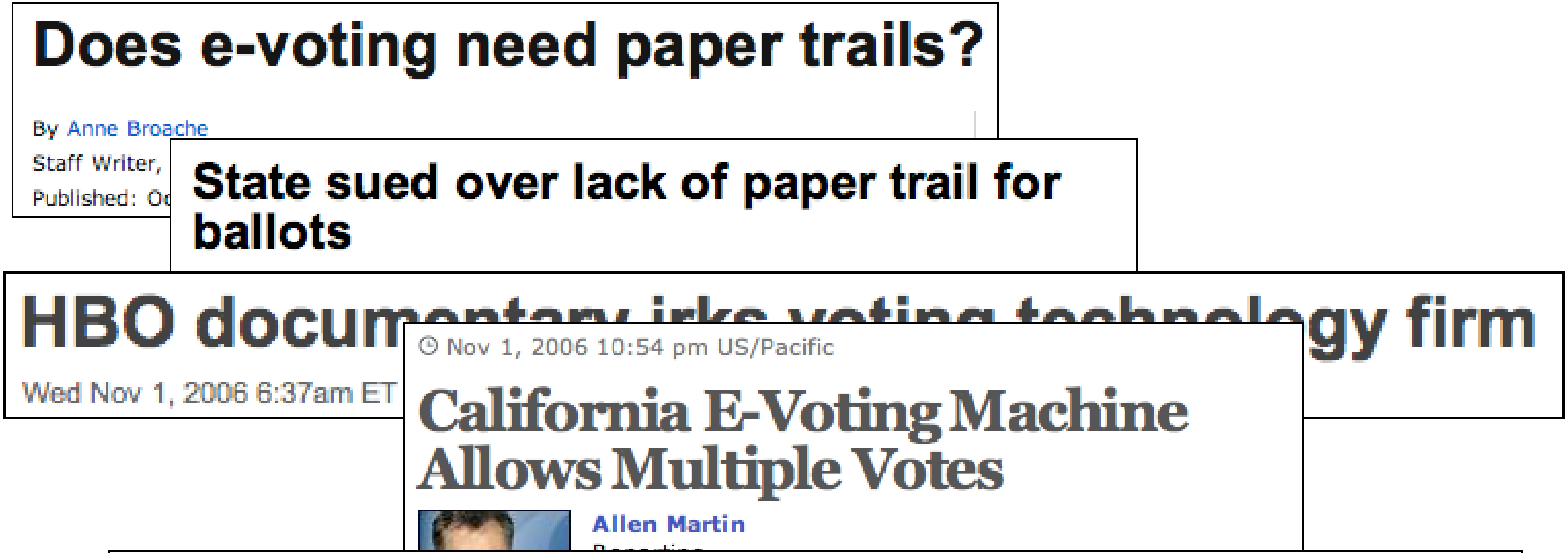
California E-Voting Machine Allows Multiple Votes

Allen Martin

Reporting

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine



Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: Oc

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET

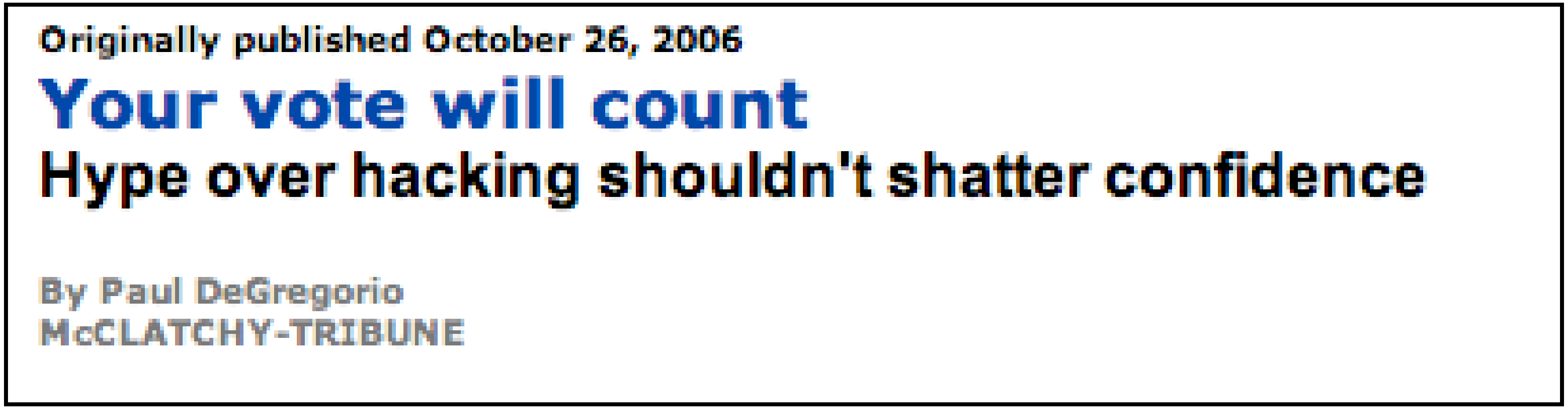
Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin
Reporting

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine



Originally published October 26, 2006

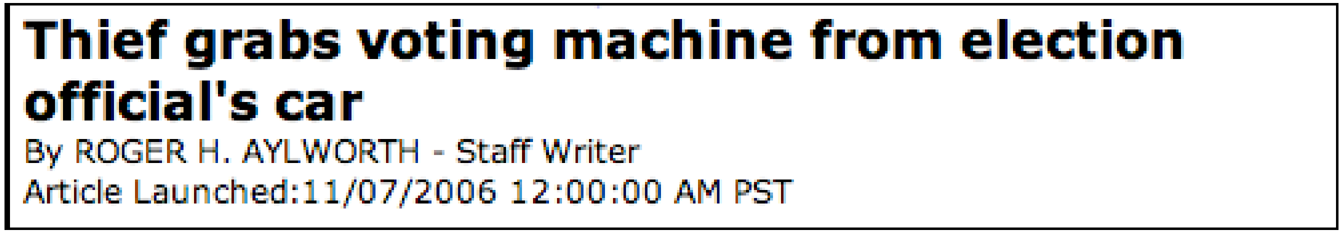
Your vote will count

Hype over hacking shouldn't shatter confidence

By Paul DeGregorio
McCLATCHY-TRIBUNE

Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.

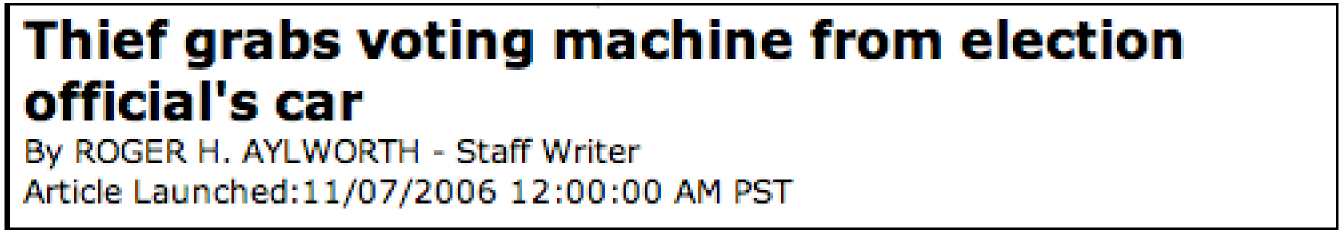


Thief grabs voting machine from election official's car

By ROGER H. AYLWORTH - Staff Writer

Article Launched:11/07/2006 12:00:00 AM PST

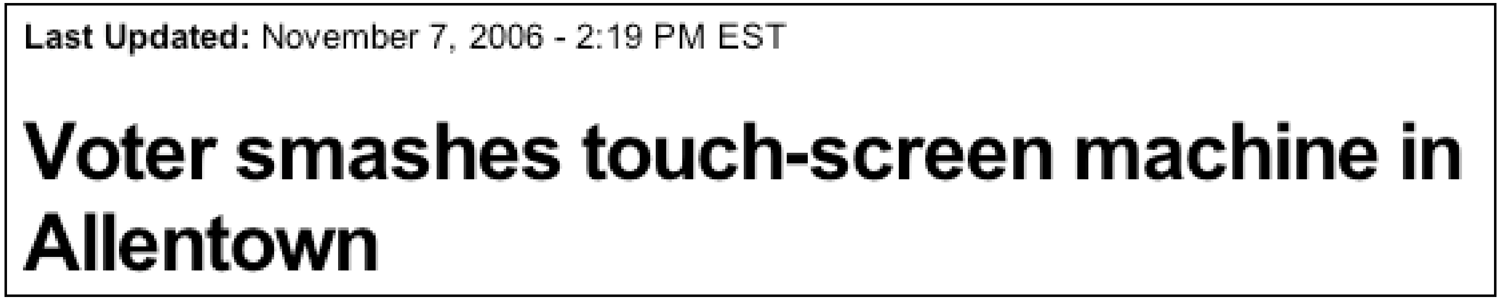
Rogers precinct, with more than 100 percent voter turnout, alarmed both of them.



Thief grabs voting machine from election official's car

By ROGER H. AYLWORTH - Staff Writer

Article Launched:11/07/2006 12:00:00 AM PST



Last Updated: November 7, 2006 - 2:19 PM EST

Voter smashes touch-screen machine in Allentown

Rogers precinct, with more than 100 percent

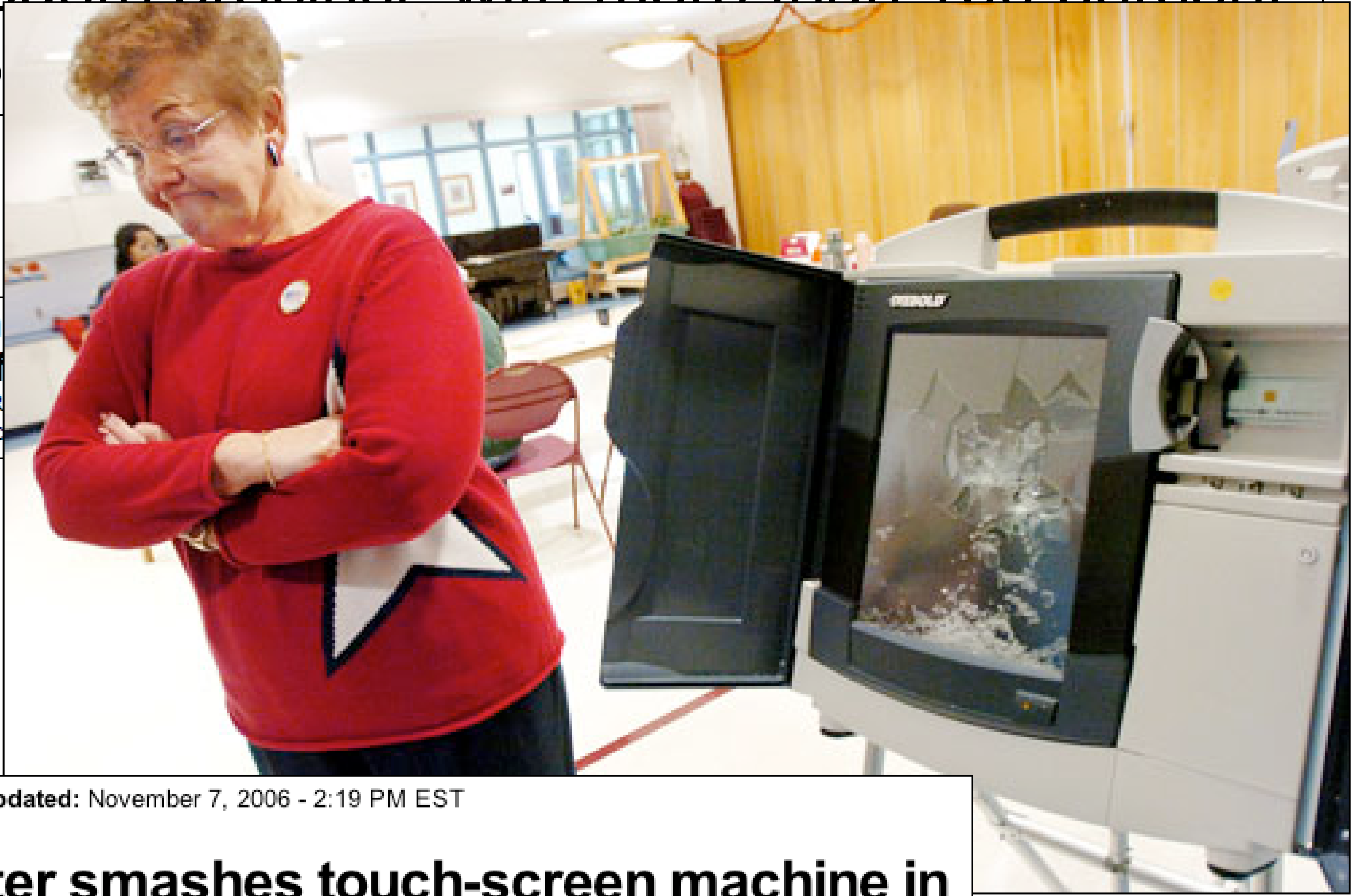
vo

Th

off

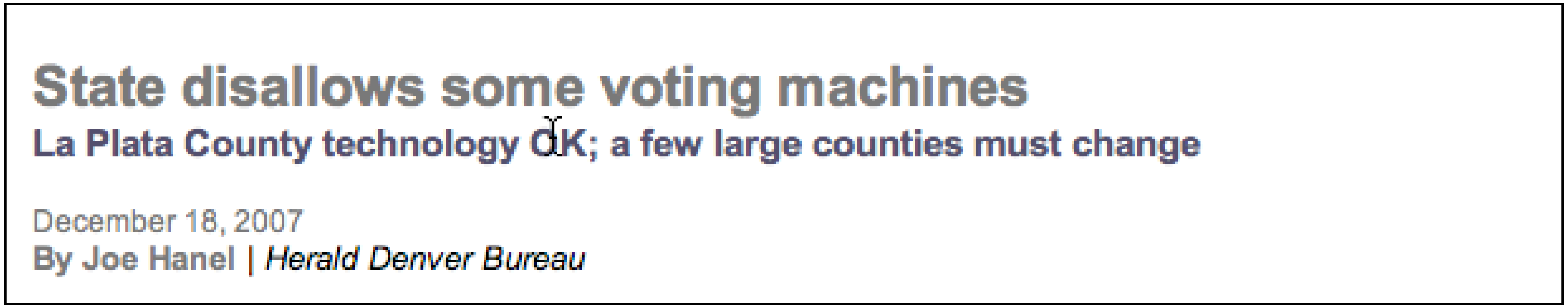
By R

Artic



Last Updated: November 7, 2006 - 2:19 PM EST

Voter smashes touch-screen machine in Allentown

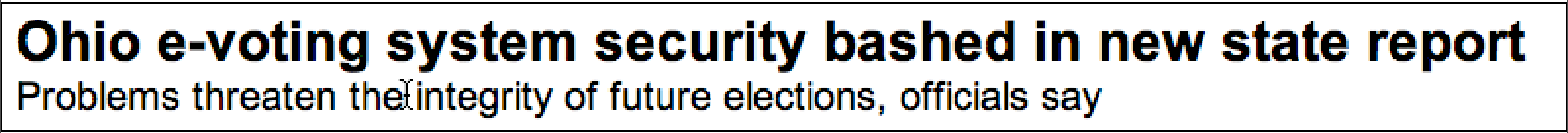


State disallows some voting machines

La Plata County technology OK; a few large counties must change

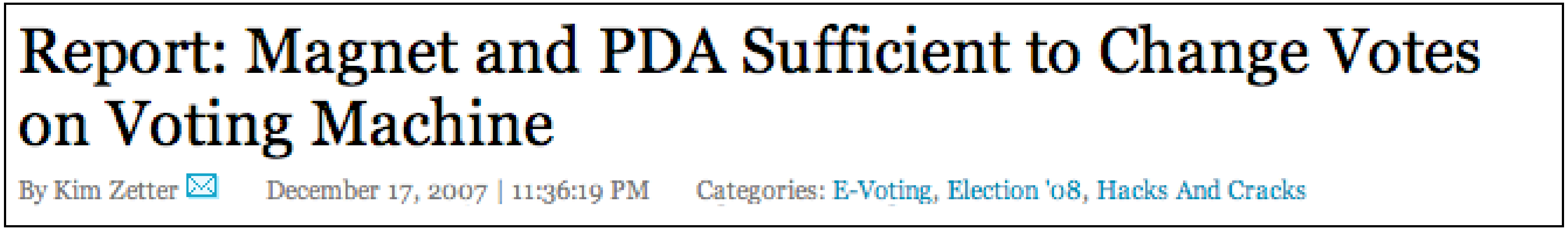
December 18, 2007

By Joe Hanel | *Herald Denver Bureau*



Ohio e-voting system security bashed in new state report

Problems threaten the integrity of future elections, officials say



Report: Magnet and PDA Sufficient to Change Votes on Voting Machine

By Kim Zetter ✉ December 17, 2007 | 11:36:19 PM Categories: E-Voting, Election '08, Hacks And Cracks

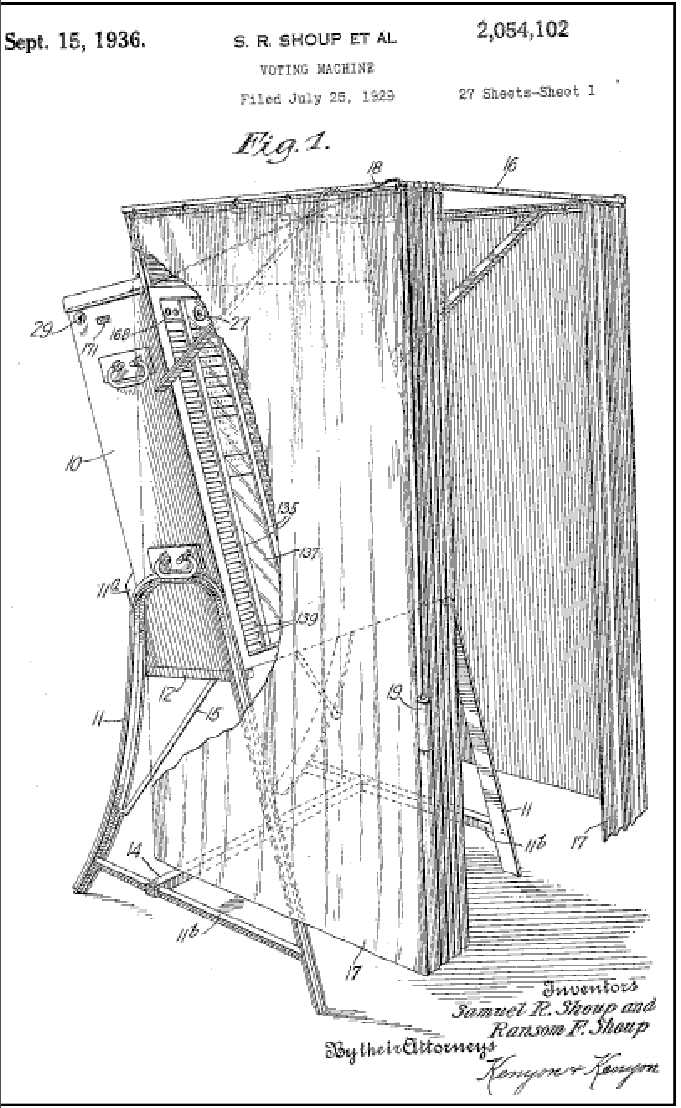
Wooten got the news from his wife, Roxanne, who went to City Hall on Wednesday to see the election results.

"She saw my name with zero votes by it. She came home and asked me if I had voted for myself or not. I told her I did," said Wooten, owner of a local bar.

How We Got Here

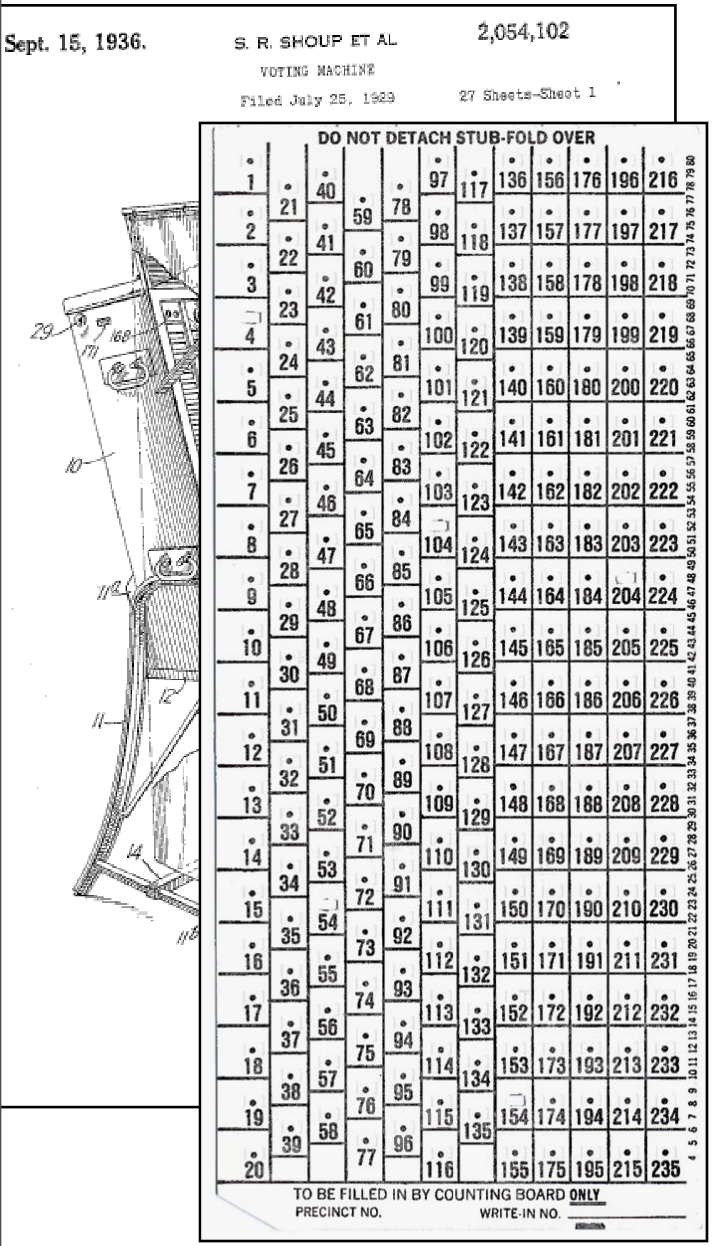
http://www.cs.uiowa.edu/~jones/voting/pictures/

How We Got Here



http://www.cs.uiowa.edu/~jones/voting/pictures/

How We Got Here



Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102

VOTING MACHINE

Filed July 25, 1929 27 Sheets-Sheet 1

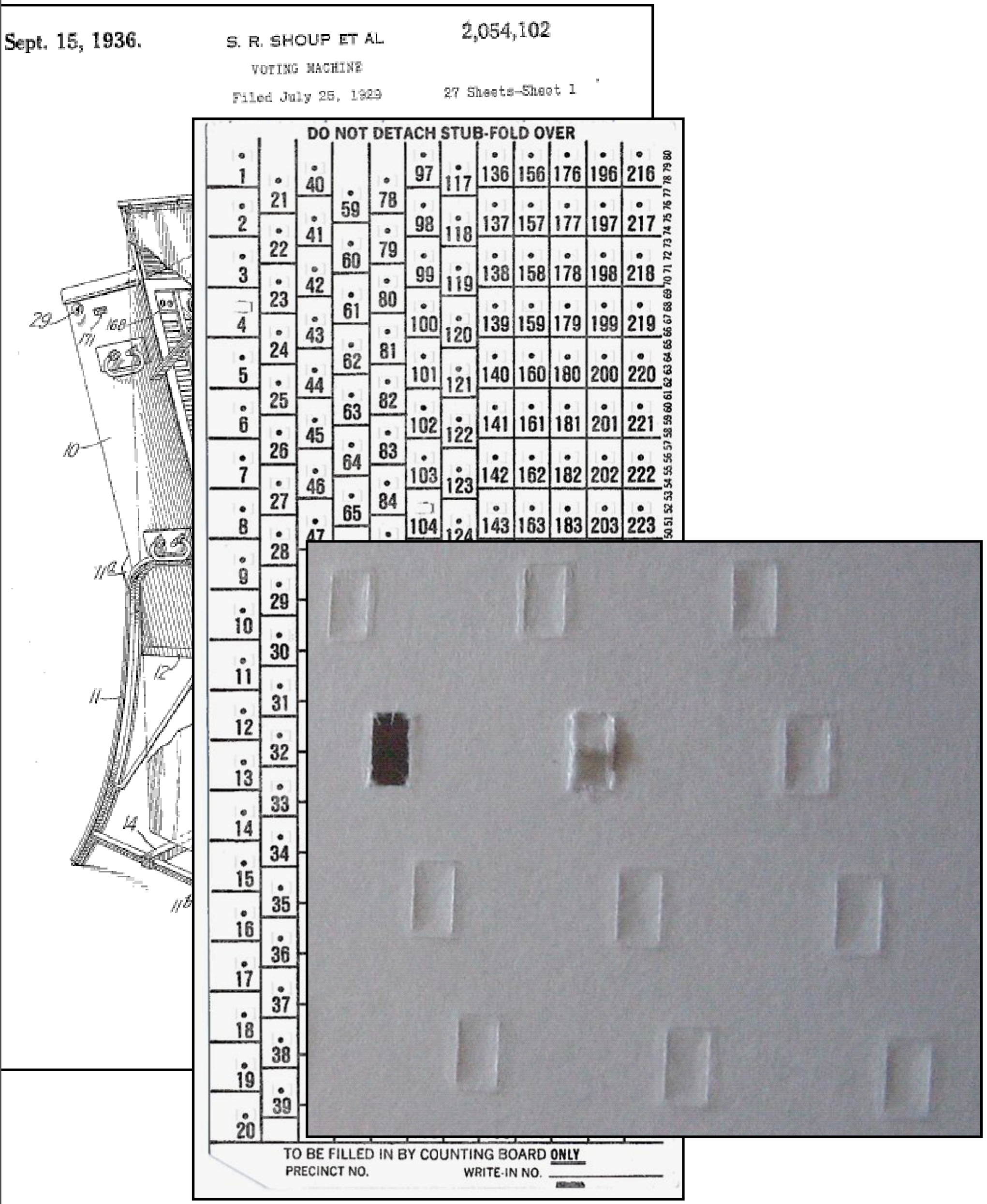
DO NOT DETACH STUB-FOLD OVER

TO BE FILLED IN BY COUNTING BOARD ONLY

PRECINCT NO. WRITE-IN NO.

http://www.cs.uiowa.edu/~jones/voting/pictures/

How We Got Here



Sept. 15, 1936. S. R. SHOUP ET AL 2,054,102

VOTING MACHINE

Filed July 25, 1929 27 Sheets-Sheet 1

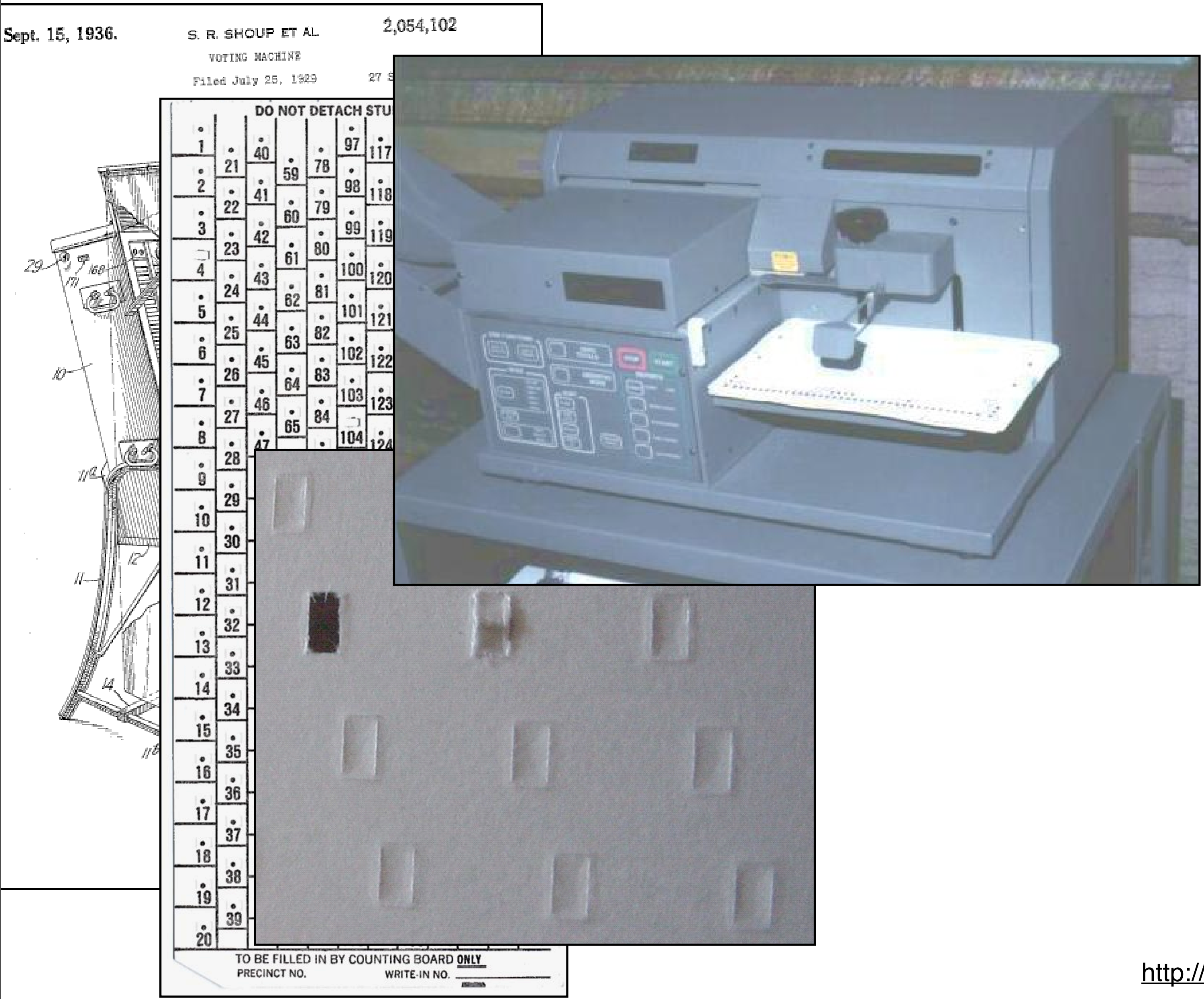
DO NOT DETACH STUB-FOLD OVER

TO BE FILLED IN BY COUNTING BOARD **ONLY**

PRECINCT NO. WRITE-IN NO.

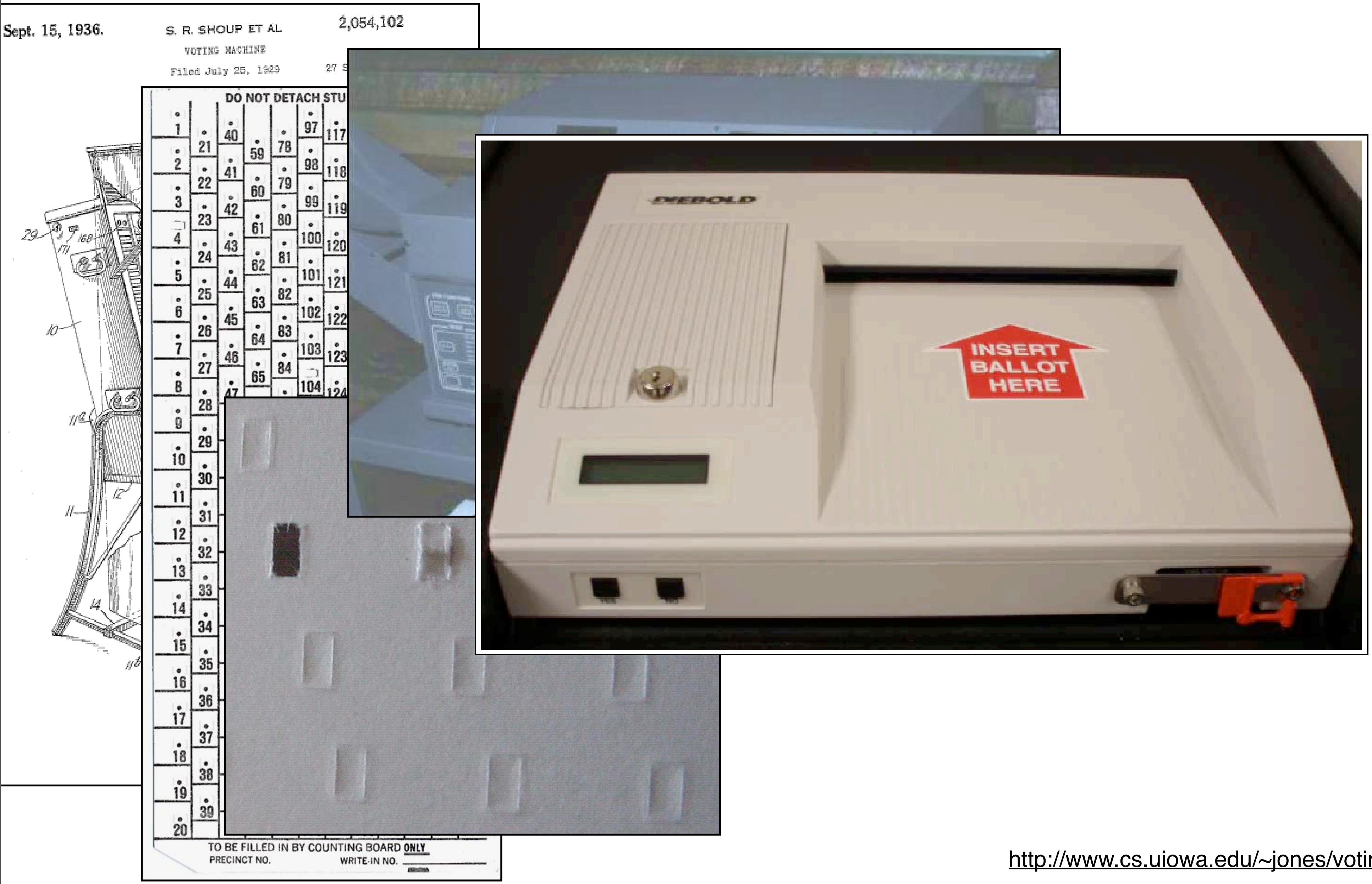
http://www.cs.uiowa.edu/~jones/voting/pictures/

How We Got Here



http://www.cs.uiowa.edu/~jones/voting/pictures/

How We Got Here

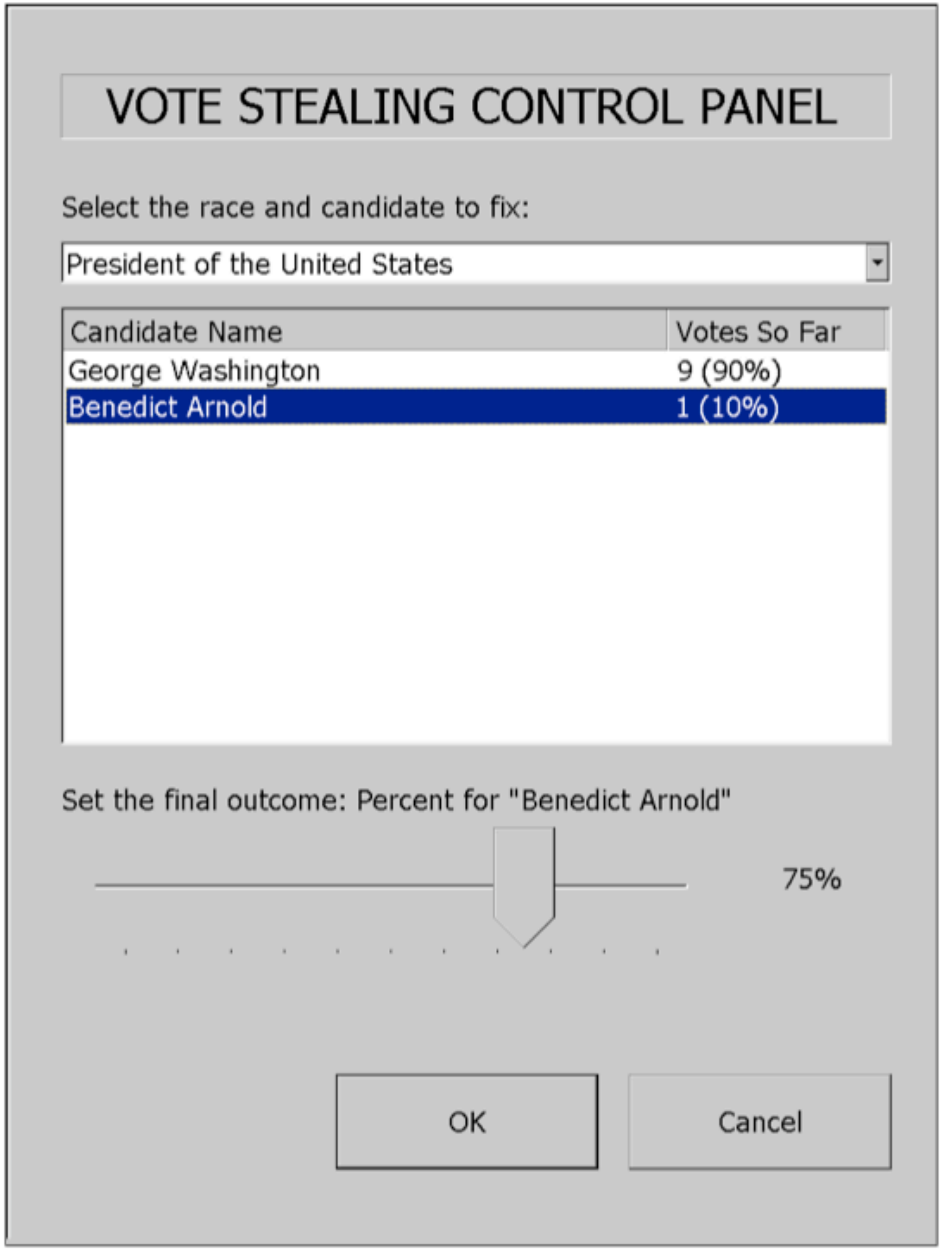


http://www.cs.uiowa.edu/~jones/voting/pictures/

How We Got Here

http://www.cs.uiowa.edu/~jones/voting/pictures/

Last Year: Princeton Report



VOTE STEALING CONTROL PANEL

Select the race and candidate to fix:

President of the United States

Candidate Name	Votes So Far
George Washington	9 (90%)
Benedict Arnold	1 (10%)

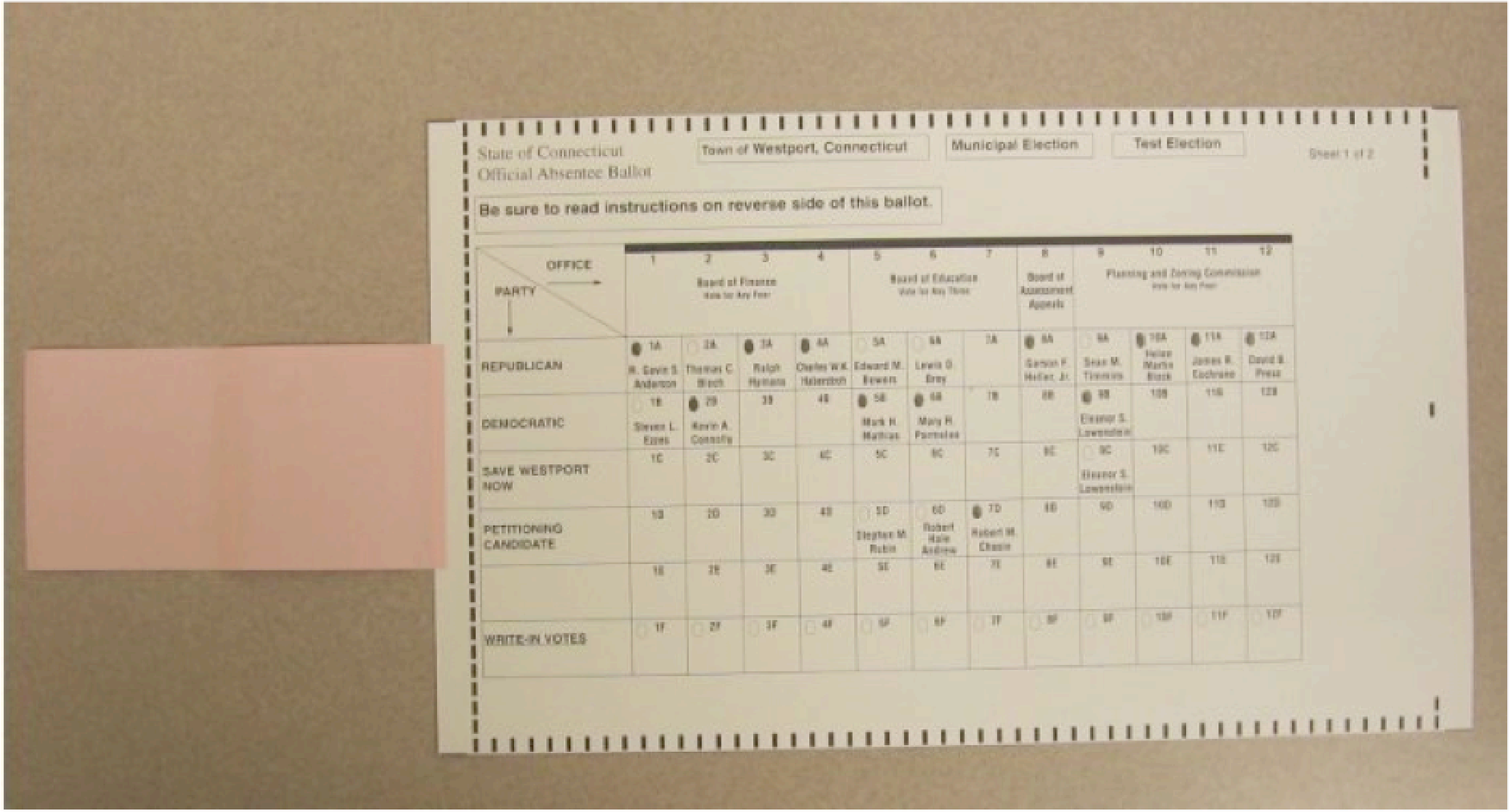
Set the final outcome: Percent for "Benedict Arnold"

75%

- Diebold touch-screen runs executable code loaded from memory card
- All audit logs modified to be consistent
- Can spread virally by memory card.

[FHF2006]

But not just DREs...



State of Connecticut
Official Absentee Ballot

Town of Westport, Connecticut

Municipal Election

Test Election

Sheet 1 of 2

Be sure to read instructions on reverse side of this ballot.

OFFICE → PARTY ↓	1	2	3	4	5	6	7	8	9	10	11	12
	Board of Finance Vote for Any Four				Board of Education Vote for Any Three			Board of Assessment Appeals	Planning and Zoning Commission Vote for Any Four			
REPUBLICAN	● 1A R. Gavin S. Anderson	○ 2A Thomas C. Bloch	● 3A Ralph Hymans	● 4A Charles W.K. Haberstroh	○ 5A Edward M. Bowers	○ 6A Lewis O. Bray	7A	● 8A Gordon F. Heller, Jr.	○ 9A Sean M. Timmins	● 10A Helen Martin Block	● 11A James R. Cochrane	● 12A David B. Press
DEMOCRATIC	○ 1B Steven L. Epps	● 2B Kevin A. Connolly	3B	4B	● 5B Mark H. Mathias	● 6B Mary R. Parmelee	7B	8B	● 9B Eleanor S. Lowenstein	10B	11B	12B
SAVE WESTPORT NOW	1C	2C	3C	4C	5C	6C	7C	8C	○ 9C Eleanor S. Lowenstein	10C	11C	12C
PETITIONING CANDIDATE	1D	2D	3D	4D	○ 5D Stephen M. Rubin	○ 6D Robert Hale Andrew	● 7D Robert M. Chasin	8D	9D	10D	11D	12D
	1E	2E	3E	4E	5E	6E	7E	8E	9E	10E	11E	12E
WRITE-IN VOTES	○ 1F	○ 2F	○ 3F	○ 4F	○ 5F	○ 6F	○ 7F	○ 8F	○ 9F	○ 10F	○ 11F	○ 12F

[KMRS2006]

How can Cryptography help?

Cryptography provides more than confidentiality.

Cryptography can provide **verifiability** while maintaining **ballot secrecy**.

The Point of An Election

“The People have spoken....
the bastards!”

Dick Tuck
1966 Concession Speech

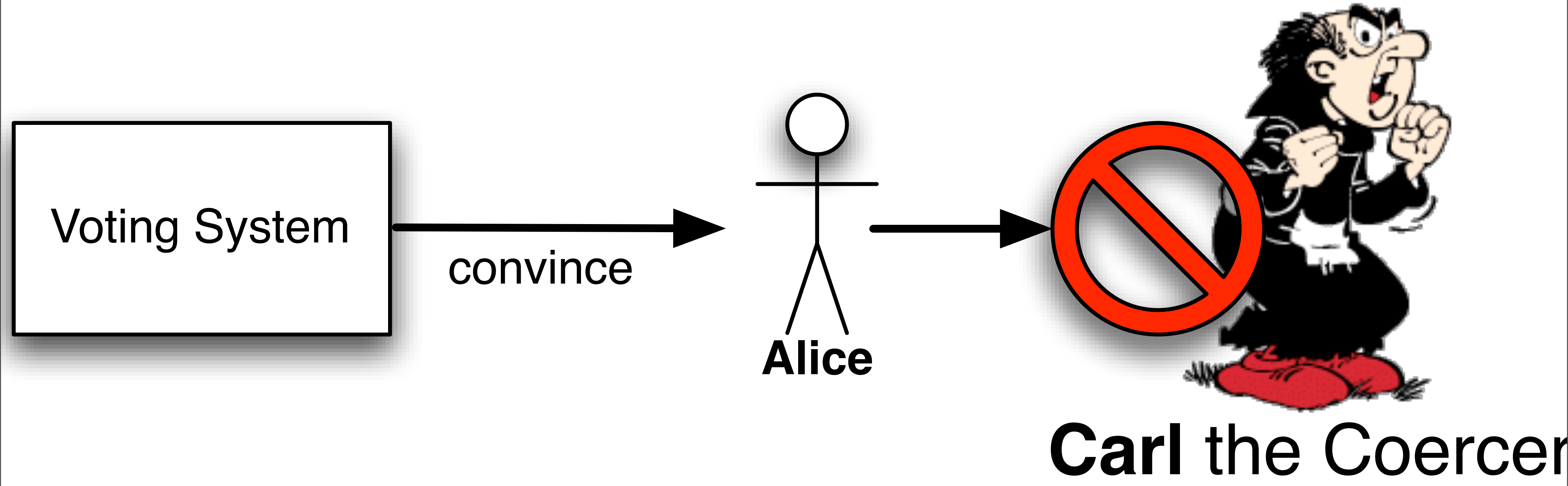
The Point of An Election

“The People have spoken....
the bastards!”

Dick Tuck
1966 Concession Speech

Provide enough evidence to convince the loser.

Secret Ballot *vs.* Verifiability



Voting System

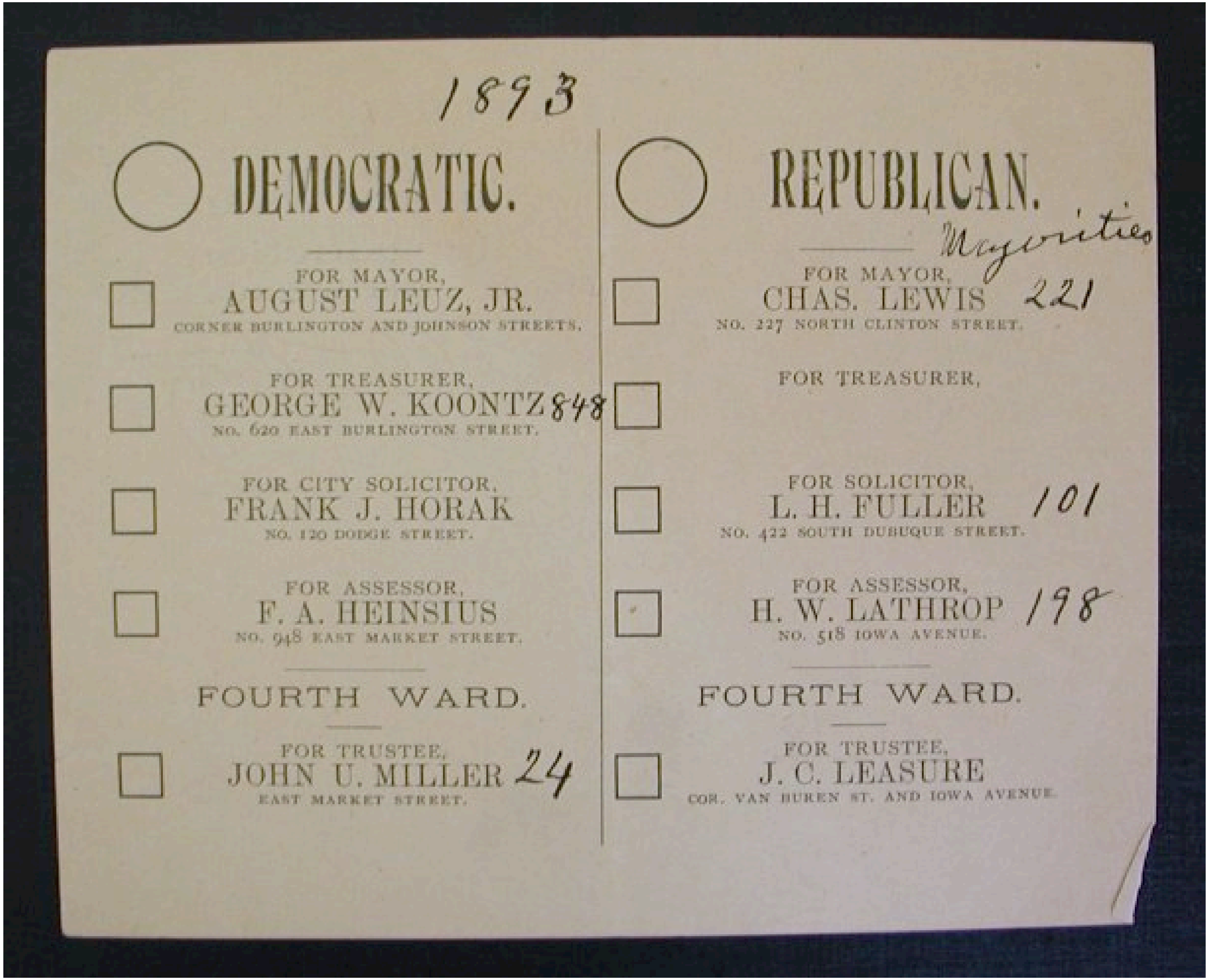
convince

Alice

Carl the Coercer

http://www.cs.uiowa.edu/~jones/voting/pictures/

1892 - Australian Ballot



1893

○ DEMOCRATIC.

FOR MAYOR,
□ AUGUST LEUZ, JR.
CORNER BURLINGTON AND JOHNSON STREETS.

FOR TREASURER,
□ GEORGE W. KOONTZ 848
NO. 620 EAST BURLINGTON STREET.

FOR CITY SOLICITOR,
□ FRANK J. HORAK
NO. 120 DODGE STREET.

FOR ASSESSOR,
□ F. A. HEINSIUS
NO. 948 EAST MARKET STREET.

FOURTH WARD.

FOR TRUSTEE,
□ JOHN U. MILLER 24
EAST MARKET STREET.

○ REPUBLICAN.

Majorities

FOR MAYOR,
□ CHAS. LEWIS 221
NO. 227 NORTH CLINTON STREET.

FOR TREASURER,
□

FOR SOLICITOR,
□ L. H. FULLER 101
NO. 422 SOUTH DUBUQUE STREET.

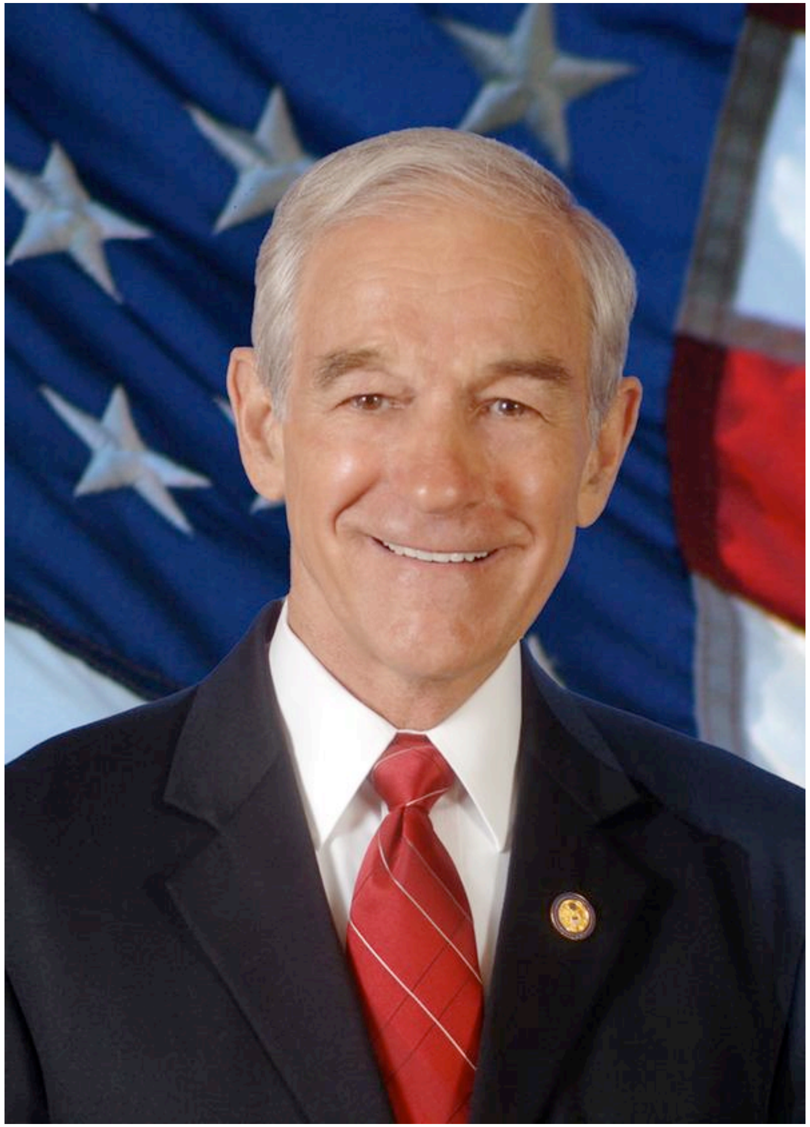
FOR ASSESSOR,
□ H. W. LATHROP 198
NO. 518 IOWA AVENUE.

FOURTH WARD.

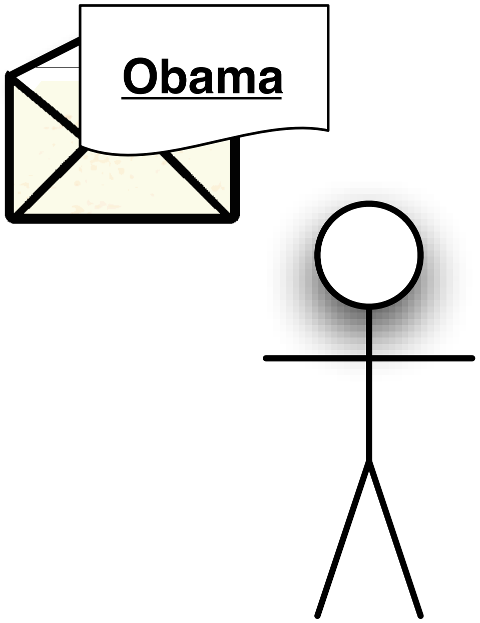
FOR TRUSTEE,
□ J. C. LEASURE
COR. VAN BUREN ST. AND IOWA AVENUE.

http://www.cs.uiowa.edu/~jones/voting/pictures/

Election 2008

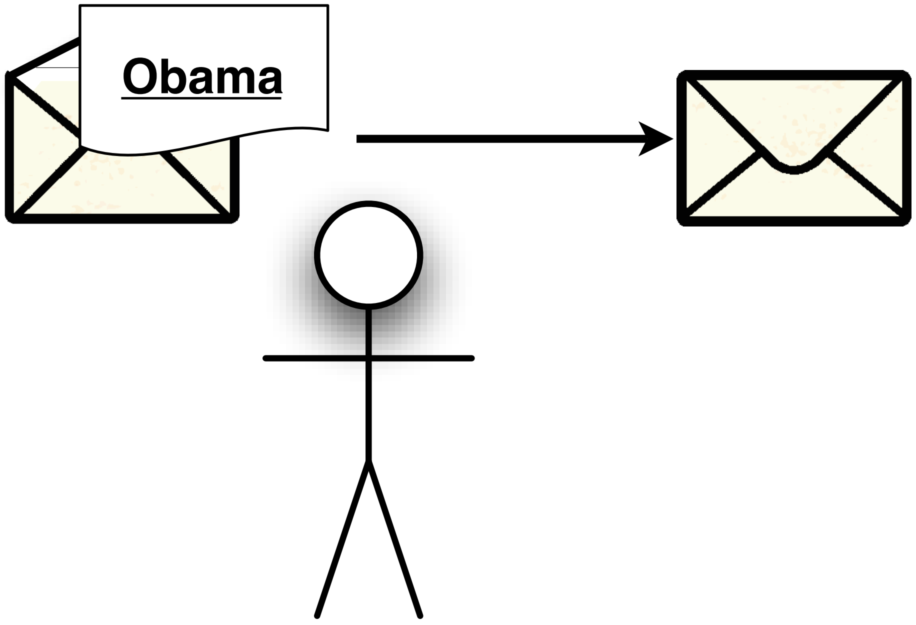


The Ballot Handoff



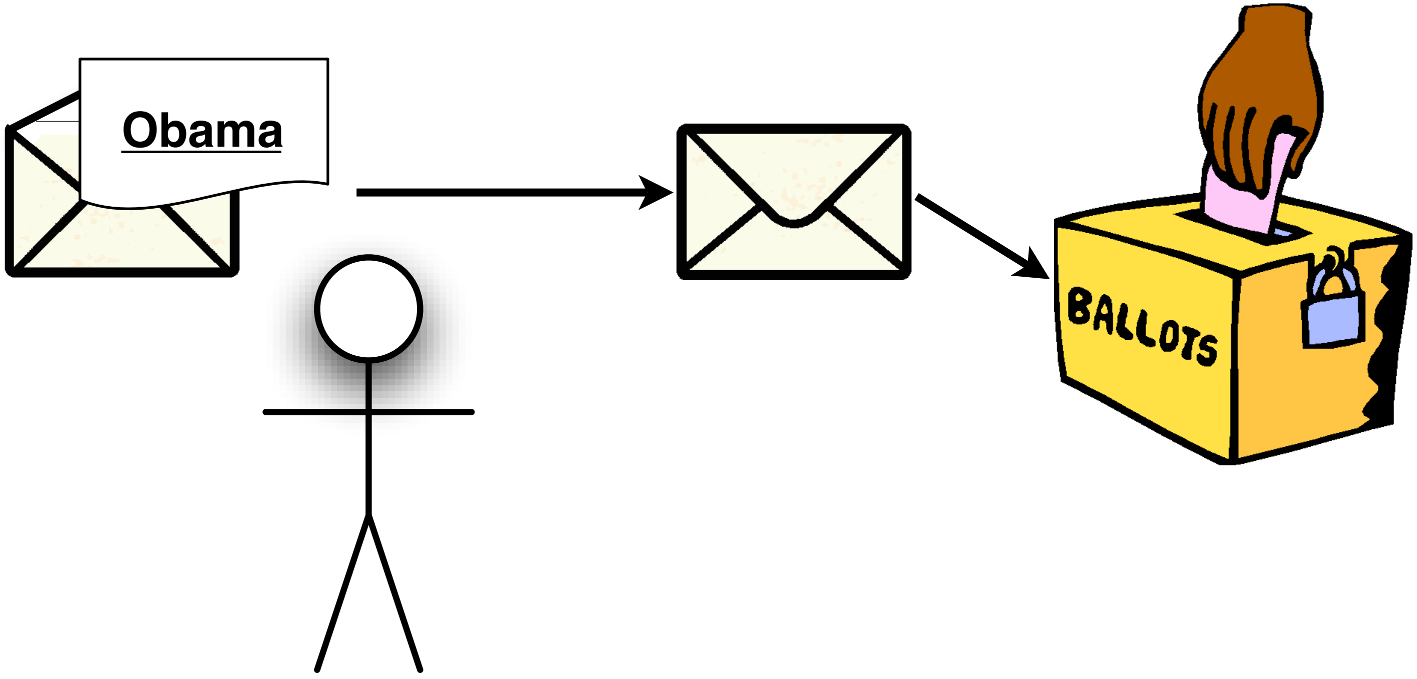
Alice the Voter

The Ballot Handoff



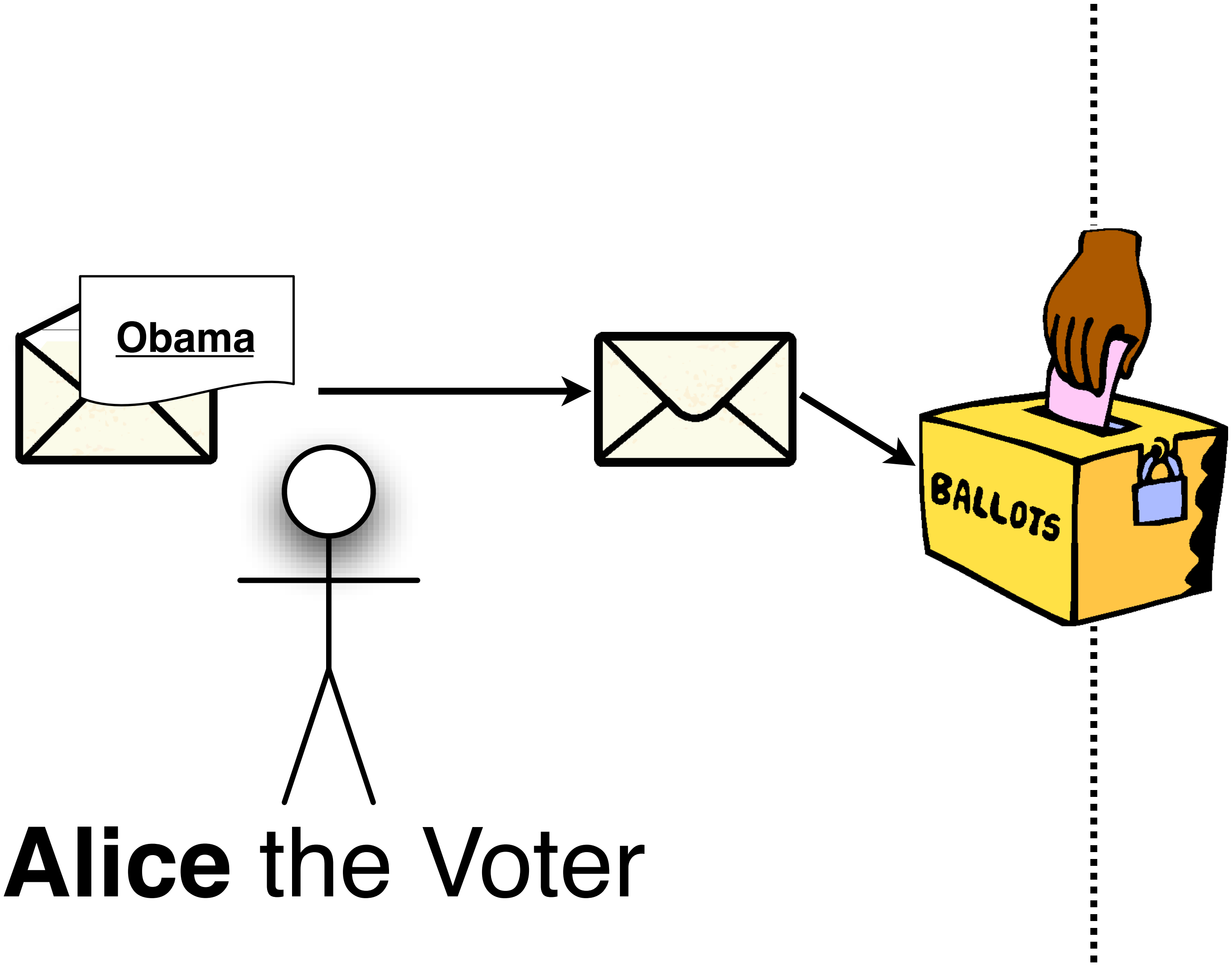
Alice the Voter

The Ballot Handoff



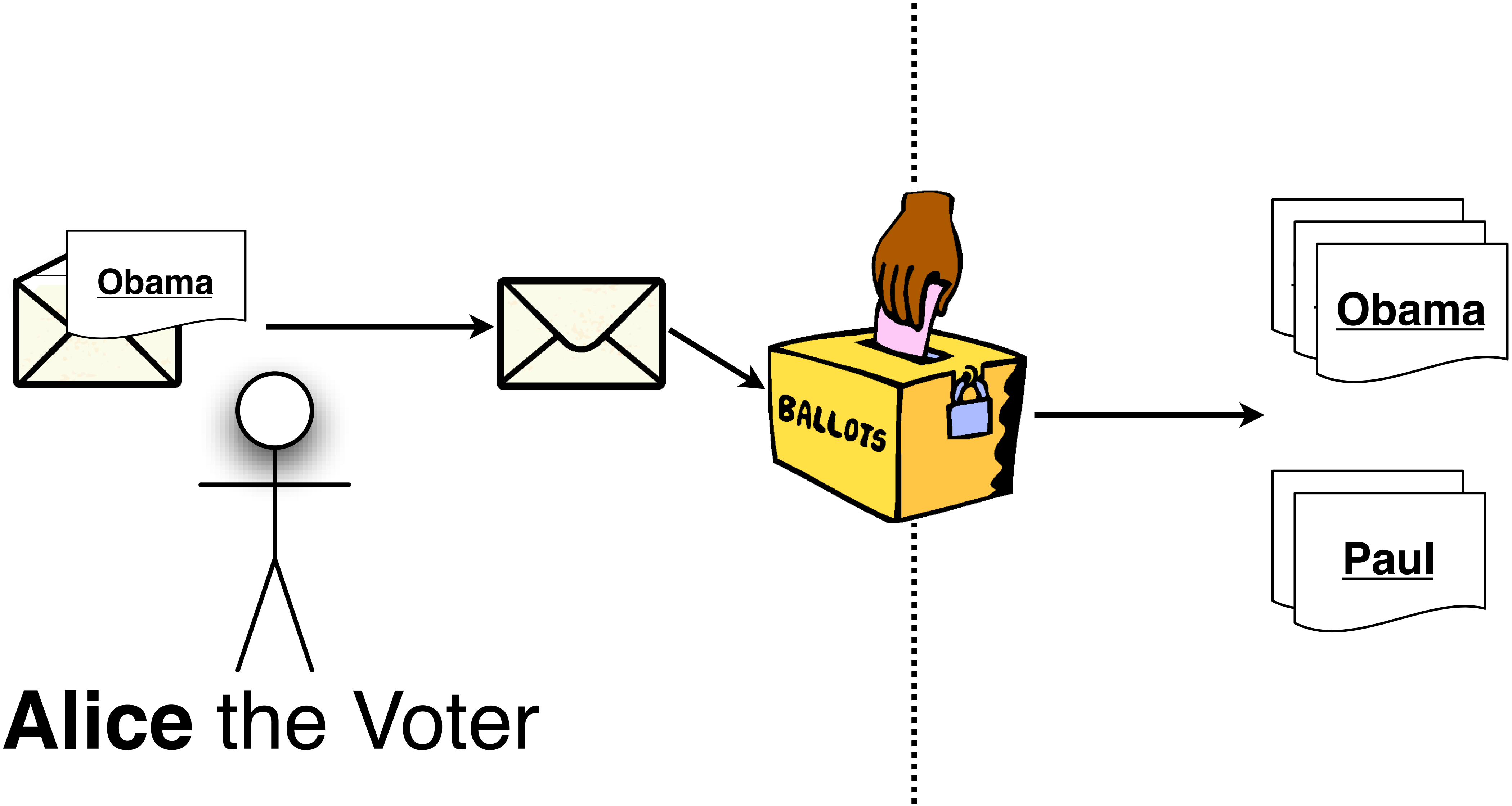
Alice the Voter

The Ballot Handoff



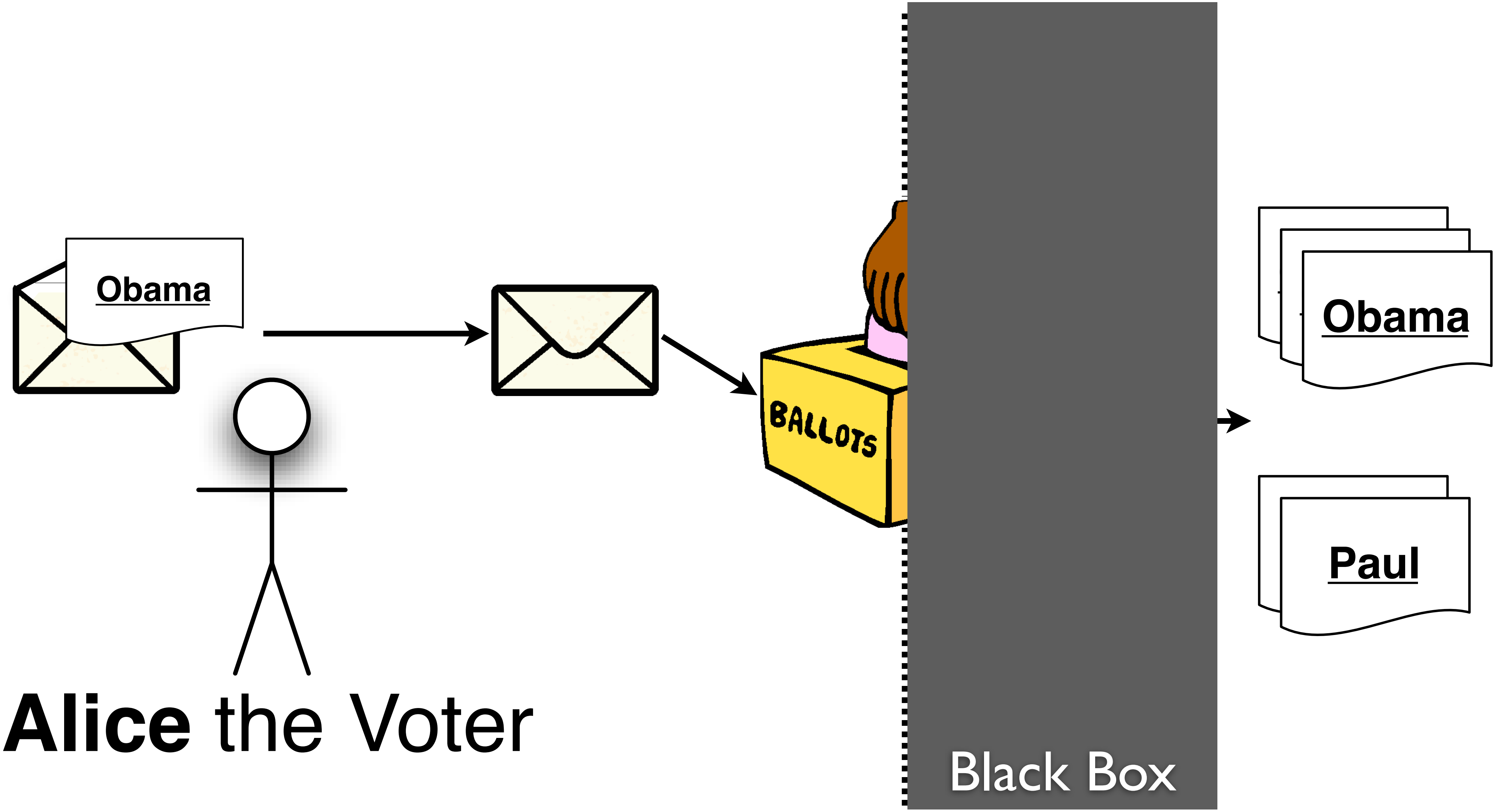
Alice the Voter

The Ballot Handoff



Alice the Voter

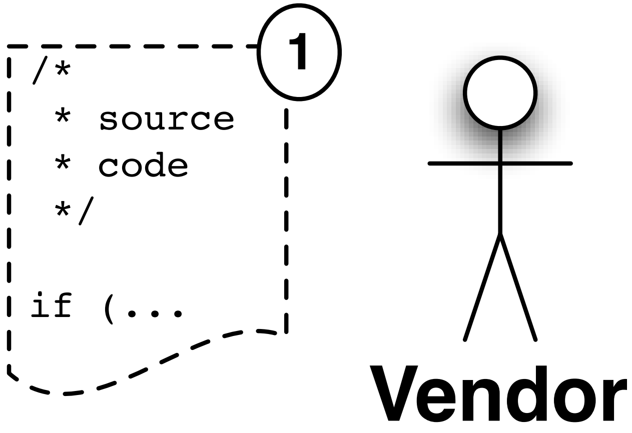
The Ballot Handoff



Alice the Voter

Chain of Custody

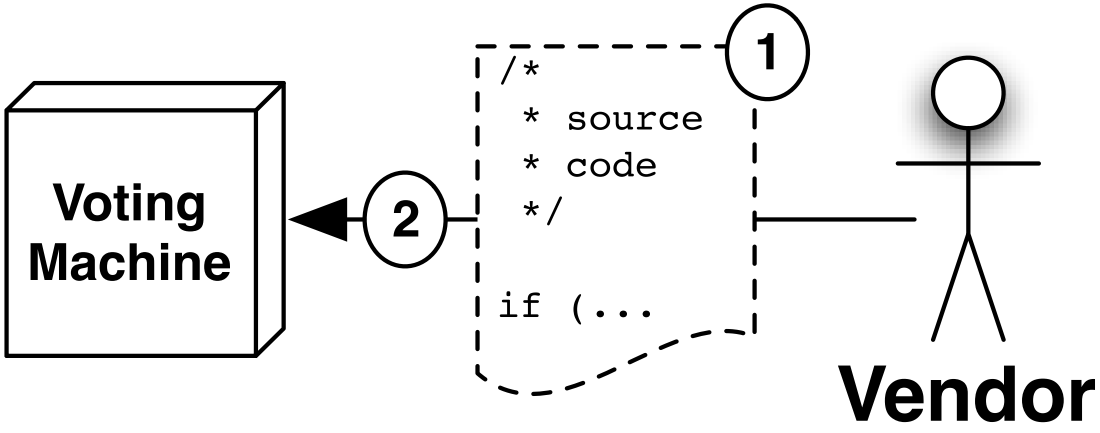
Chain of Custody



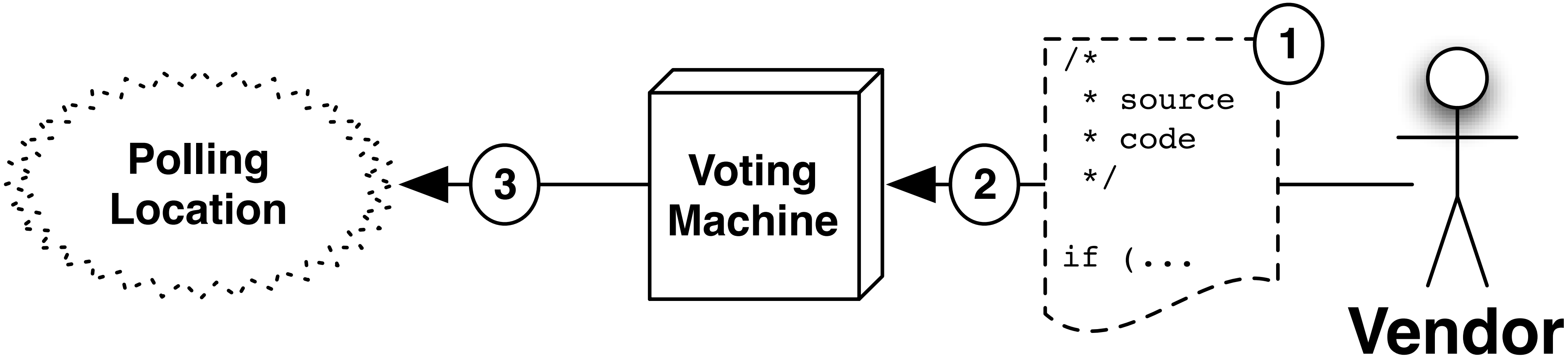
```
/*
 * source
 * code
 */

if (...
```

Chain of Custody



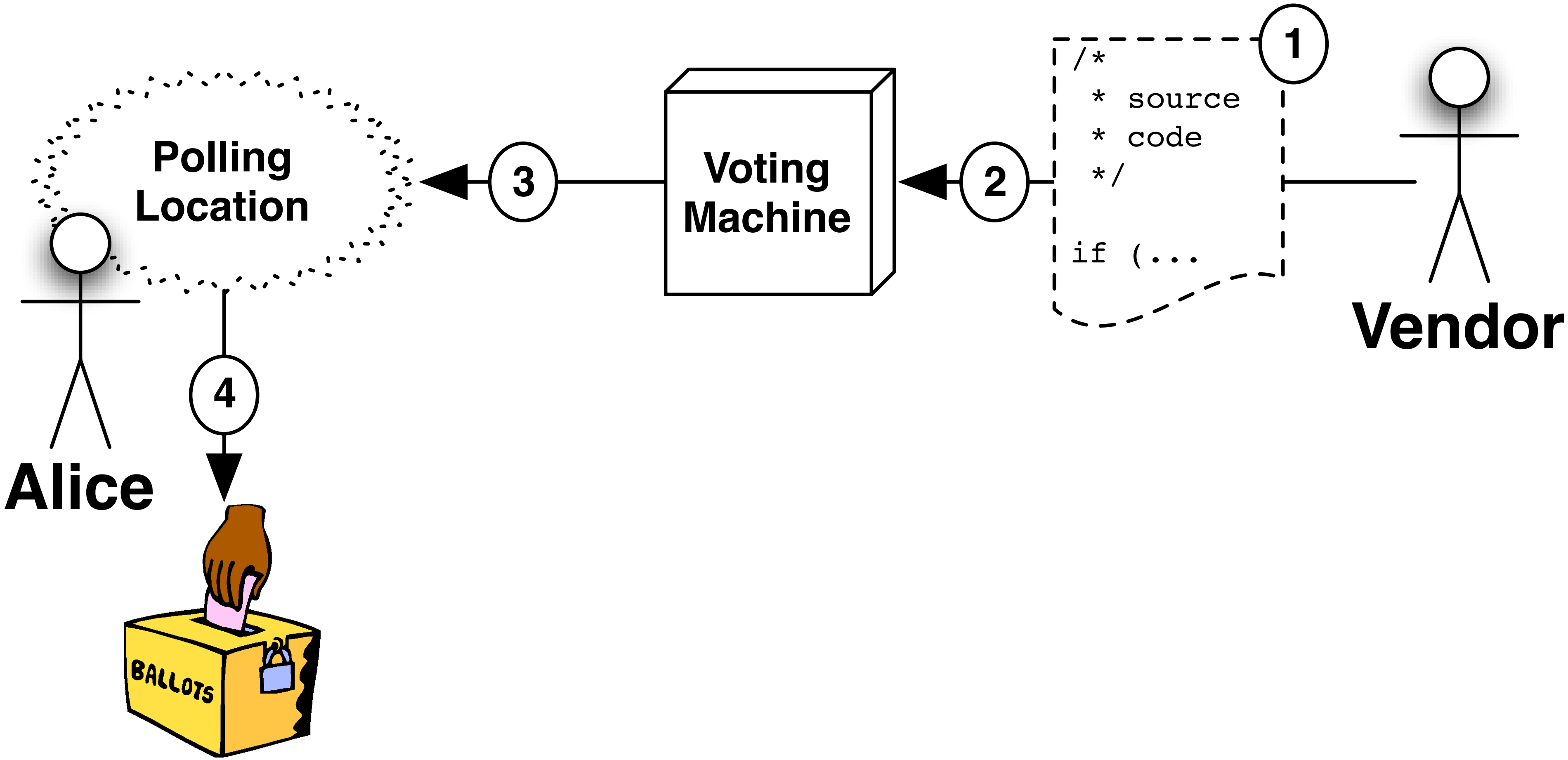
Chain of Custody



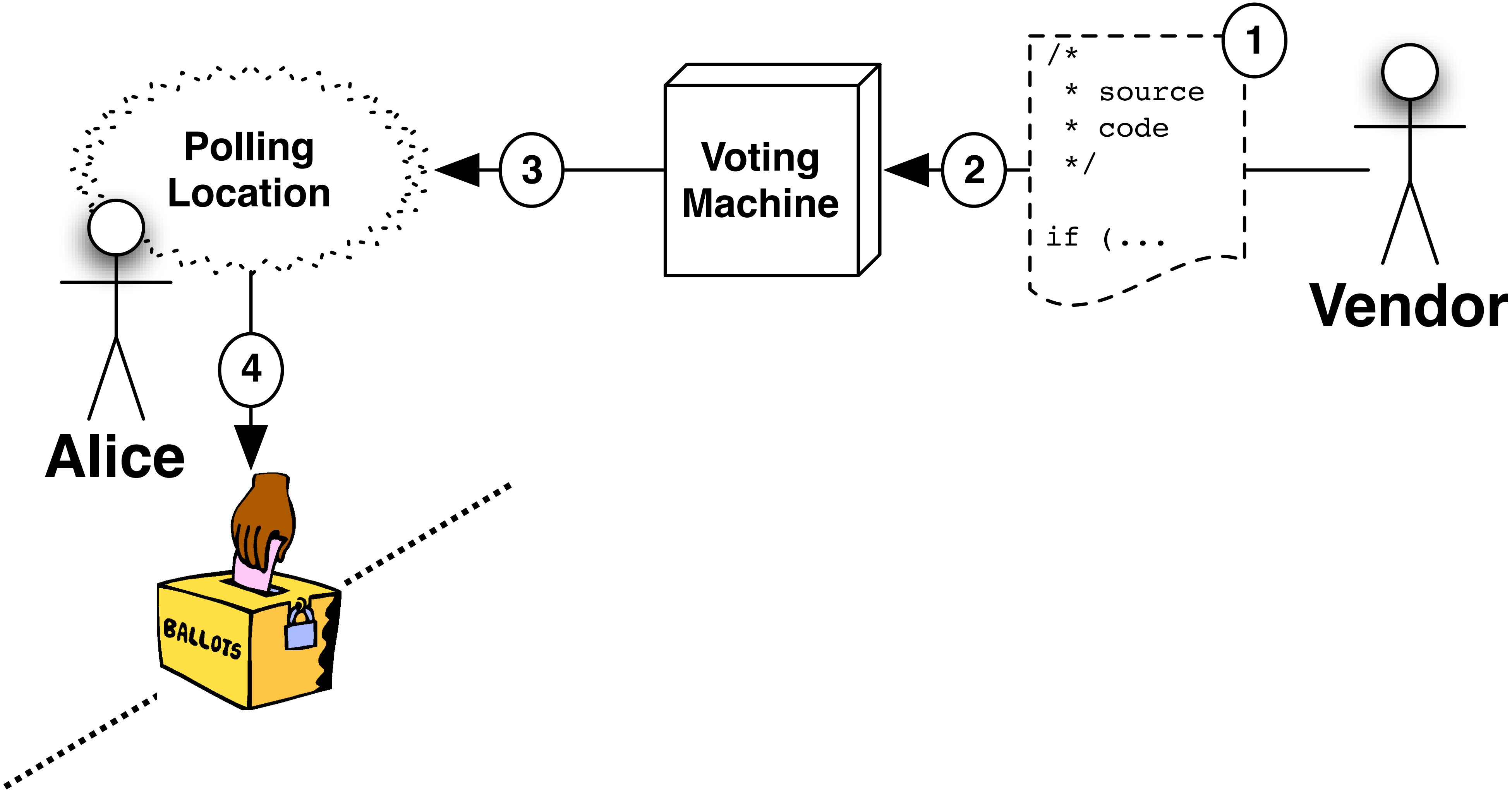
```
/*
 * source
 * code
 */

if (...
```

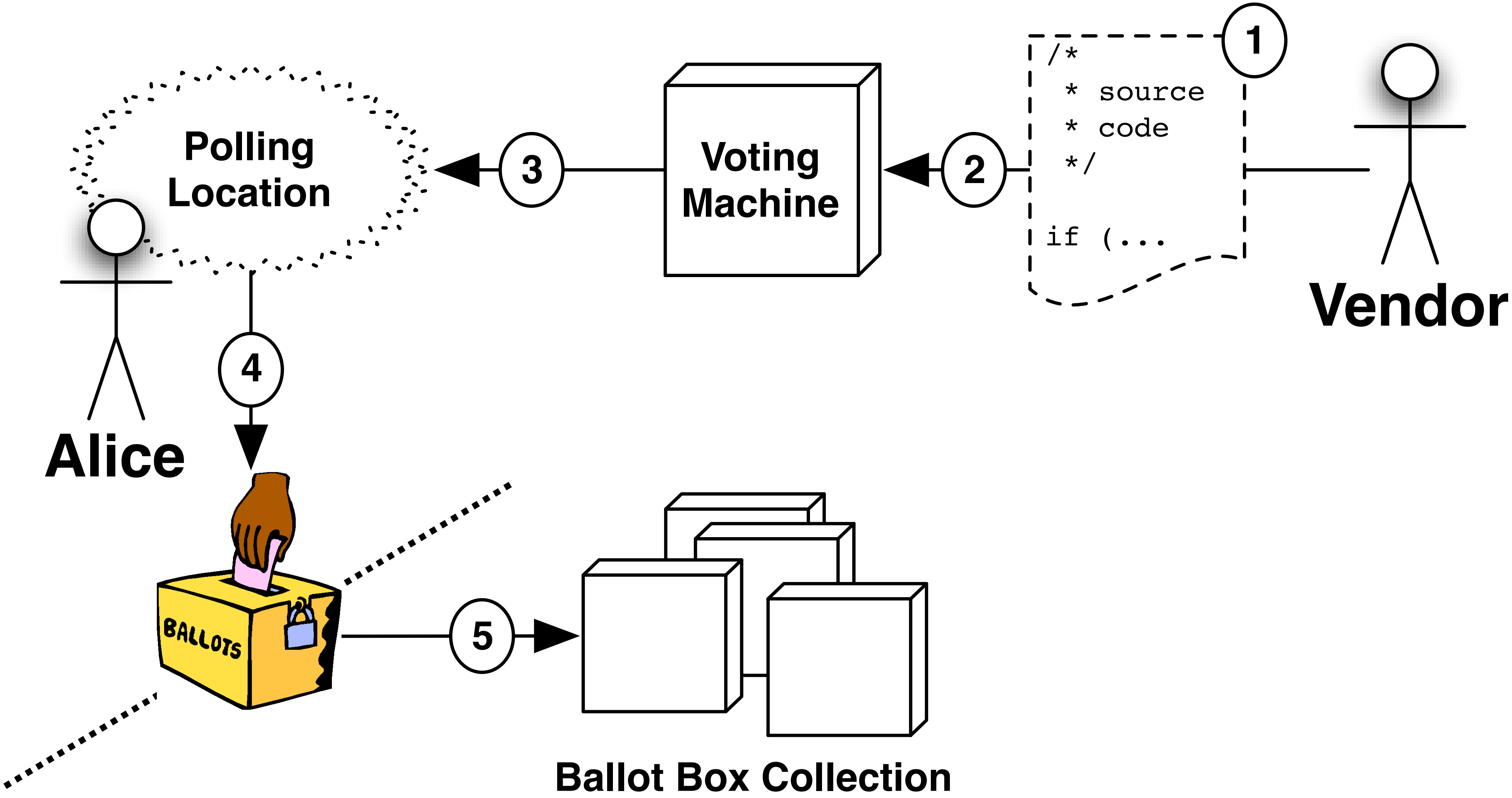
Chain of Custody



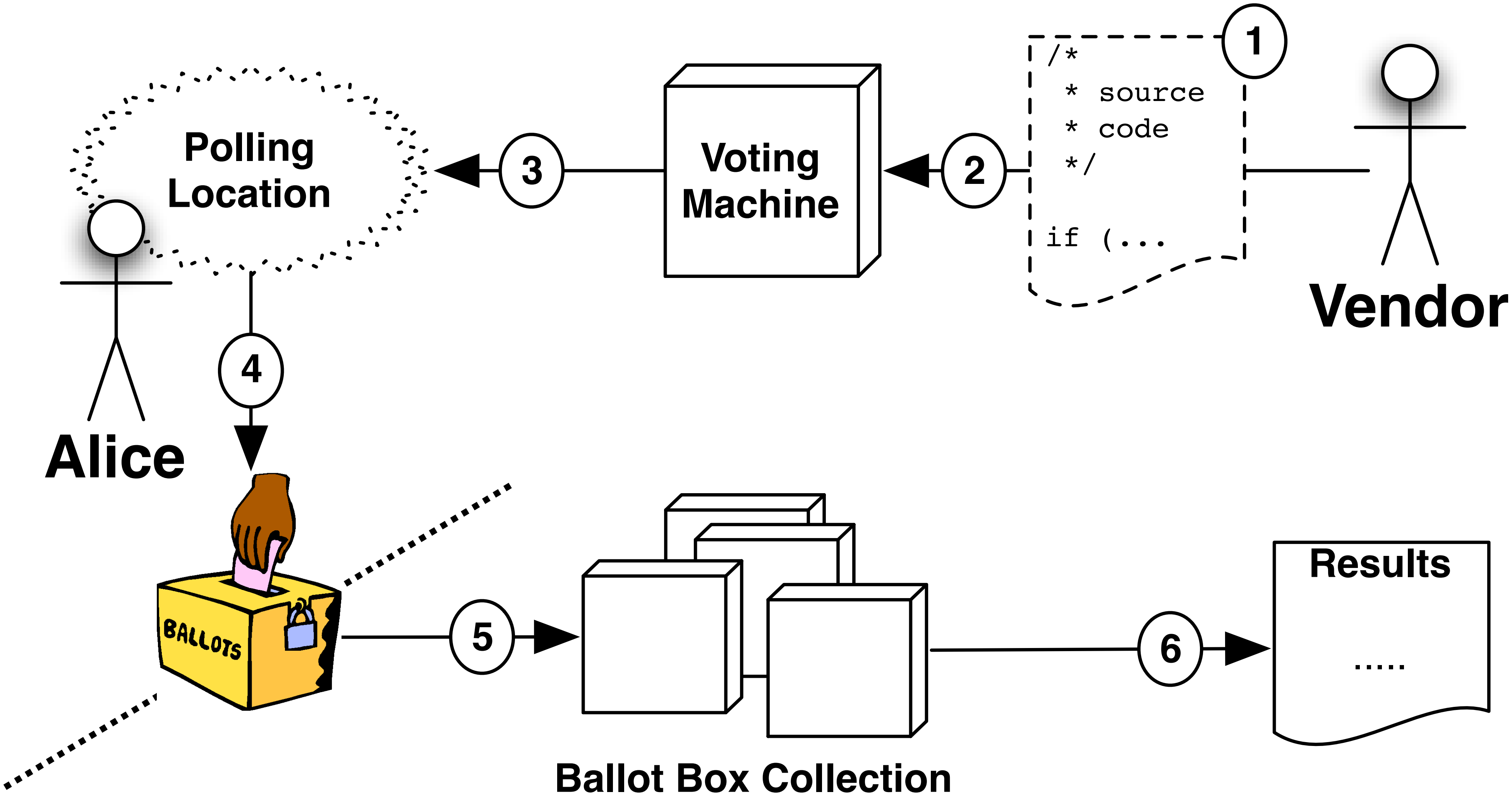
Chain of Custody



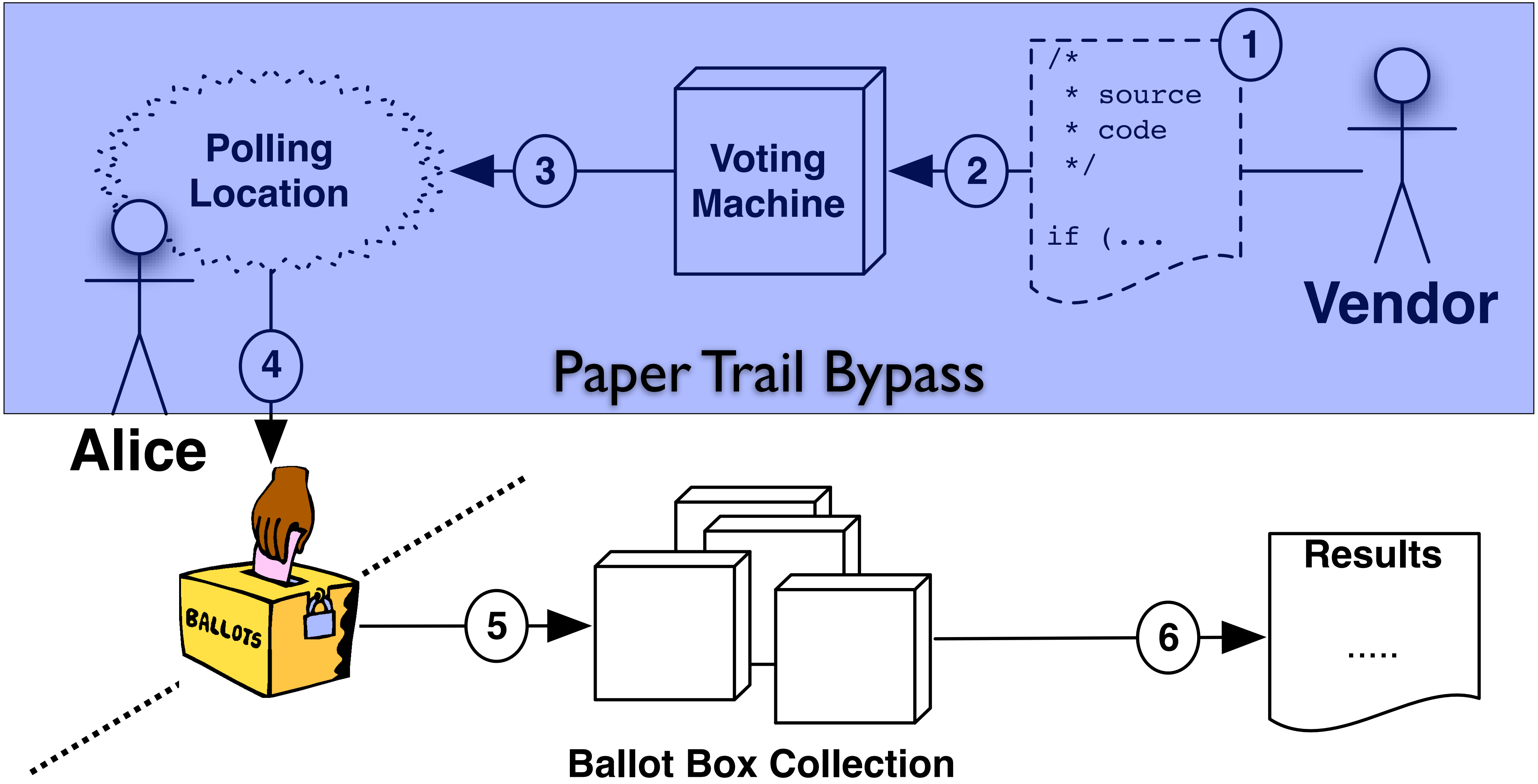
Chain of Custody



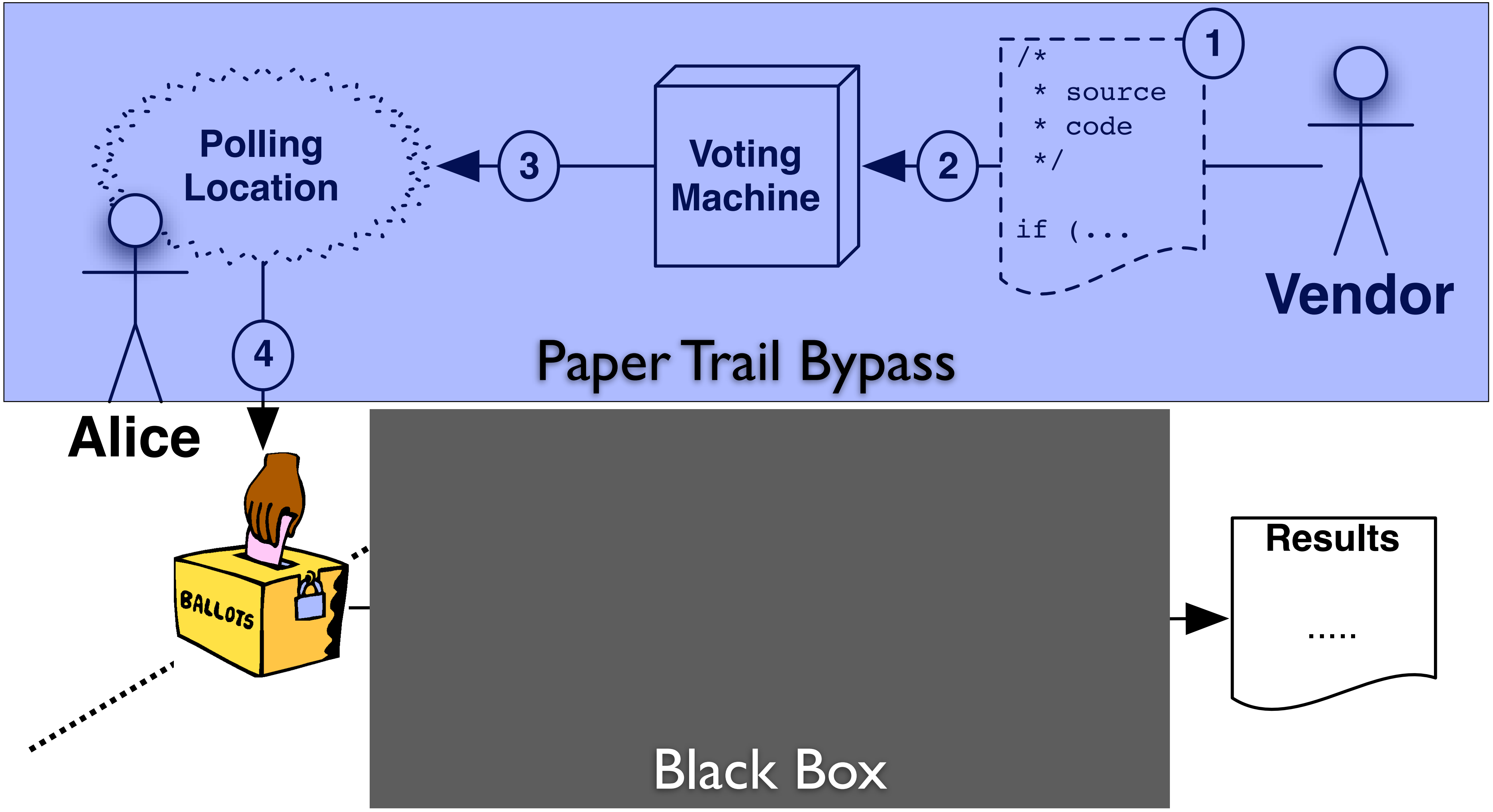
Chain of Custody



Chain of Custody

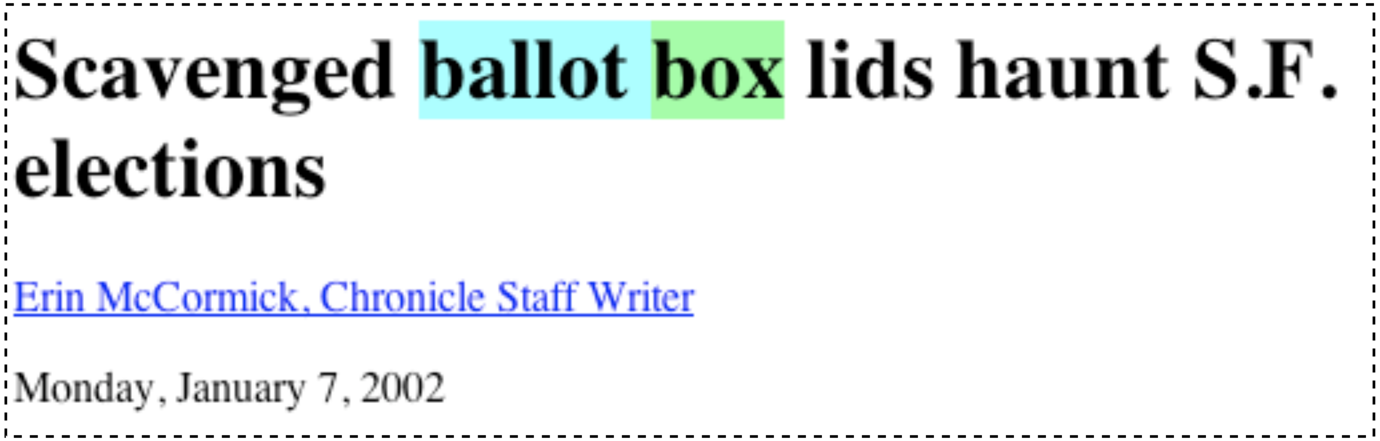


Chain of Custody



The Cost of Secrecy

The Cost of Secrecy

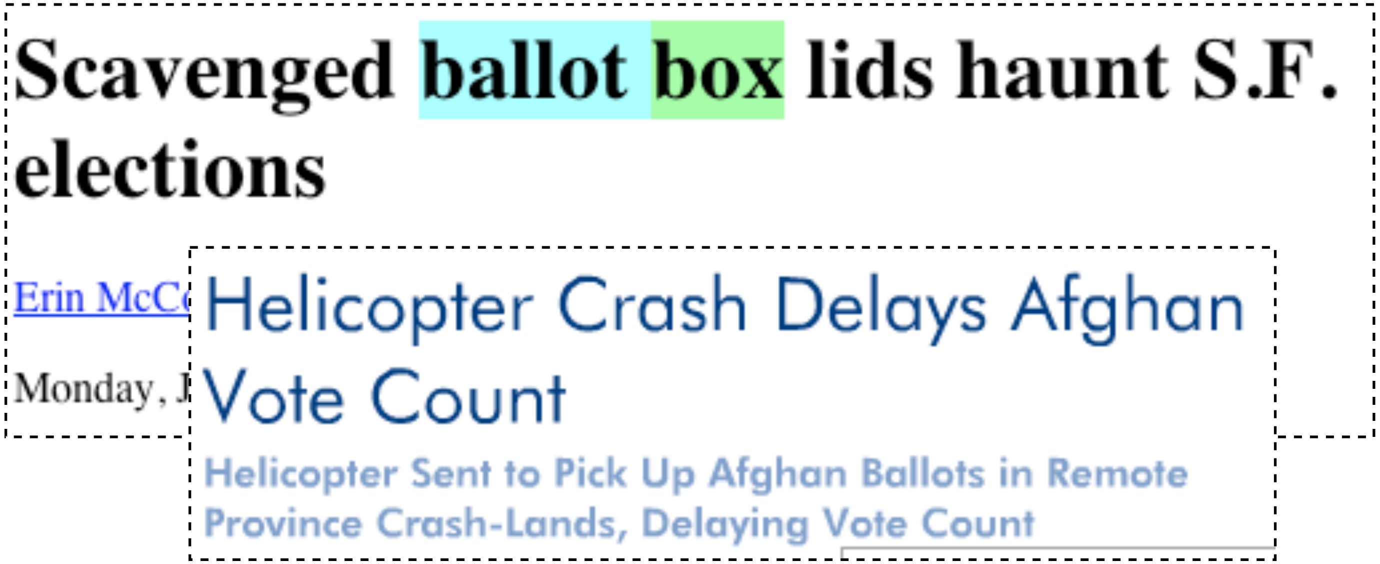


Scavenged ballot box lids haunt S.F. elections

Erin McCormick, Chronicle Staff Writer

Monday, January 7, 2002

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

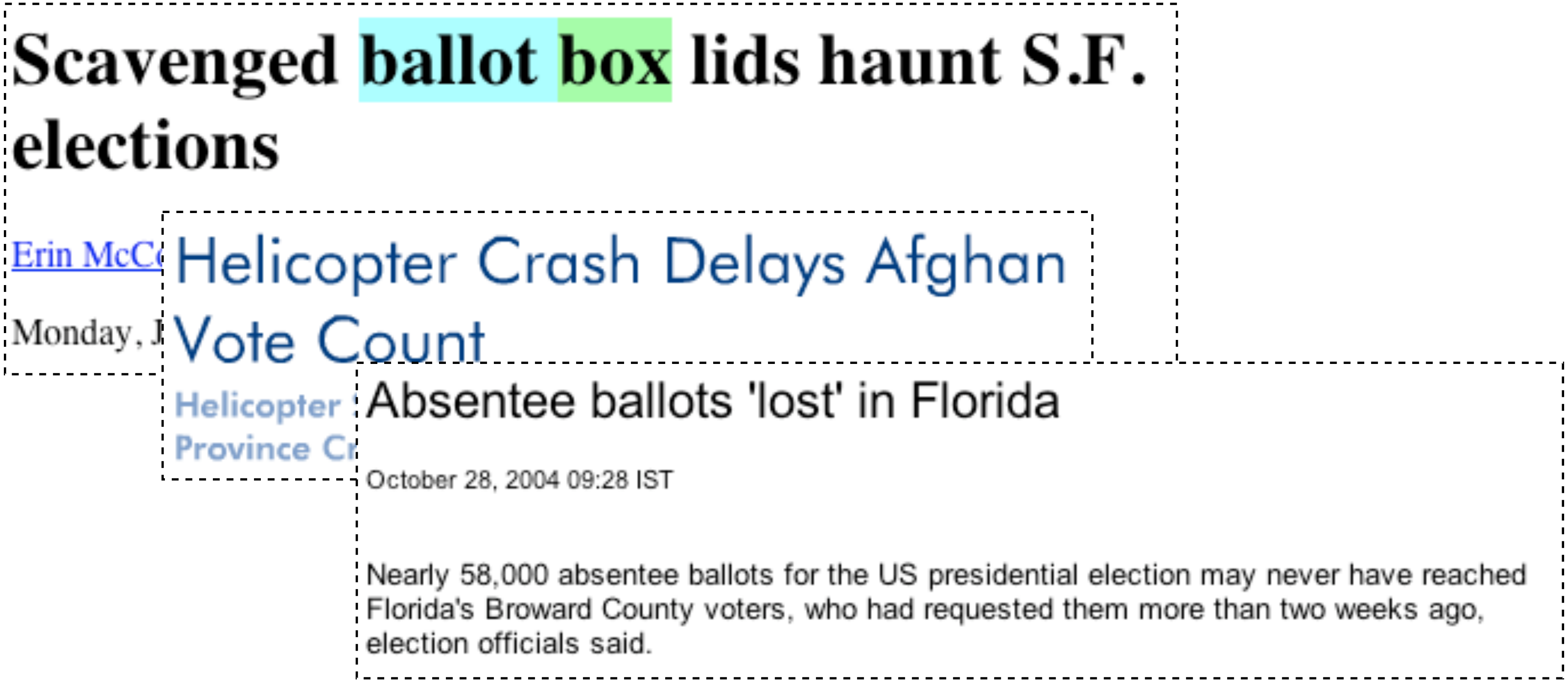
Erin McC

Monday, J

Helicopter Crash Delays Afghan Vote Count

Helicopter Sent to Pick Up Afghan Ballots in Remote Province Crash-Lands, Delaying Vote Count

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, J

Helicopter Crash Delays Afghan Vote Count

Helicopter

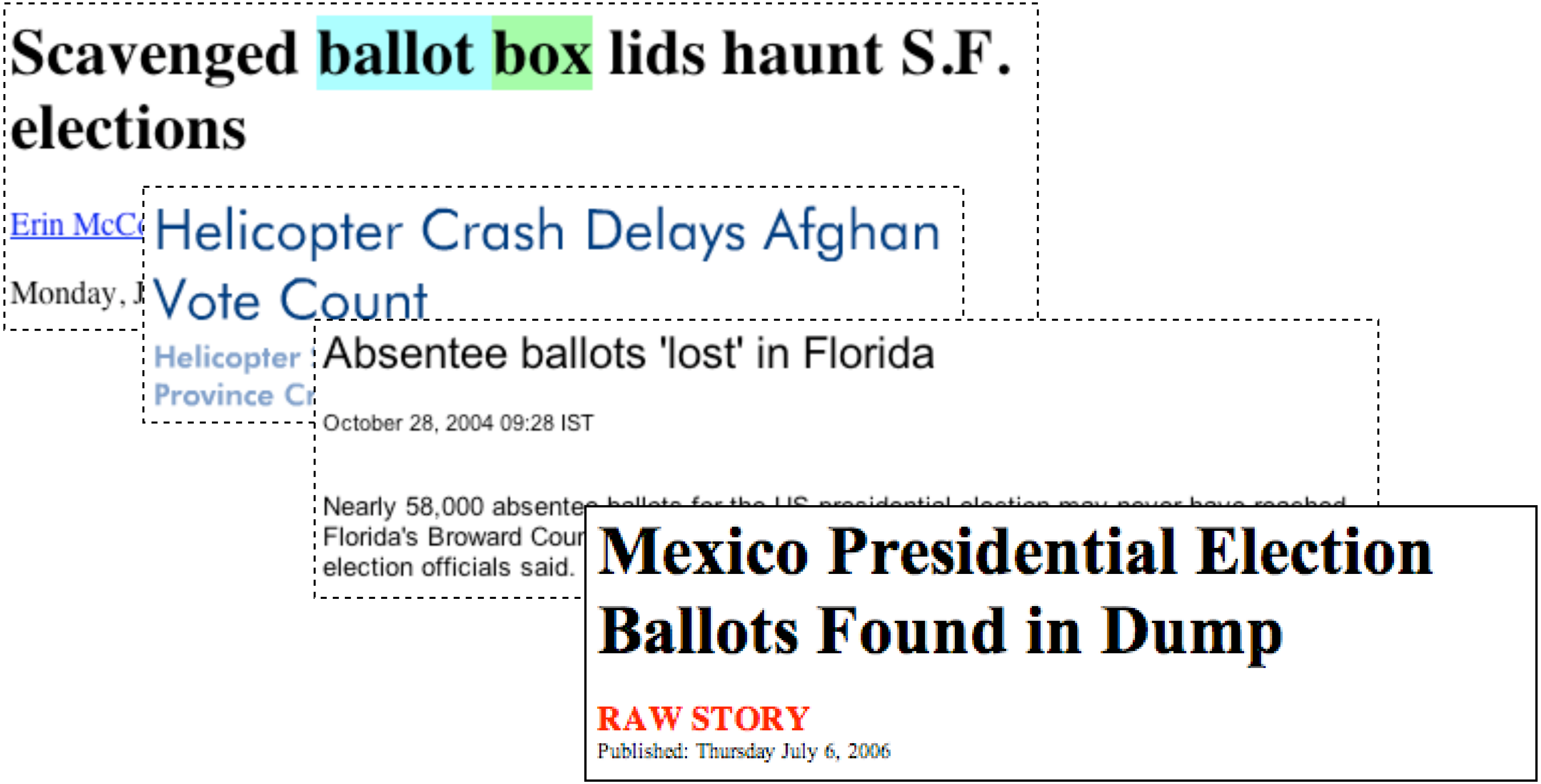
Province Cr

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward County voters, who had requested them more than two weeks ago, election officials said.

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, J

Helicopter Crash Delays Afghan Vote Count

Helicopter

Province Cr

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward Cour

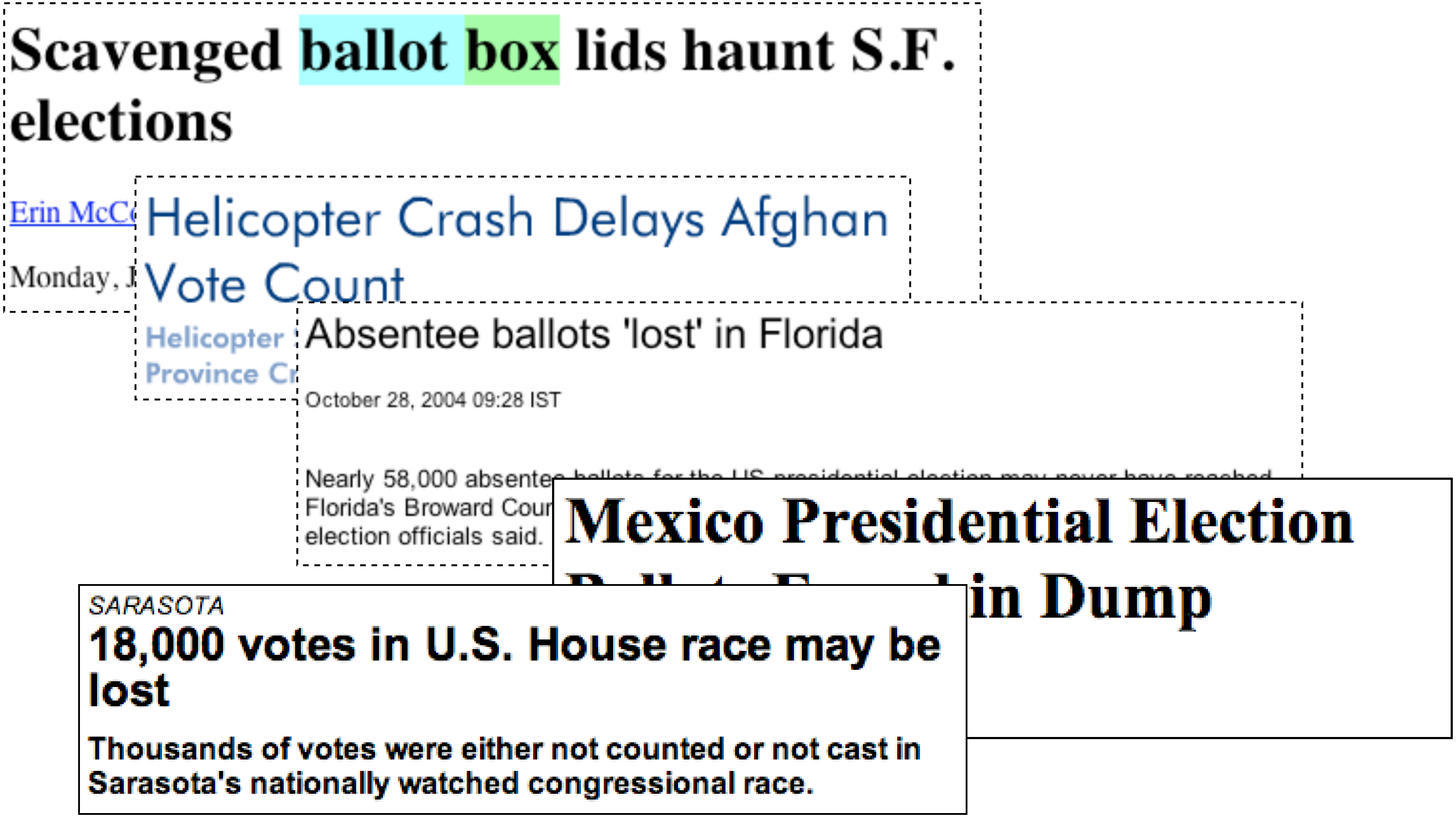
election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY

Published: Thursday July 6, 2006

The Cost of Secrecy



Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, J

Helicopter Crash Delays Afghan Vote Count

Helicopter

Province Cr

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

Nearly 58,000 absente

Florida's Broward Cour

election officials said.

Mexico Presidential Election

in Dump

SARASOTA

18,000 votes in U.S. House race may be lost

Thousands of votes were either not counted or not cast in Sarasota's nationally watched congressional race.

Is Secrecy Important? Actually, it is.

Secret Ballot implemented in Chile in 1958.

"the **secrecy of the ballot** [...] has **first-order implications** for resource allocation, political outcomes, and social efficiency."

[BalandRobinson 2004]

Verifying with Cryptography

[Chaum81], [Benaloh85], [PIK93], [BenalohTuinstra92], [SK94], [Neff2001], [FS2001],[Chaum2004], [Neff2004], [Ryan2004], [Chaum2005]

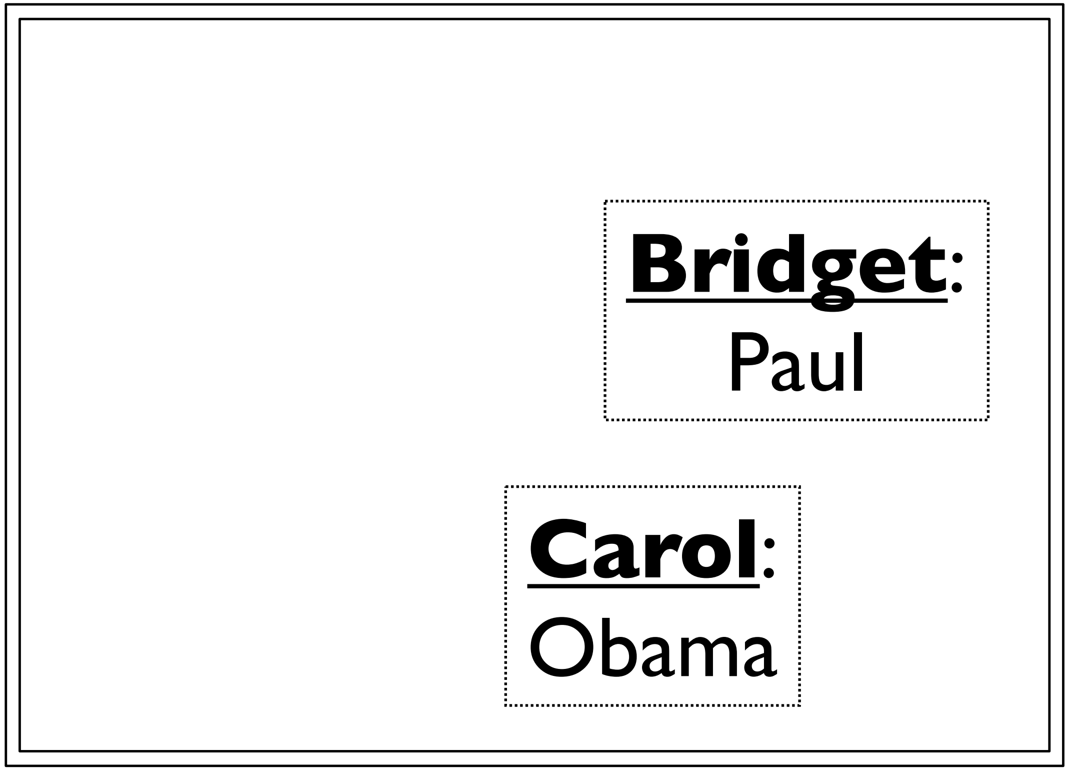
Desired Properties

(1) **Alice** verifies **her vote**.

(2) **Everyone** verifies **tallying**.

(3) Alice **cannot be coerced** by Eve.

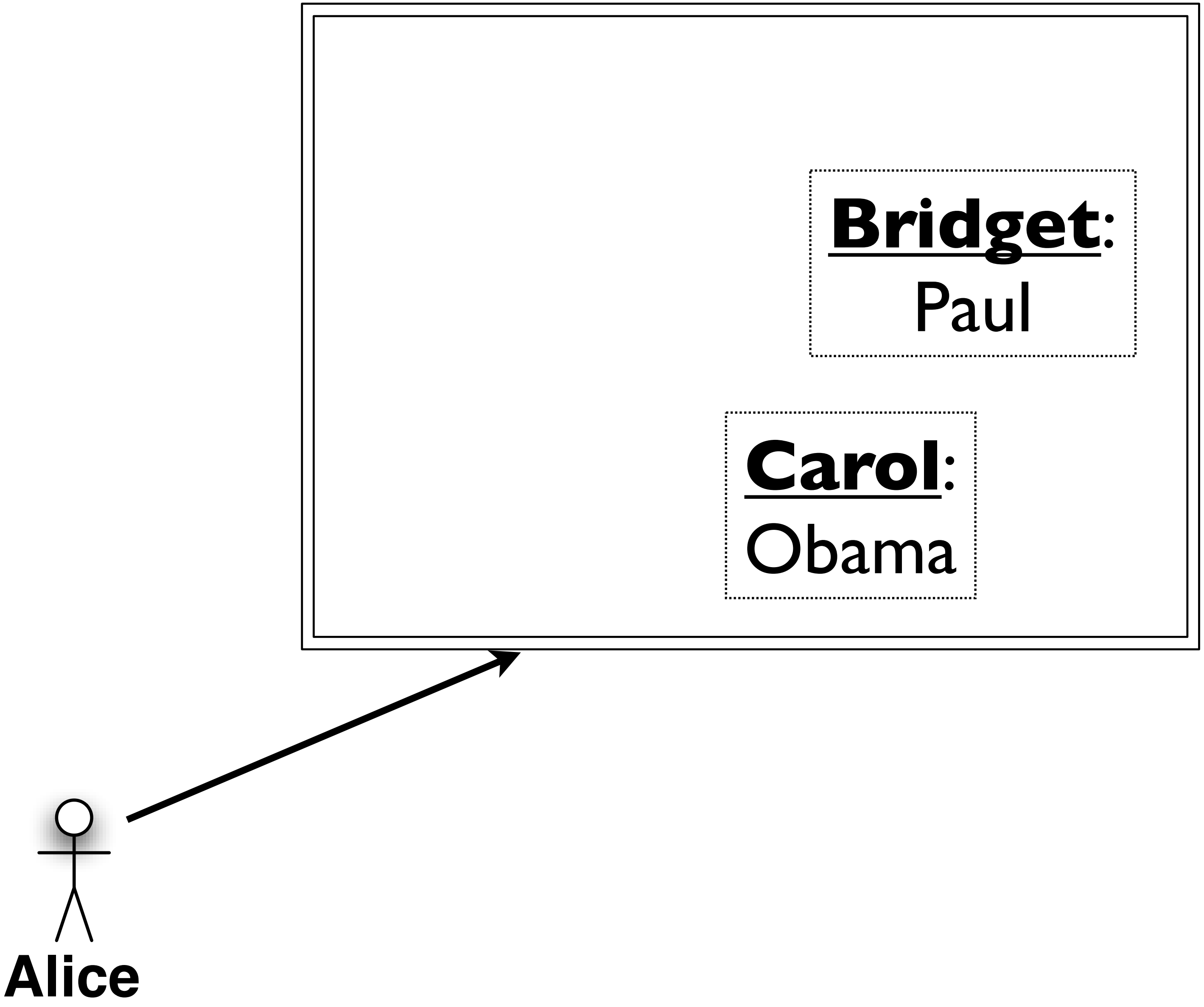
Public Ballots



Bridget:
Paul

Carol:
Obama

Public Ballots

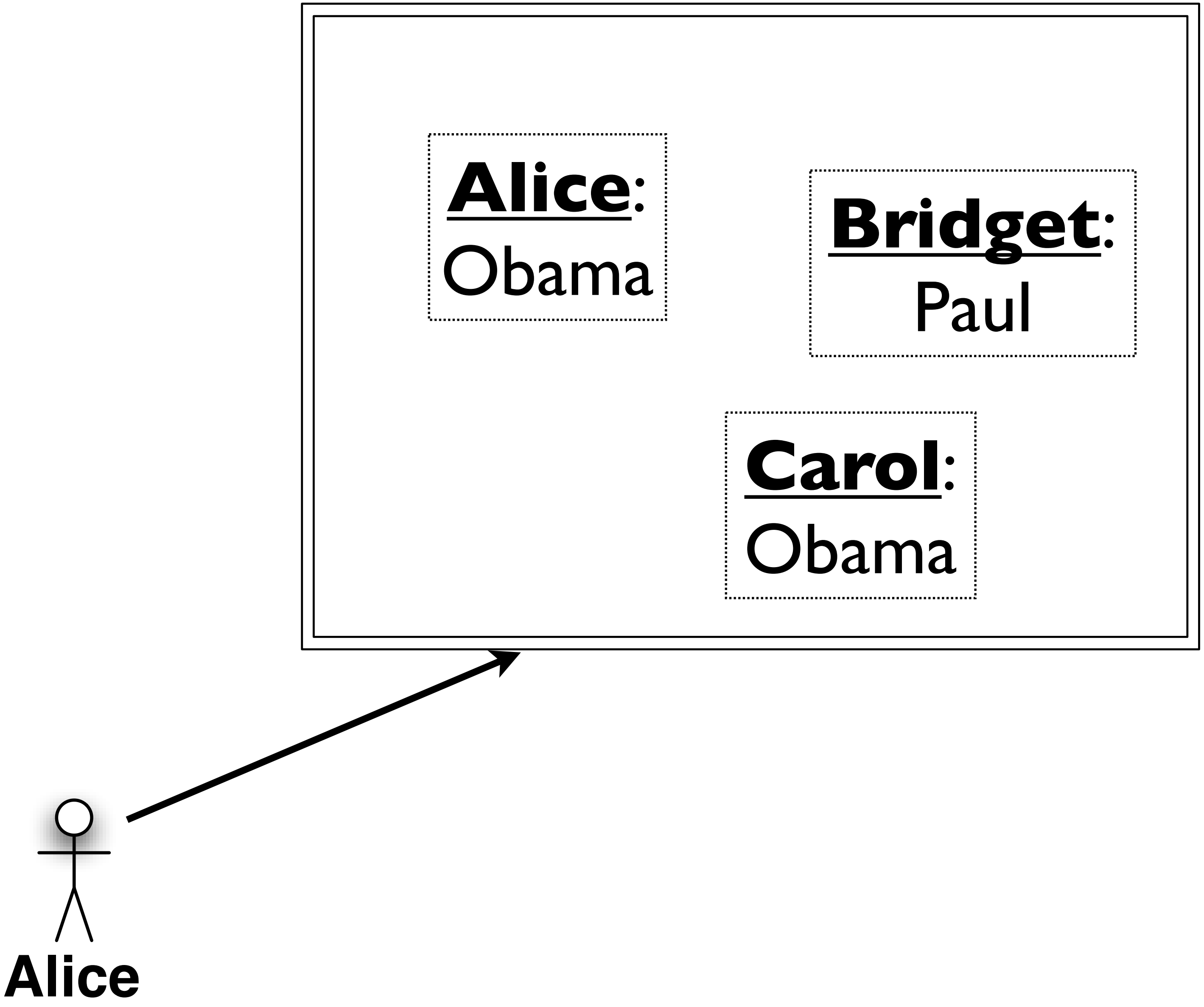


Bridget: Paul

Carol: Obama

Alice

Public Ballots



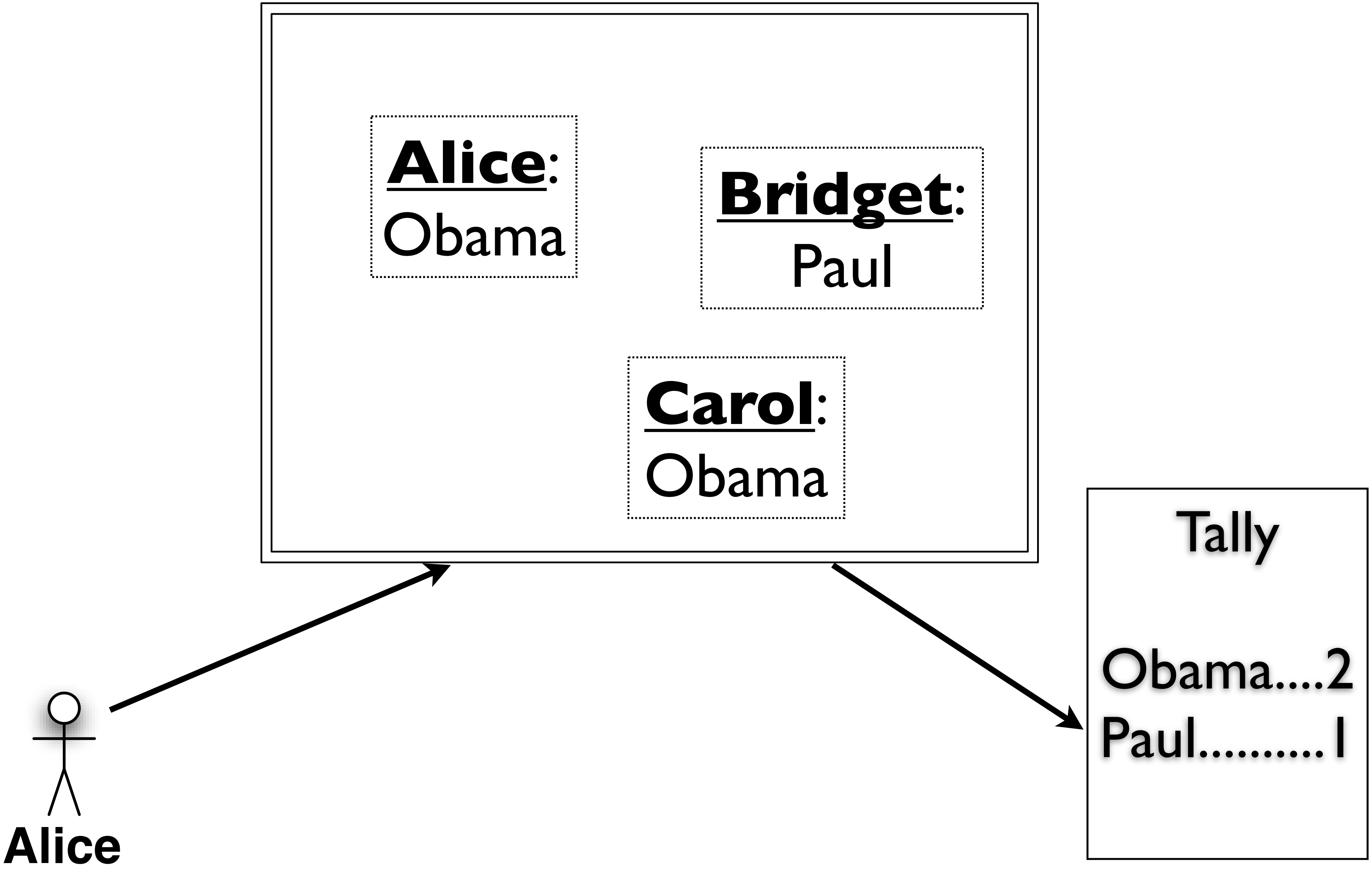
Alice: Obama

Bridget: Paul

Carol: Obama

Alice

Public Ballots



Alice: Obama

Bridget: Paul

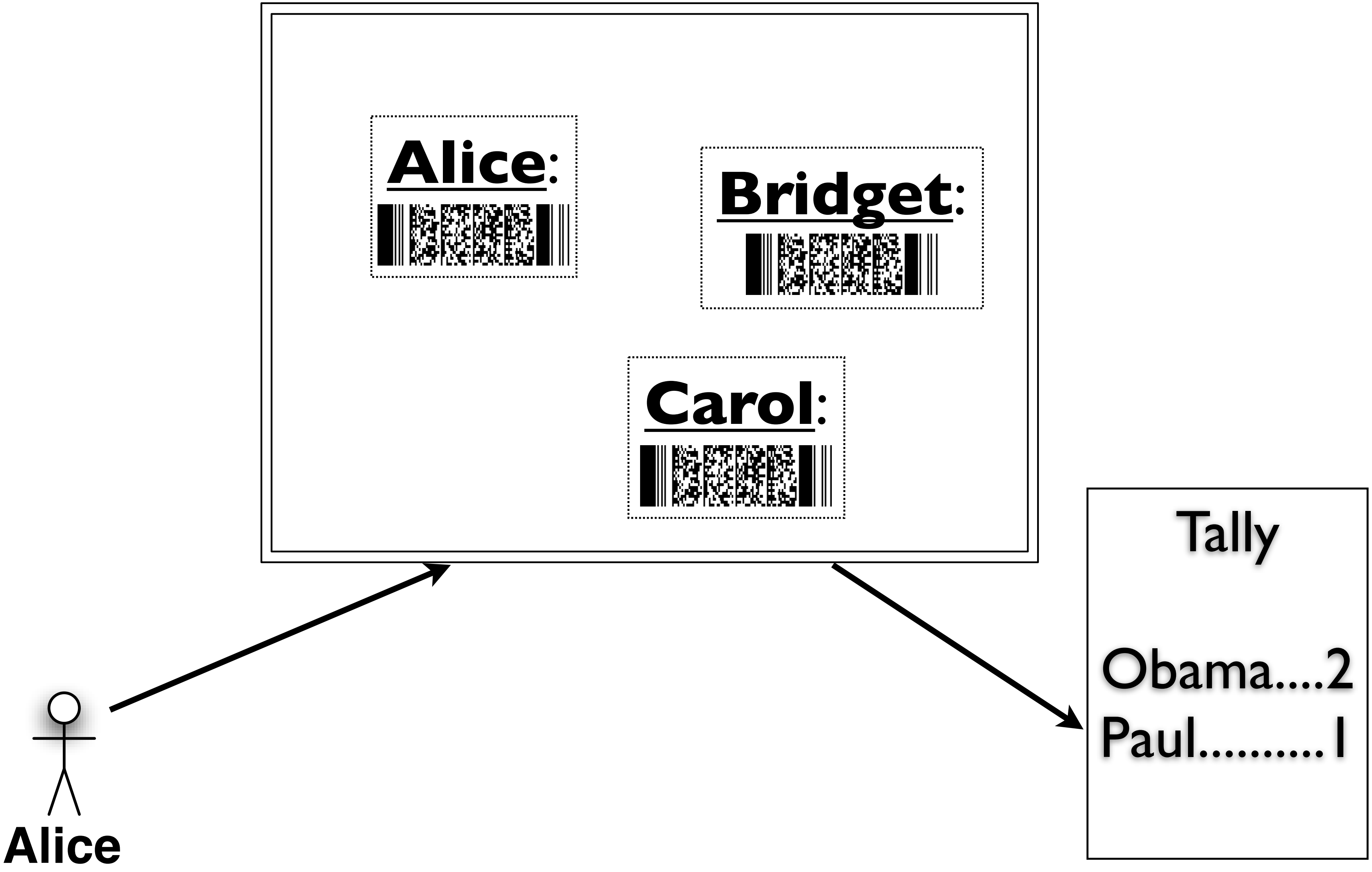
Carol: Obama

Tally

Obama....2
Paul..........1

Alice

Encrypted Public Ballots



Alice:

Bridget:

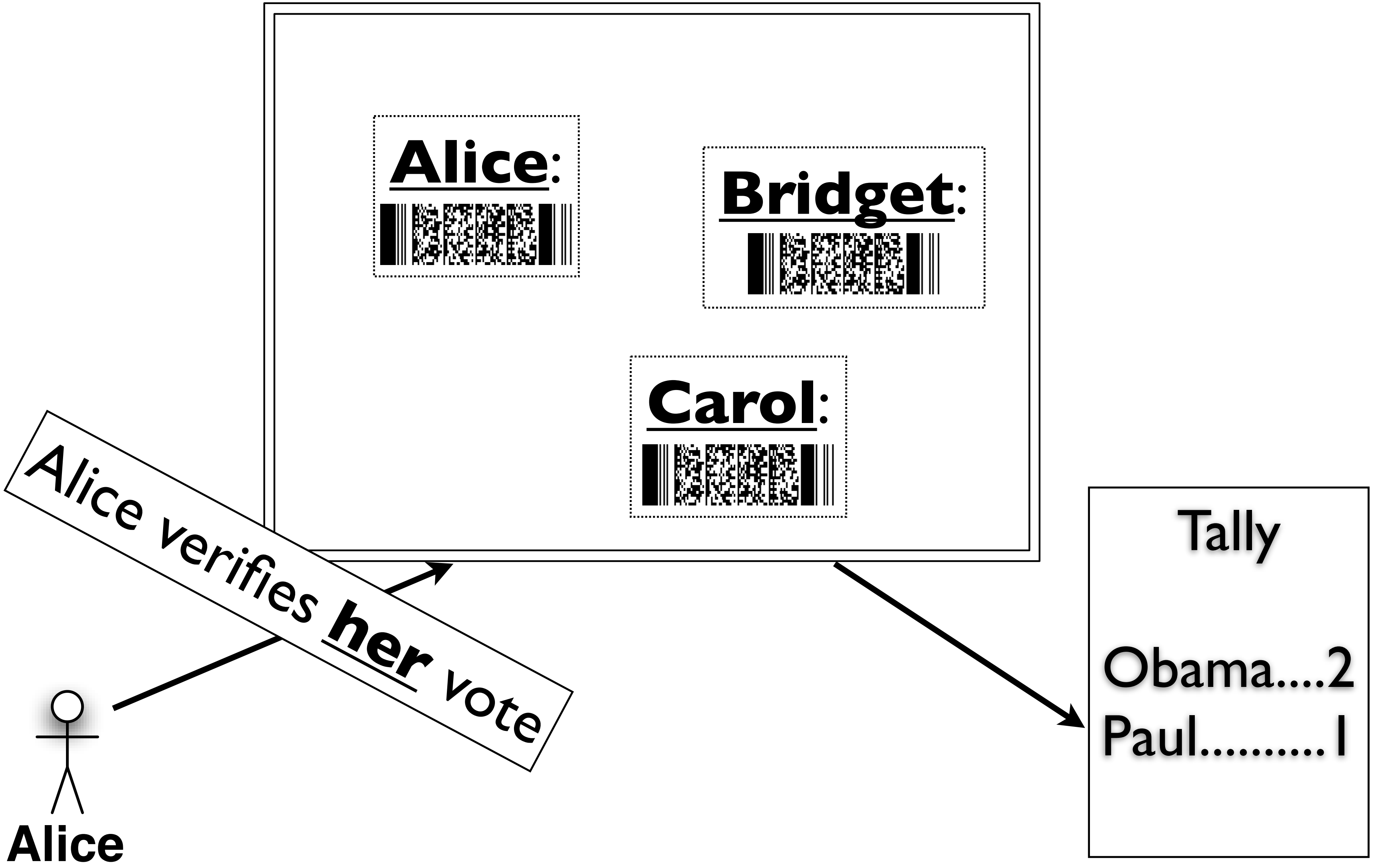
Carol:

Tally

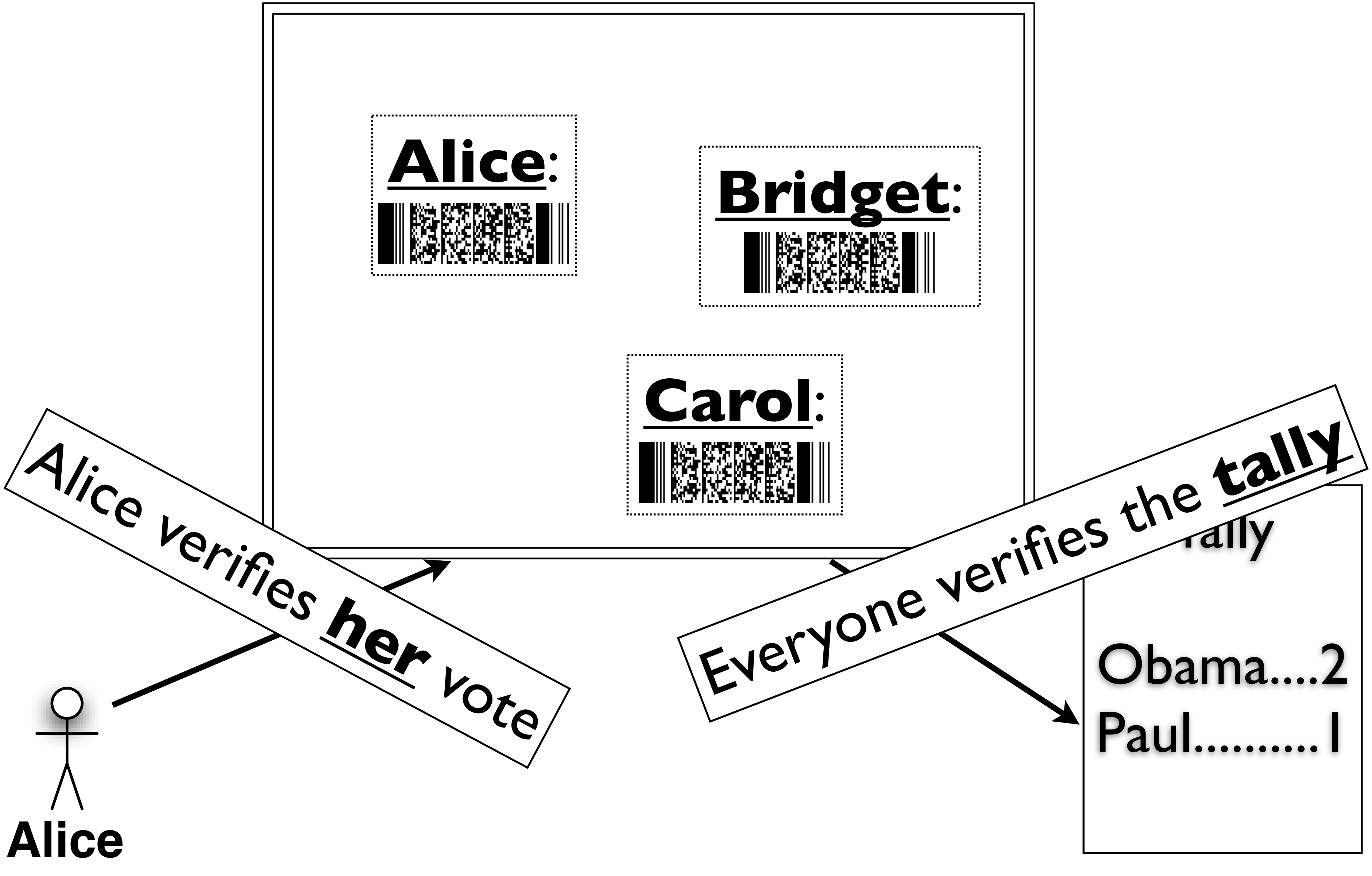
Obama....2
Paul..........1

Alice

Encrypted Public Ballots



Encrypted Public Ballots



Alice:

Bridget:

Carol:

Tally

Obama....2
Paul..........1

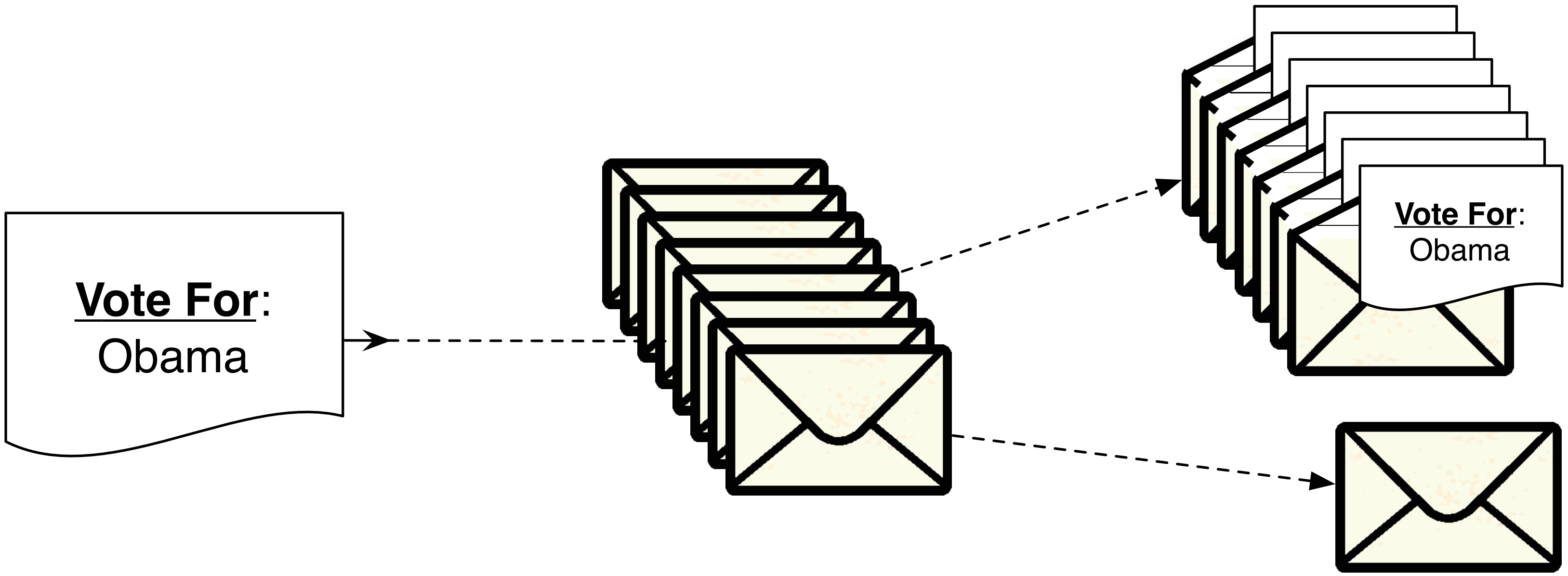
Alice

Alice verifies **her** vote

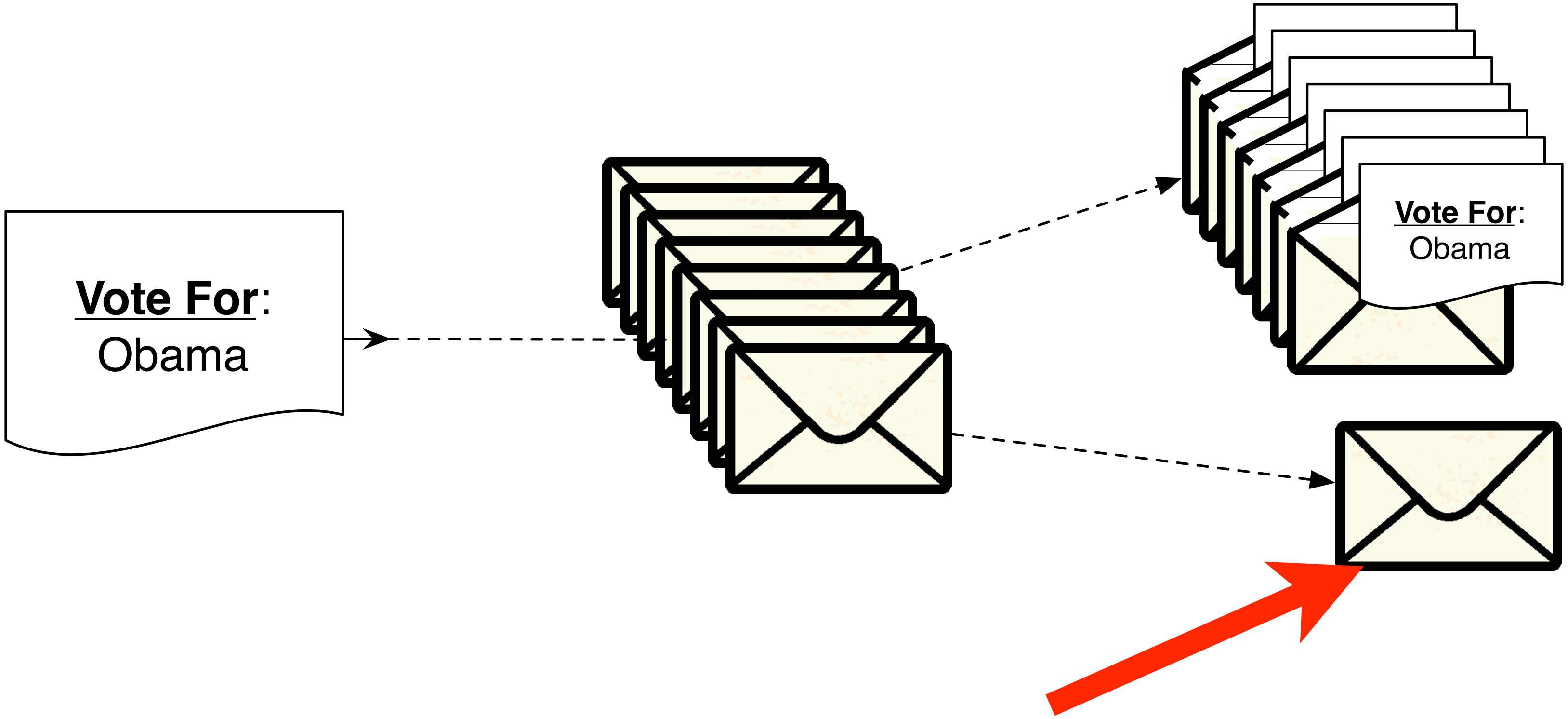
Everyone verifies the **tally**

How can we ***verify*** operations on ***encrypted*** data?

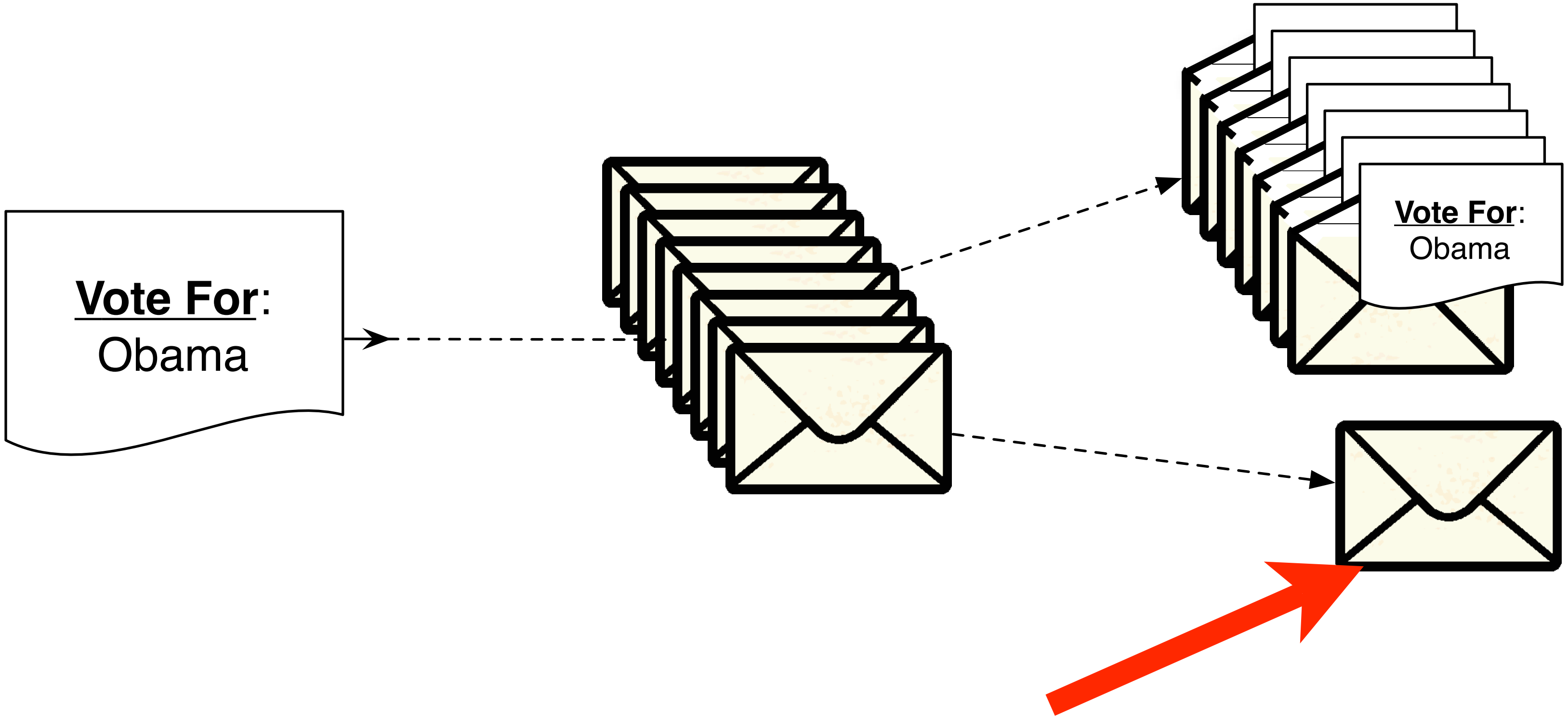
Zero-Knowledge Proof



Zero-Knowledge Proof

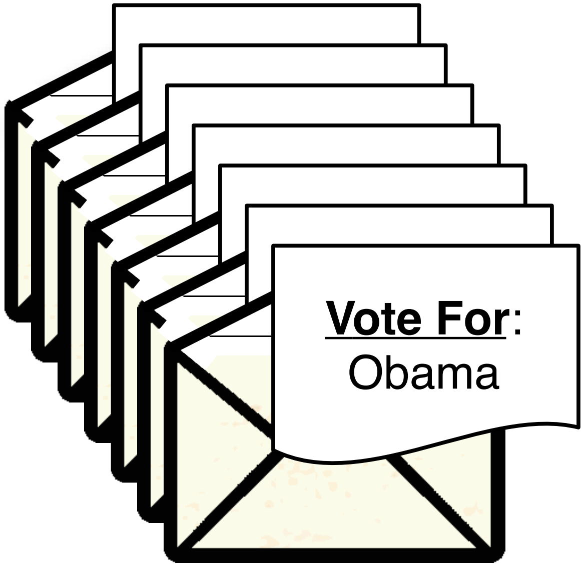


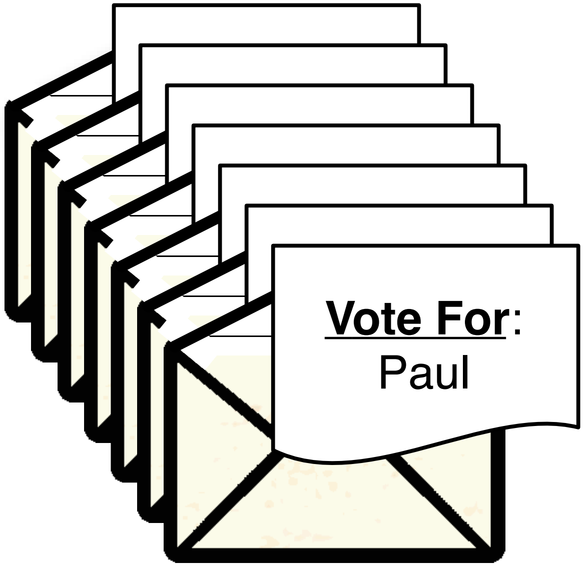
Zero-Knowledge Proof



This last envelope likely contains "Obama"

Zero-Knowledge Proof

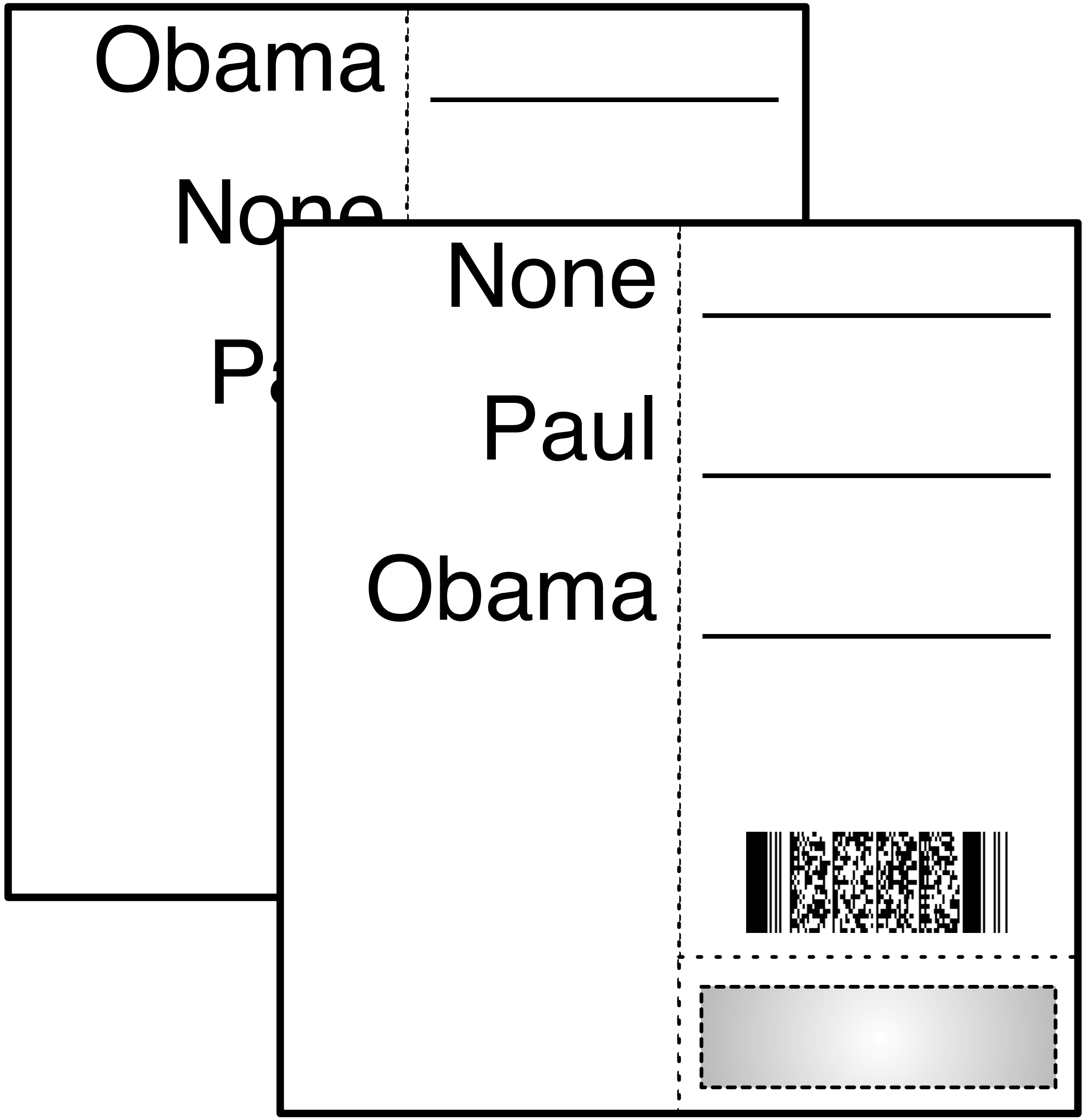




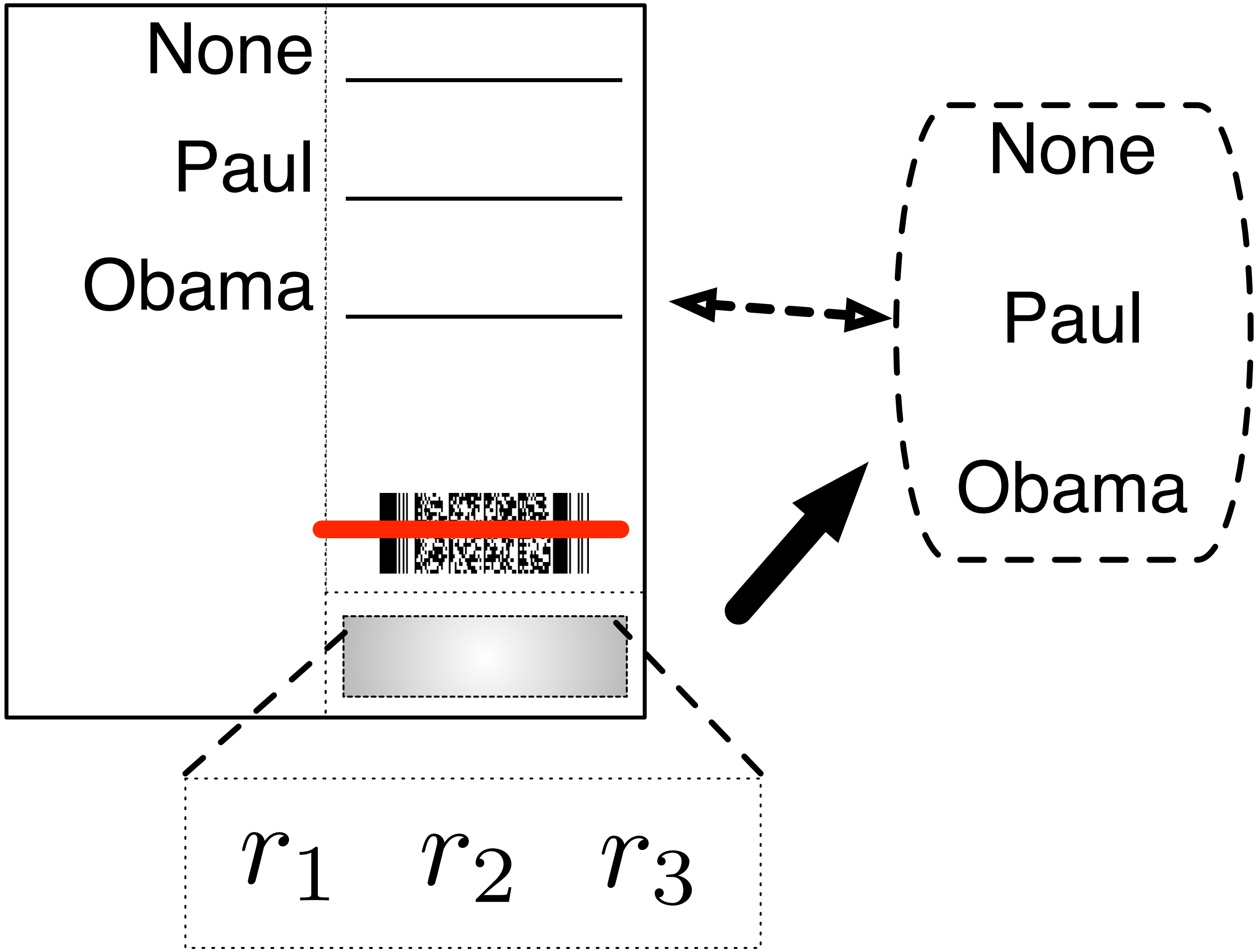
Open envelopes don't prove anything after the fact.

Scratch & Vote

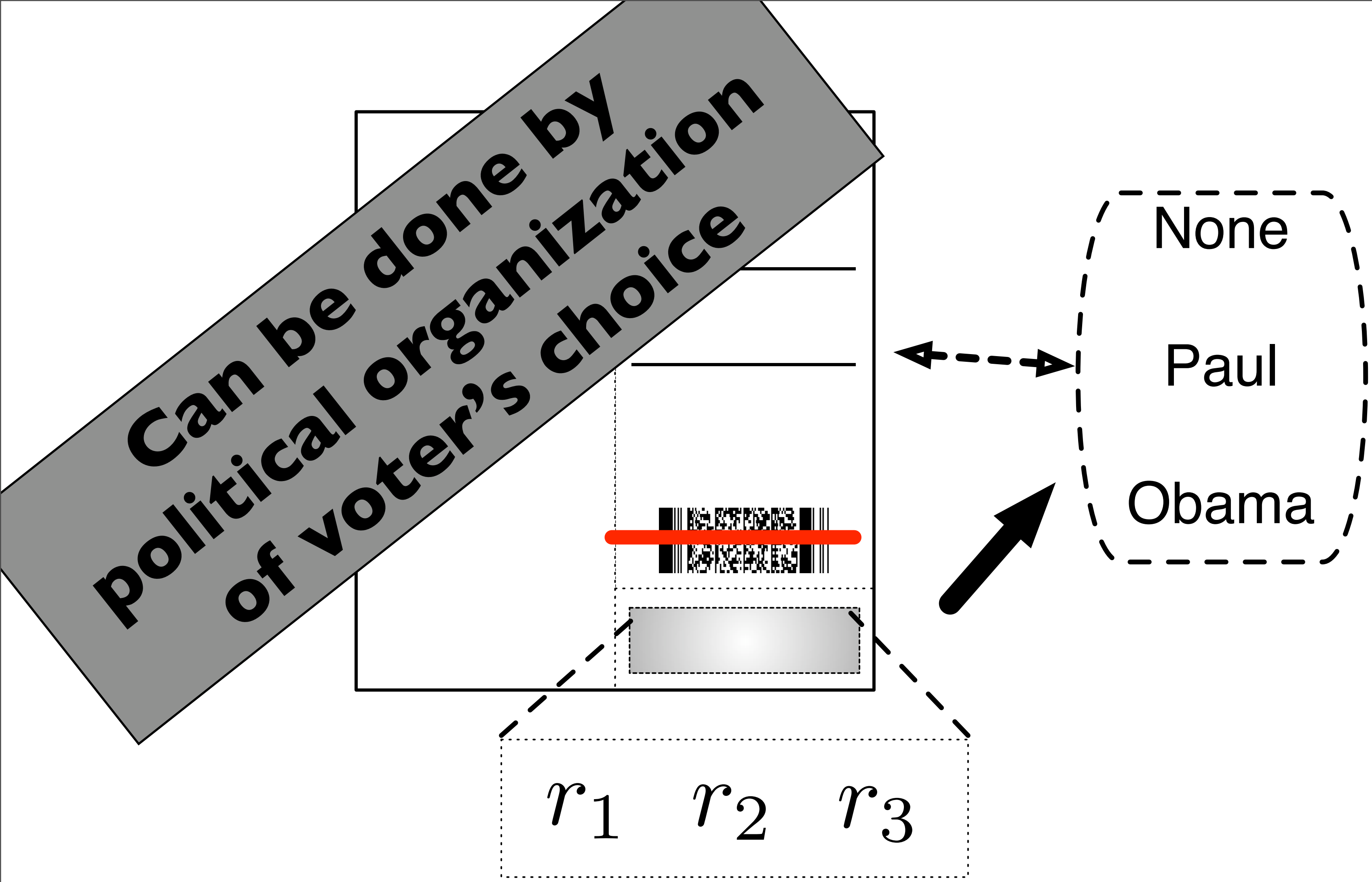
[AR2006]



1. Receive two ballots.



2. Choose one randomly for auditing by scratch-off.



Can be done by political organization of voter's choice

None

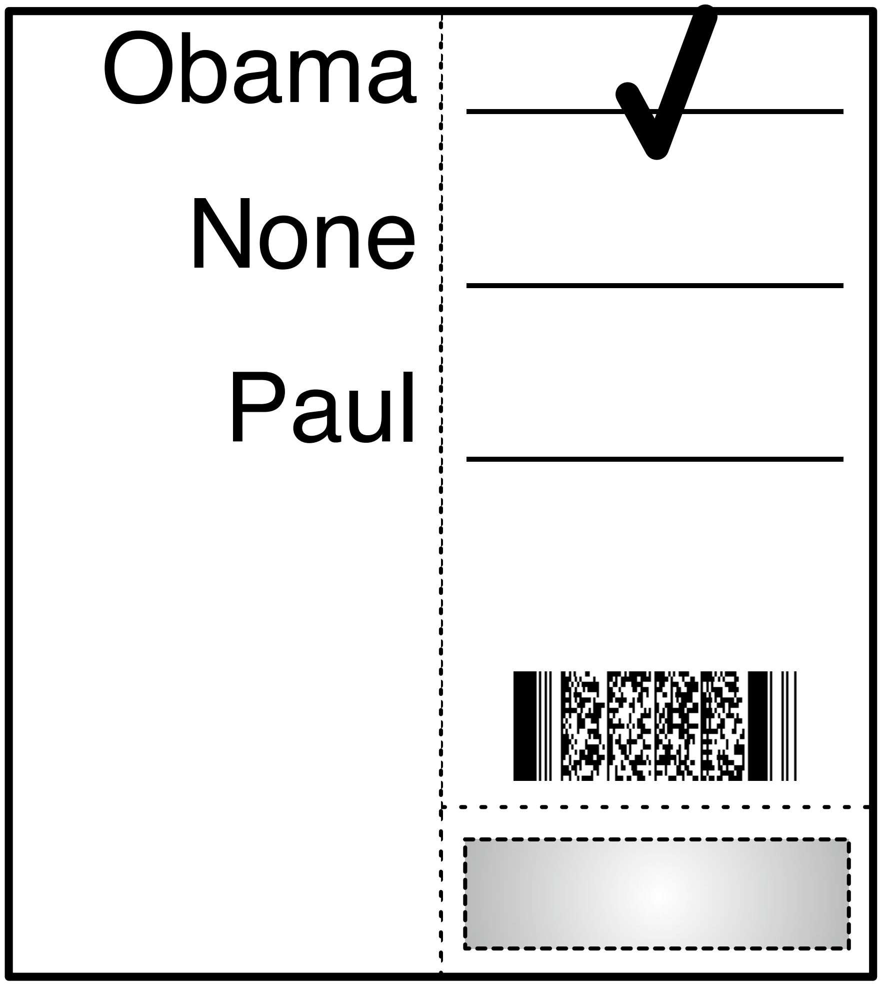
Paul

Obama

r_1 r_2 r_3

2. Choose one randomly for auditing by scratch-off.

In Private



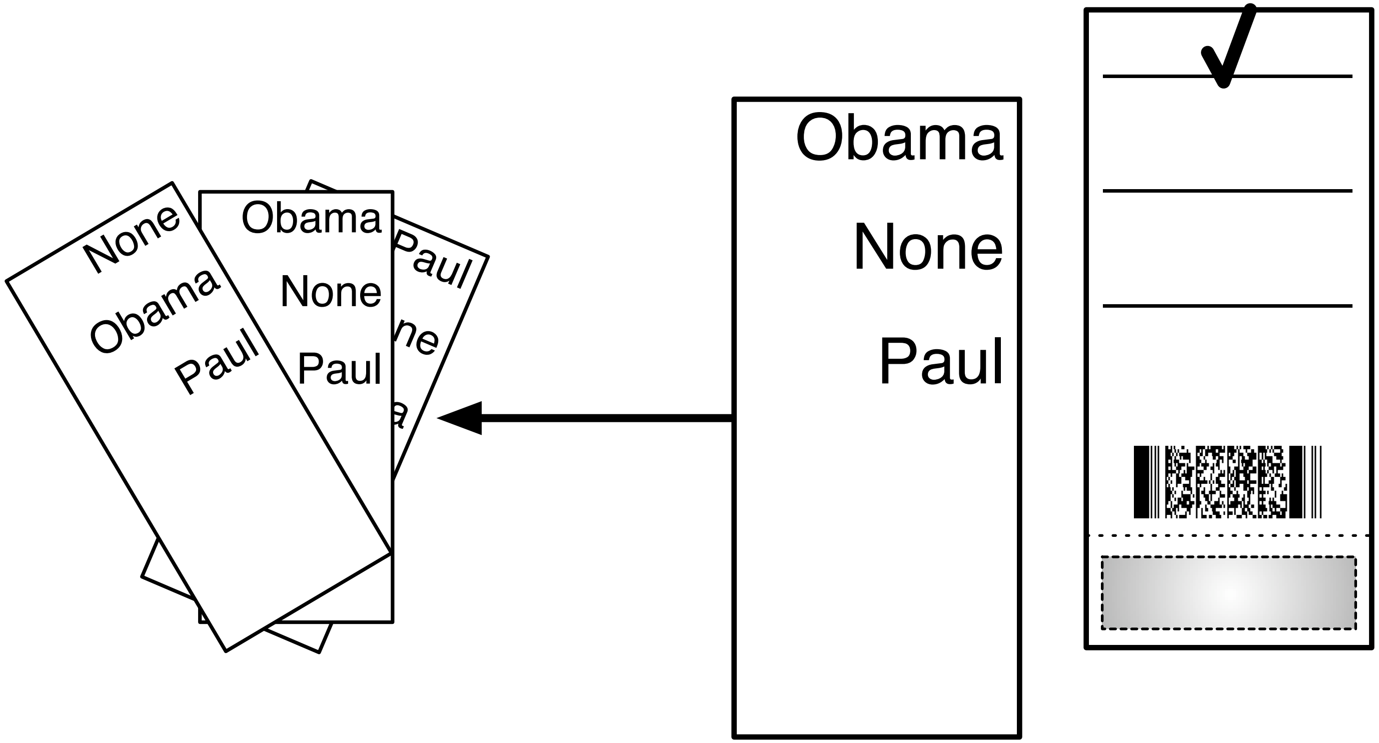
Obama ✓

None

Paul

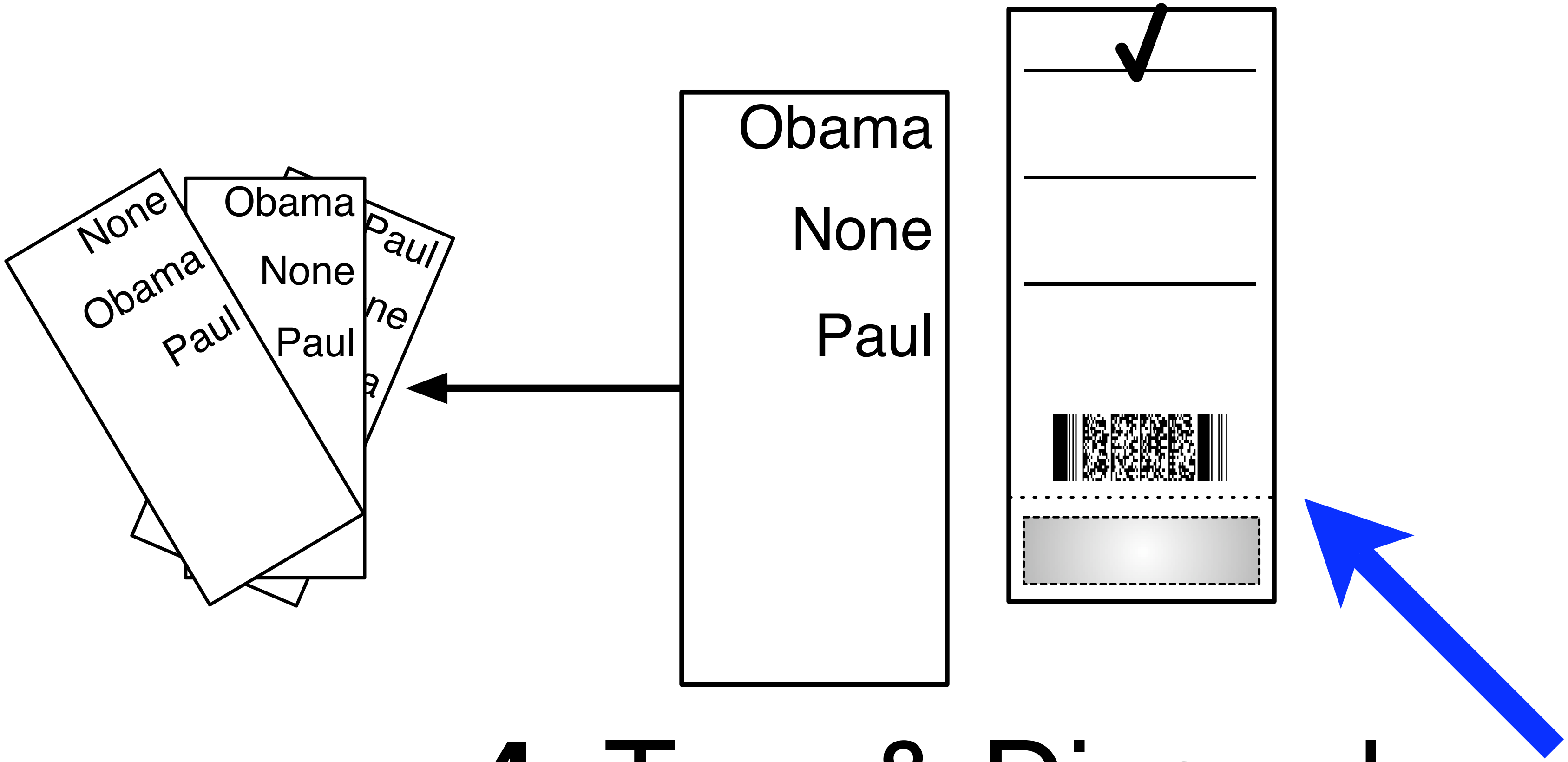
3. Vote.

In Private

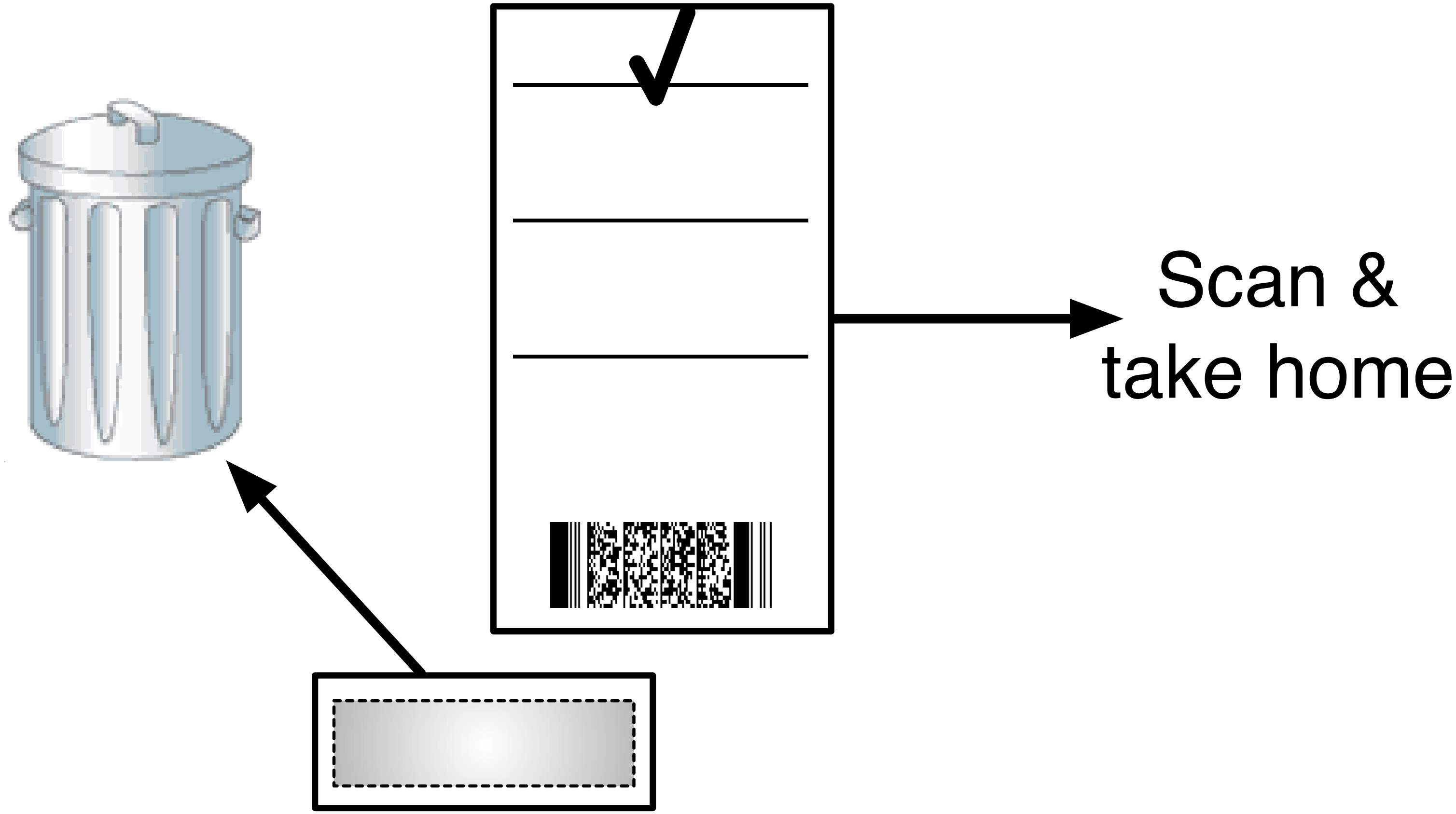


4. Tear & Discard left half of ballot.

In Private



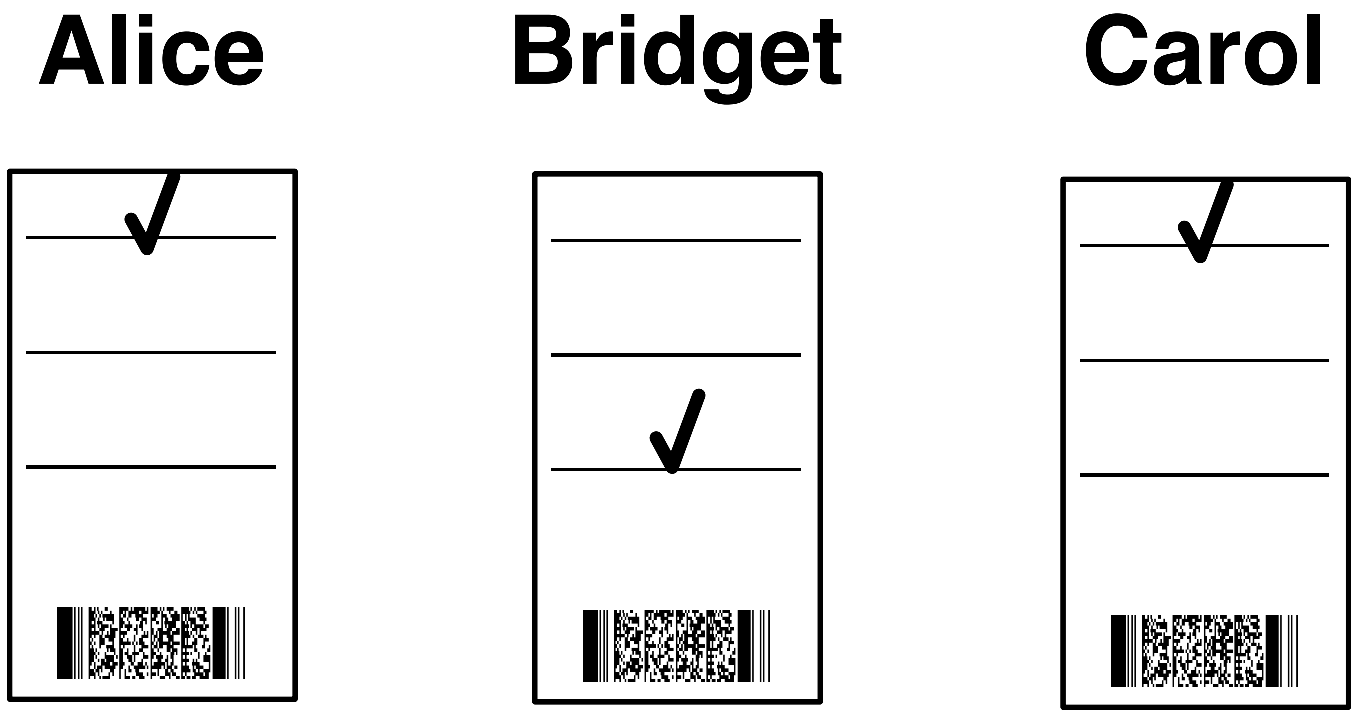
4. Tear & Discard left half of ballot.



Scan &
take home

5. Tear & Discard scratch-off.

Bulletin Board



Alice

Bridget

Carol

El Gamal

setting: $p \text{ prime}, q \text{ prime}, q|(p-1)$

private key: $x \in \mathcal{Z}_q^*$

public key: $y = g^x \ (mod\ p)$

El Gamal

setting: $p \text{ prime}, q \text{ prime}, q|(p-1)$

private key: $x \in \mathcal{Z}_q^*$

public key: $y = g^x \ (mod\ p)$

$$r \xleftarrow{R} \mathcal{Z}_q^*$$

$$\mathsf{Enc}_{pk}(m; r) = (\alpha, \beta) = (g^r, m \cdot y^r)$$

El Gamal

setting: $p \text{ prime}, q \text{ prime}, q|(p-1)$

private key: $x \in \mathcal{Z}_q^*$

public key: $y = g^x \ (mod\ p)$

$$r \xleftarrow{R} \mathcal{Z}_q^*$$

$$\text{Enc}_{pk}(m; r) = (\alpha, \beta) = (g^r, m \cdot y^r)$$

$$\text{Dec}_{sk}(c) = \frac{\beta}{\alpha^x}$$

Homomorphic Property

$$\mathsf{Enc}(m_1) \times \mathsf{Enc}(m_2) = \mathsf{Enc}(m_1 \times m_2)$$

Homomorphic Property

$$\mathsf{Enc}(m_1) \times \mathsf{Enc}(m_2) = \mathsf{Enc}(m_1 \times m_2)$$

$$c_1 = (g^{r_1}, m_1 y^{r_1})$$

$$c_2 = (g^{r_2}, m_2 y^{r_2})$$

$$c_1 \cdot c_2 = (g^{r_1+r_2}, (m_1 \cdot m_2) y^{r_1+r_2})$$

Wouldn’t it be nice if....

Wouldn’t it be nice if....

$$\mathsf{Enc}_{pk}(m_1) \cdot \mathsf{Enc}_{pk}(m_2) = \mathsf{Enc}_{pk}(m_1 + m_2)$$

Wouldn’t it be nice if....

$$\mathsf{Enc}_{pk}(m_1) \cdot \mathsf{Enc}_{pk}(m_2) = \mathsf{Enc}_{pk}(m_1 + m_2)$$

then we could simply
sum up votes homomorphically!

Exponential El Gamal

$$\mathsf{Enc}_{pk}(m, r) = (g^r, g^m y^r)$$

First: r’th residuosity [Benaloh85]
Also: Paillier Cryptosystem [P99]

Exponential El Gamal

$$\mathsf{Enc}_{pk}(m, r) = (g^r, g^m y^r)$$

First: r’th residuosity [Benaloh85]
Also: Paillier Cryptosystem [P99]

Exponential El Gamal

$$\mathsf{Enc}_{pk}(m,r) = (g^r, g^m y^r)$$

$$\mathsf{Dec}_{sk}(c) = g^m$$

First: r'th residuosity [Benaloh85]
Also: Paillier Cryptosystem [P99]

Exponential El Gamal

$$\mathsf{Enc}_{pk}(m, r) = (g^r, g^m y^r)$$

$$\mathsf{Dec}_{sk}(c) = g^m$$

Take the discrete log base g.

First: r'th residuosity [Benaloh85]
Also: Paillier Cryptosystem [P99]

Homomorphic Tallying

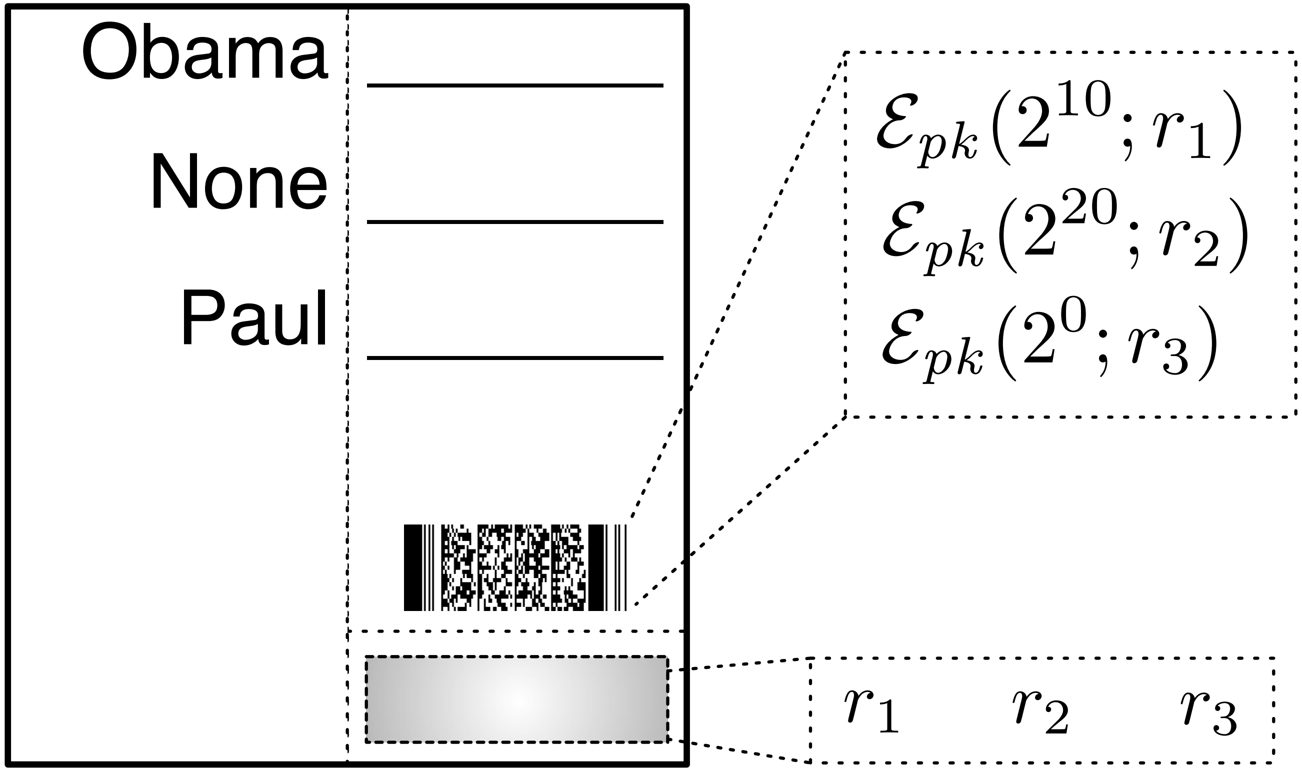
0001	0000	0000	Vote for None
0000	0001	0000	Vote for Obama
0000	0000	0001	Vote for Paul
0003	0006	0005	→ **Sample Tally**

[B+2001, P1999]

PARAMETERS

#1 - Paul
#2 - Obama
#3 - None

M=10, Public Key = pk



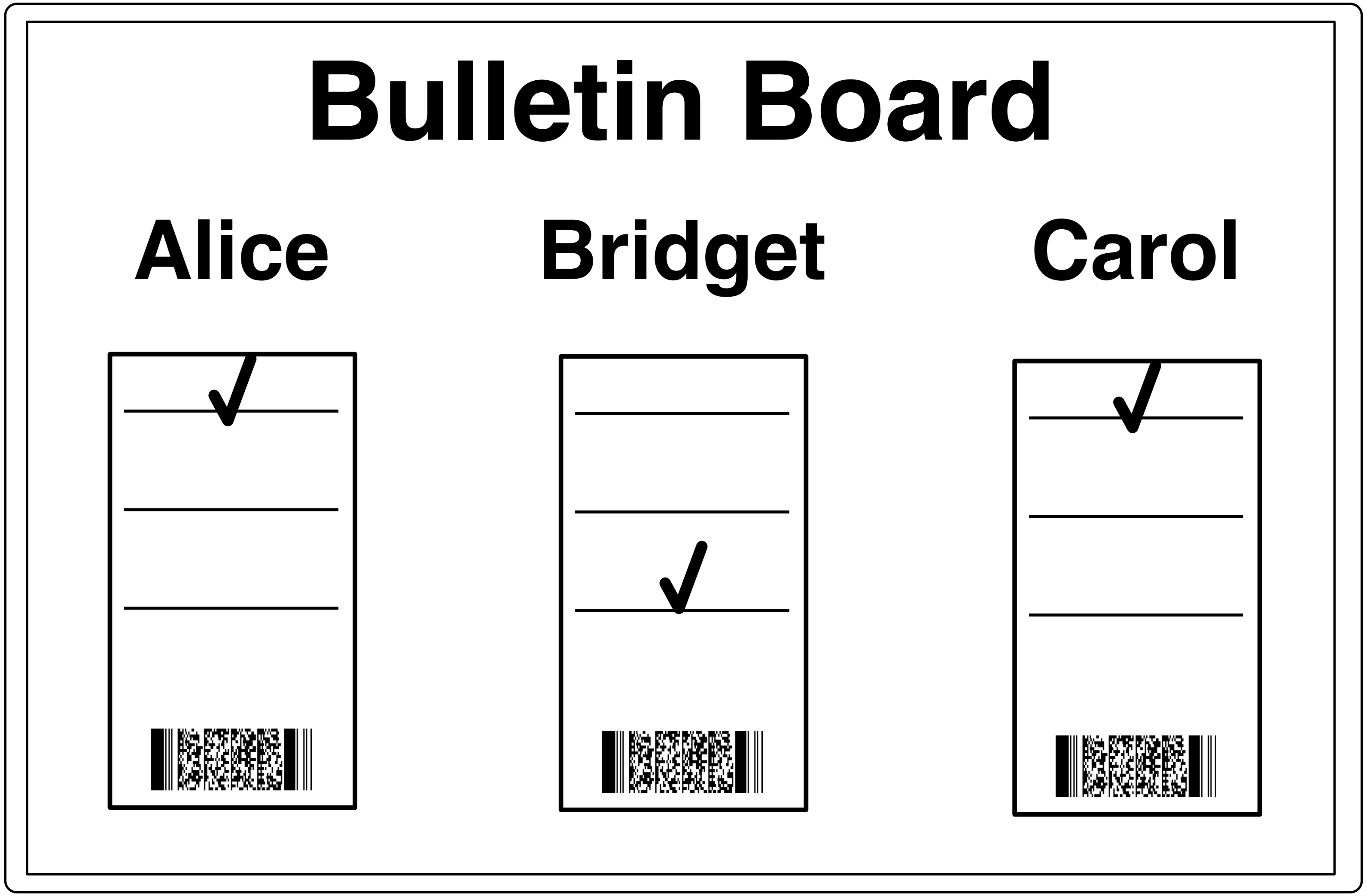
Obama

None

Paul

$\mathcal{E}_{pk}(2^{10}; r_1)$
$\mathcal{E}_{pk}(2^{20}; r_2)$
$\mathcal{E}_{pk}(2^{0}; r_3)$

r_1 r_2 r_3



Bulletin Board

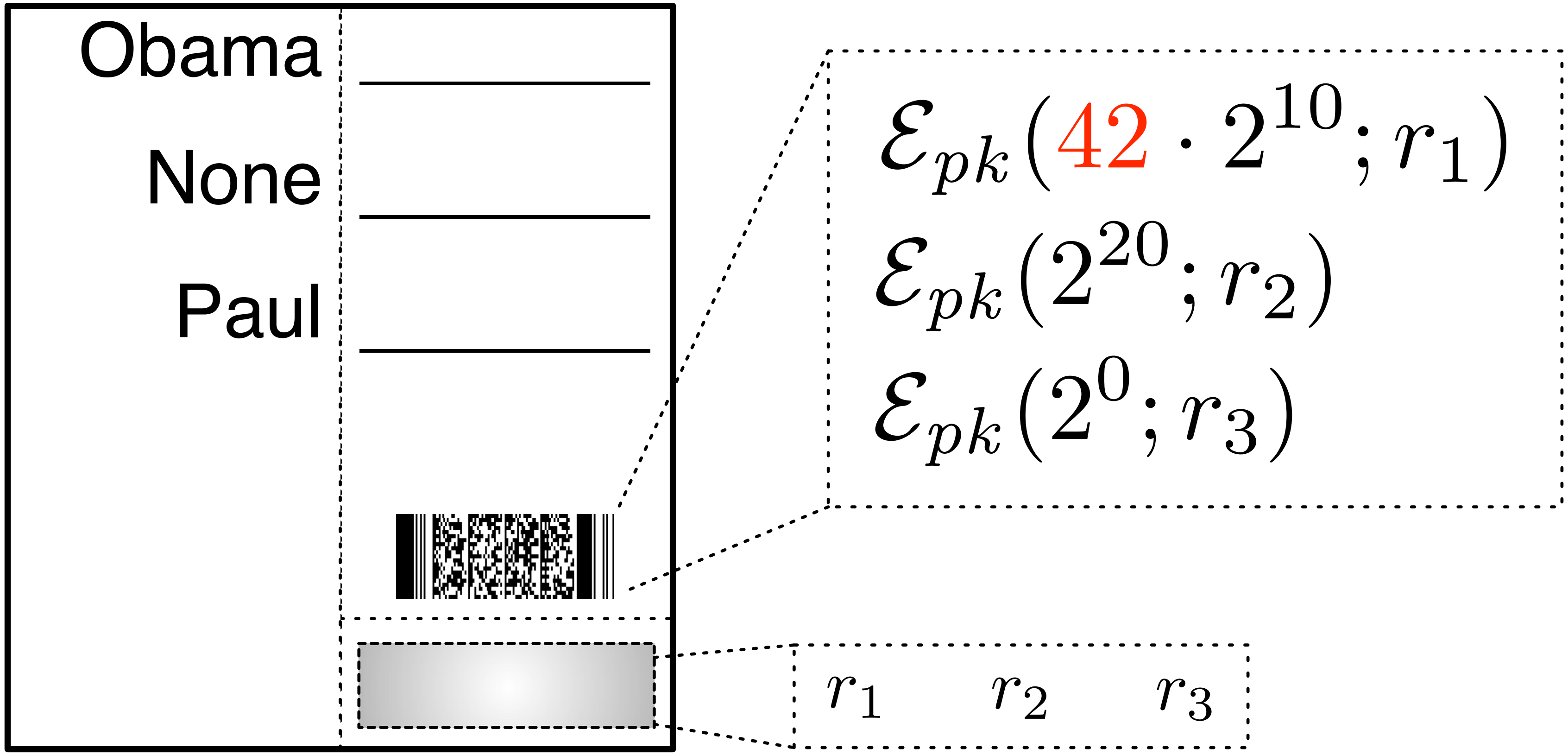
Alice

Bridget

Carol

Be Careful...

Be Careful...



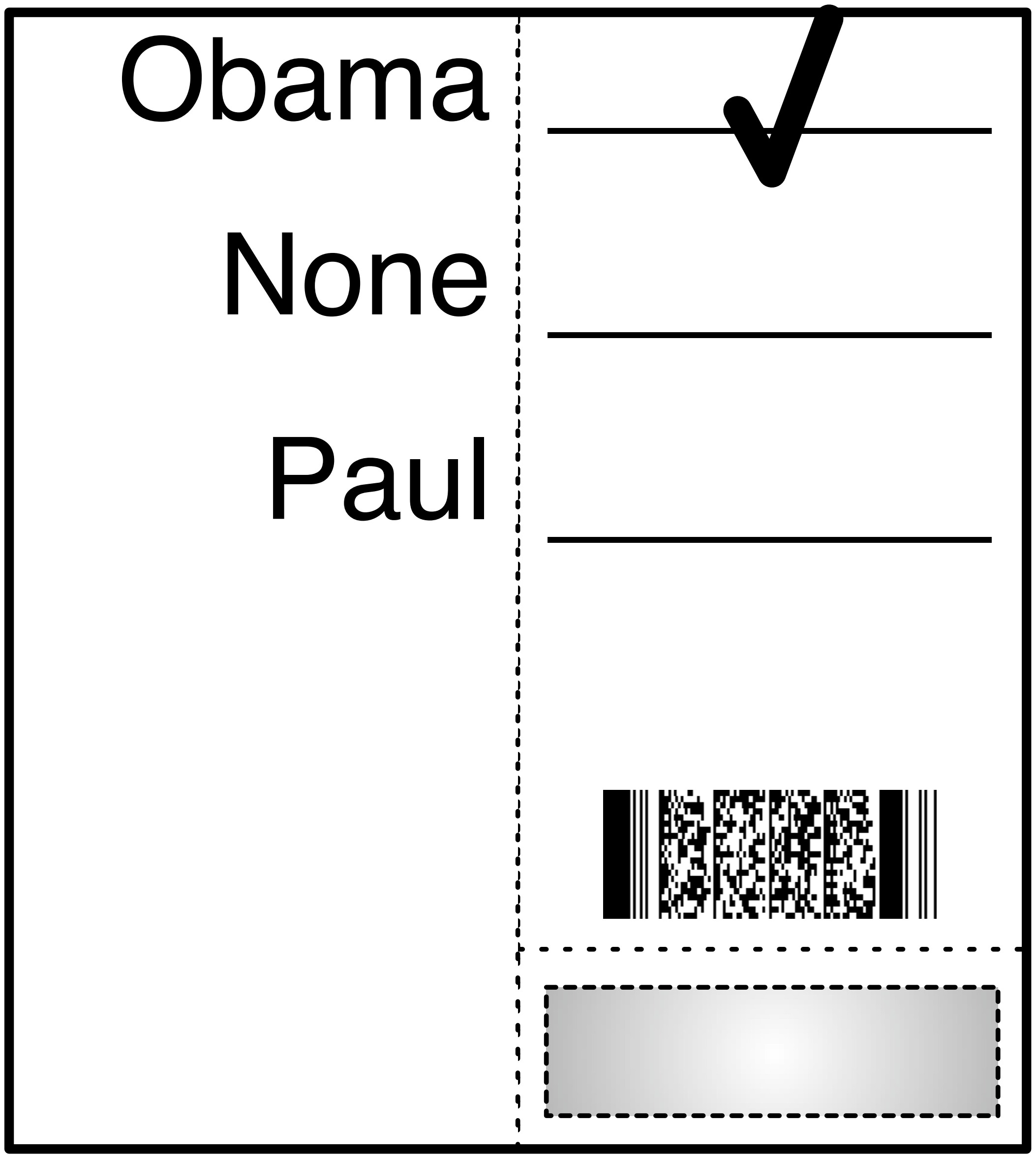
$$\mathcal{E}_{pk}(\color{red}{42} \cdot 2^{10}; r_1)$$

$$\mathcal{E}_{pk}(2^{20}; r_2)$$

$$\mathcal{E}_{pk}(2^{0}; r_3)$$

$r_1 \quad r_2 \quad r_3$

Summary of S & V



Obama ✓

None

Paul

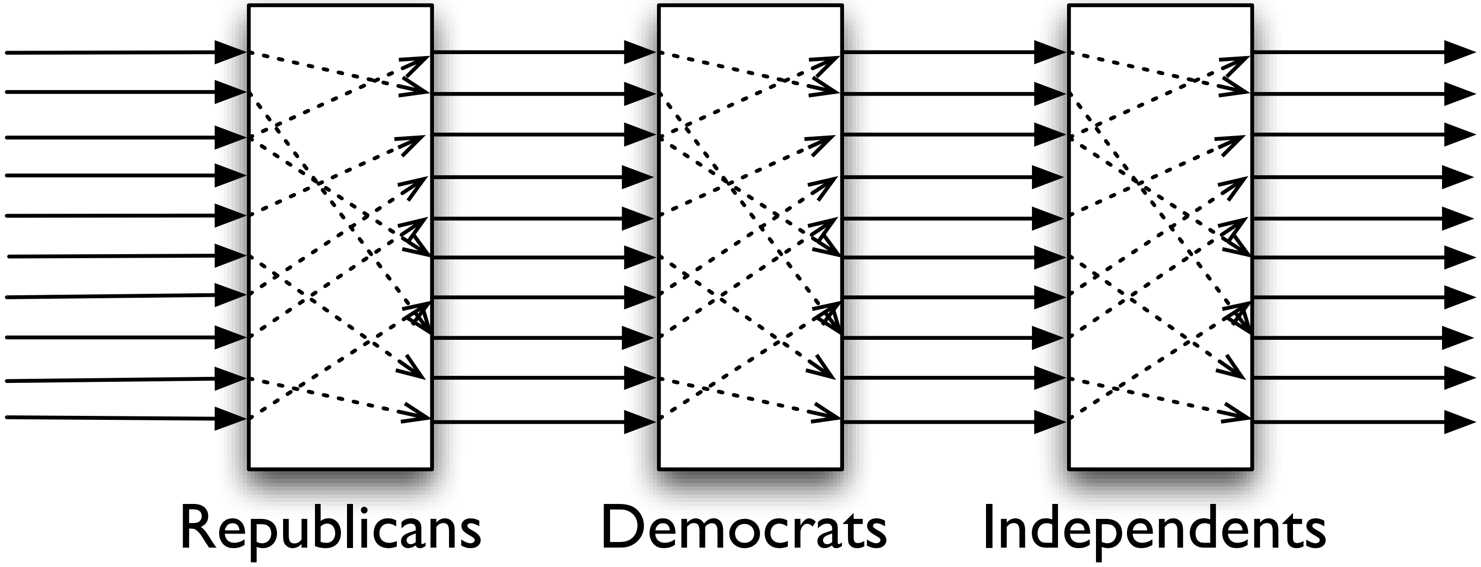
Scratch & Vote is ***one*** system.

There are many others.

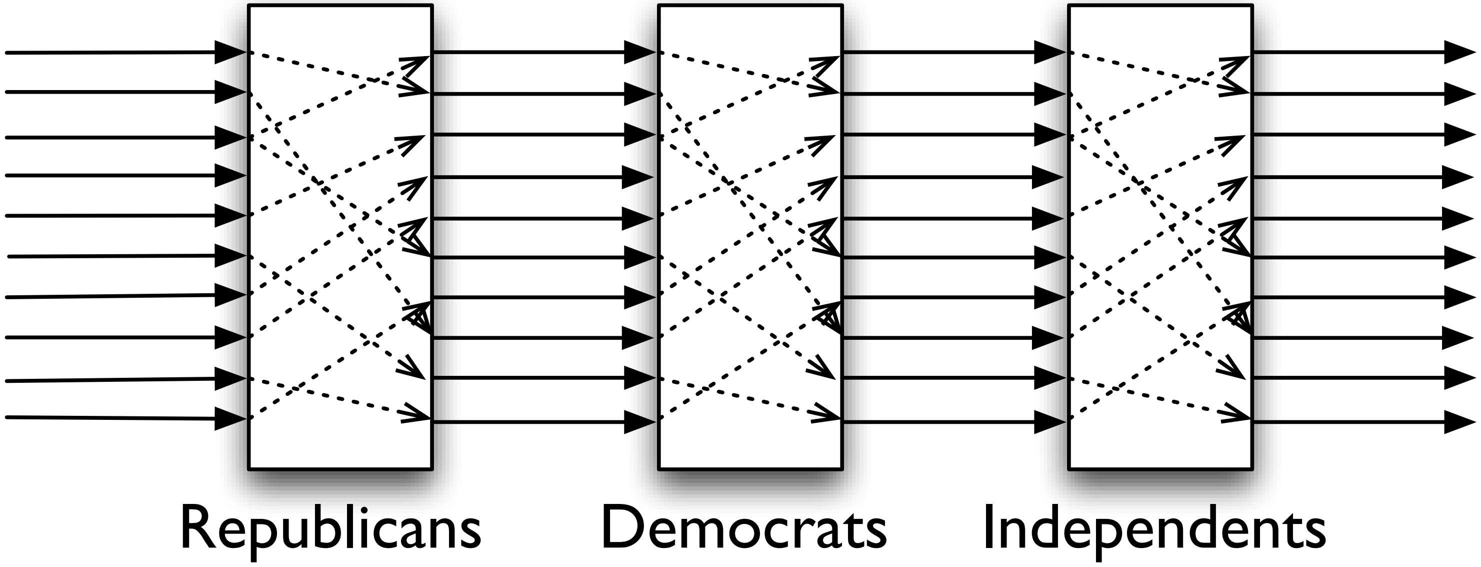
What about write-ins?

Must preserve individual ballots.

Mixnets

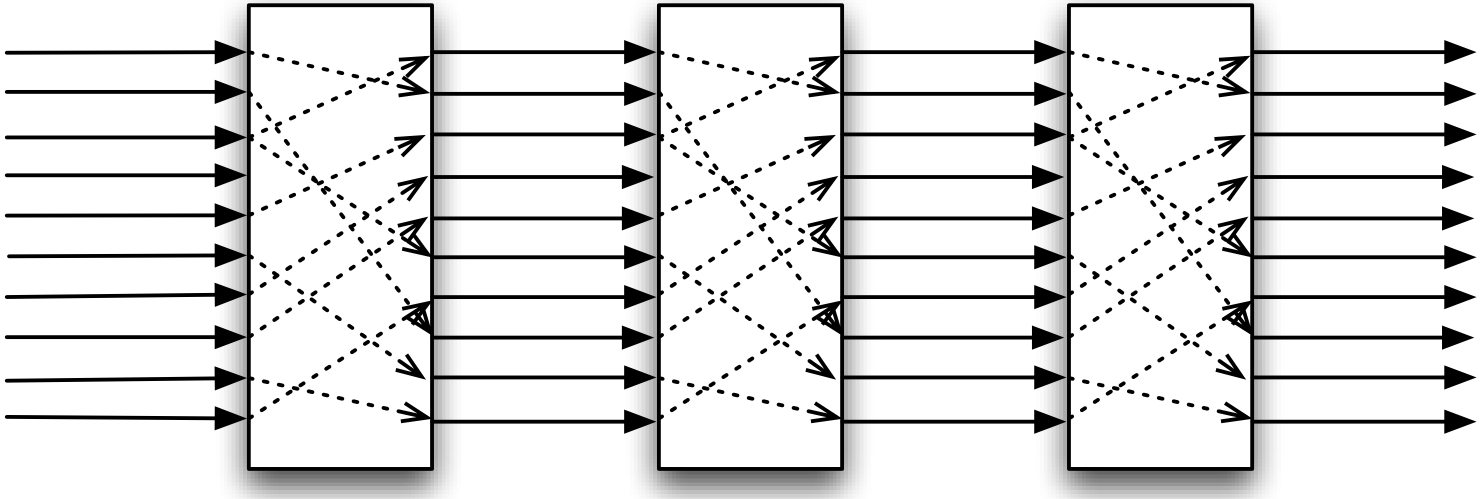


Mixnets



Mix servers operated by mutually suspicious organizations.

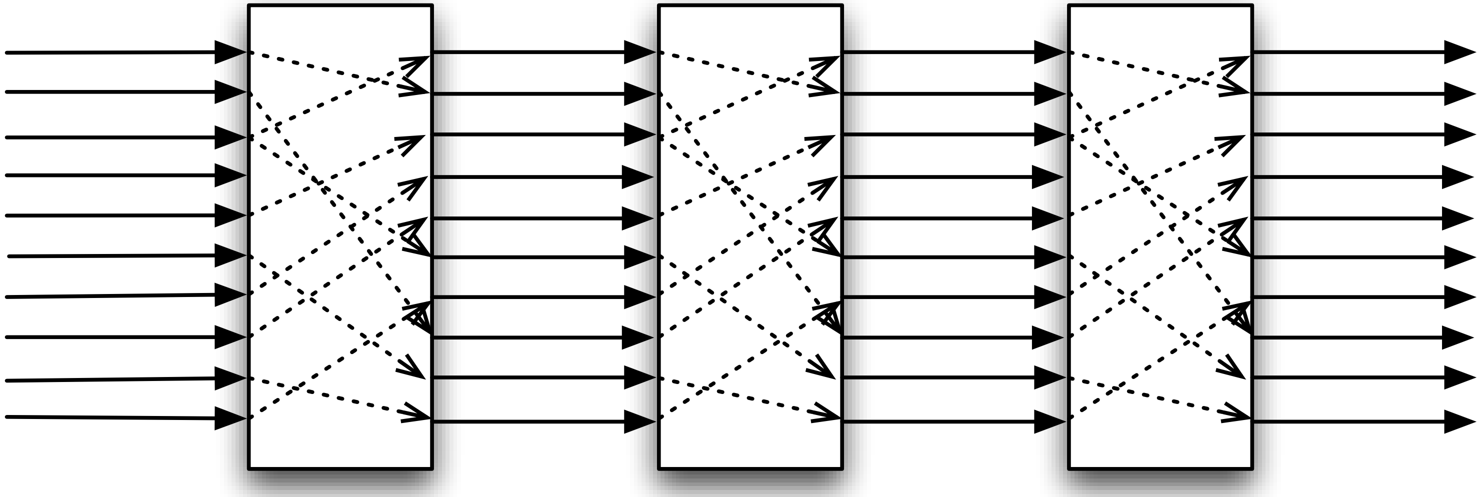
Chaumian Mixnet (Onions)



$$c_j = \mathsf{Enc}_{pk_1}(\mathsf{Enc}_{pk_2}(\mathsf{Enc}_{pk_3}(m_j)))$$

[Chaum81]

Chaumian Mixnet (Onions)

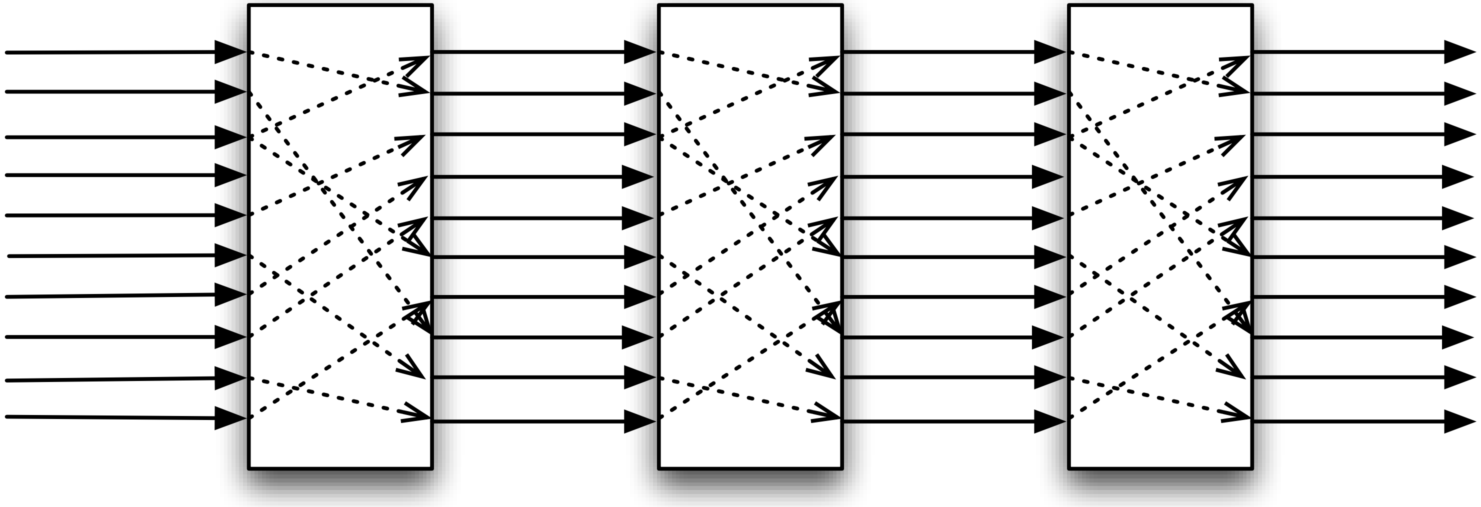


$$c_j = \mathsf{Enc}_{pk_1}(\mathsf{Enc}_{pk_2}(\mathsf{Enc}_{pk_3}(m_j)))$$

Each mix server “unwraps”
a layer of this encryption onion.

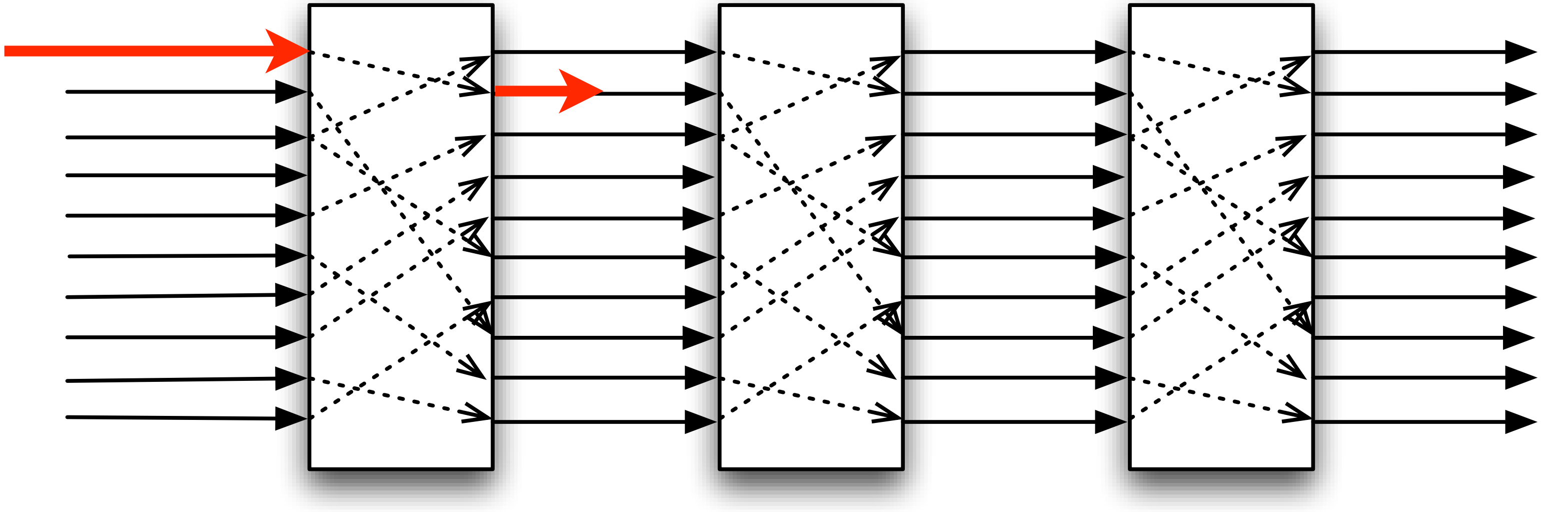
[Chaum81]

Verifying a Mixnet



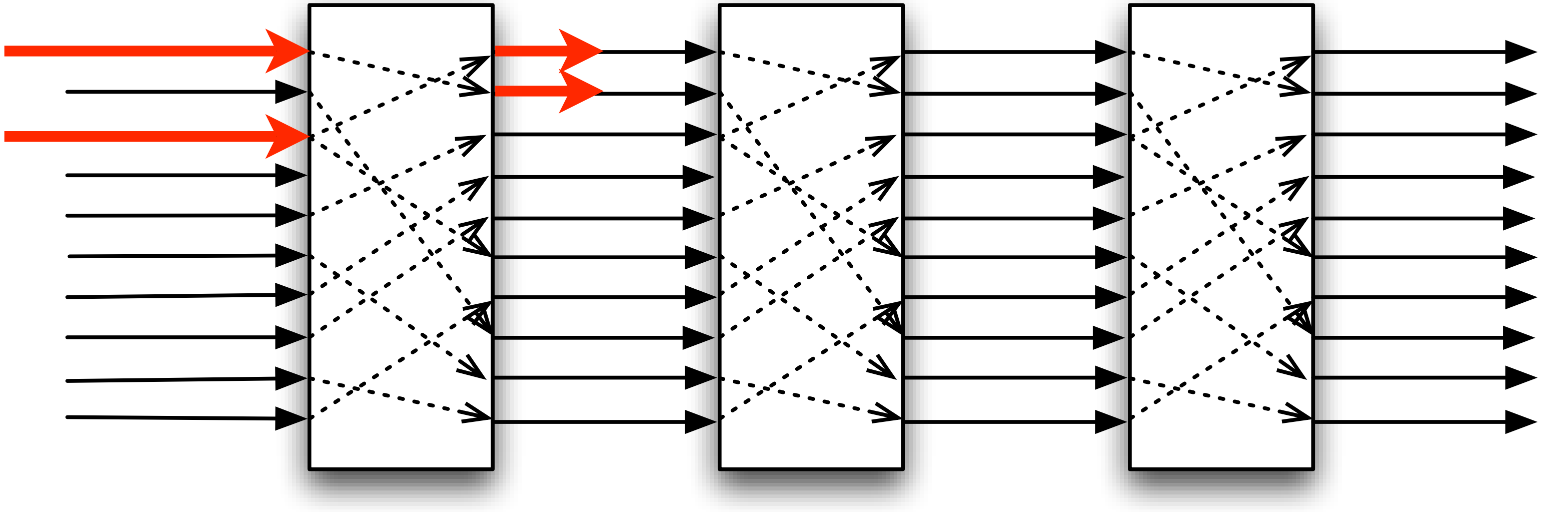
[JJR2002]

Verifying a Mixnet



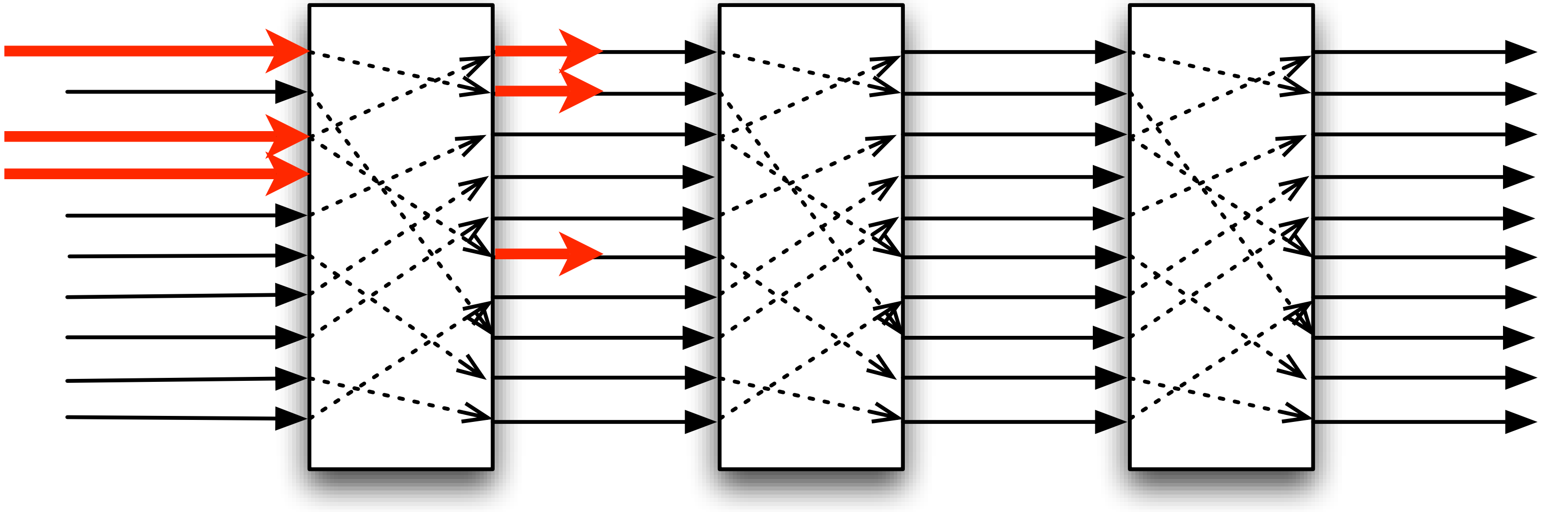
[JJR2002]

Verifying a Mixnet



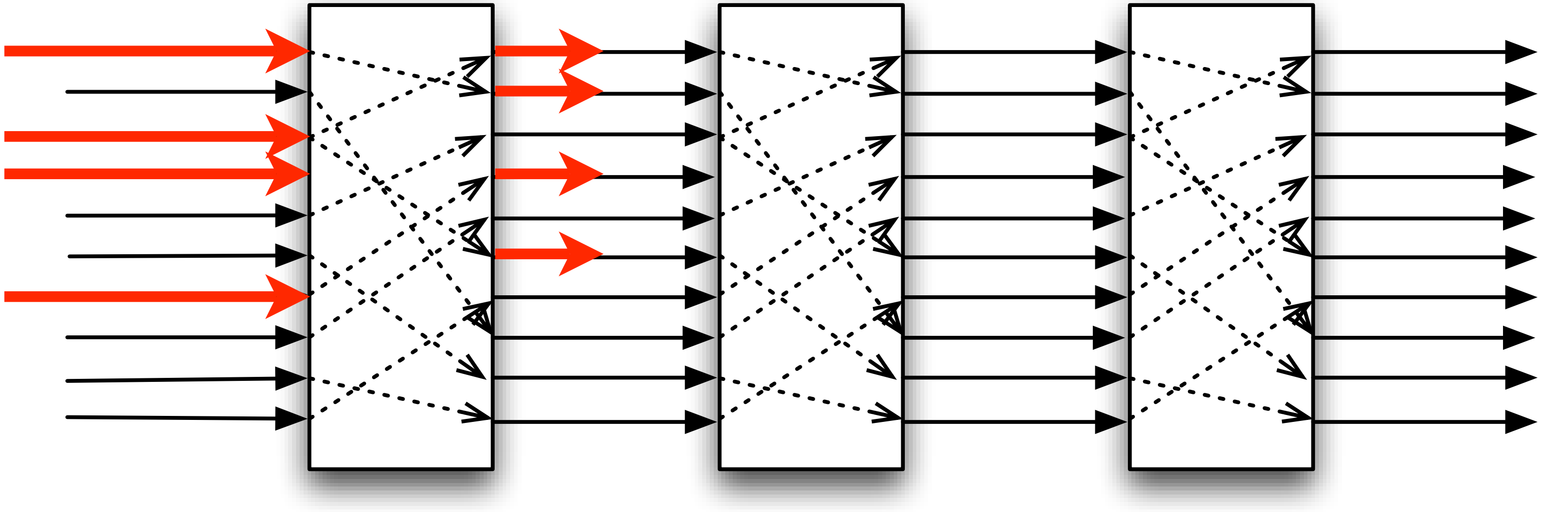
[JJR2002]

Verifying a Mixnet



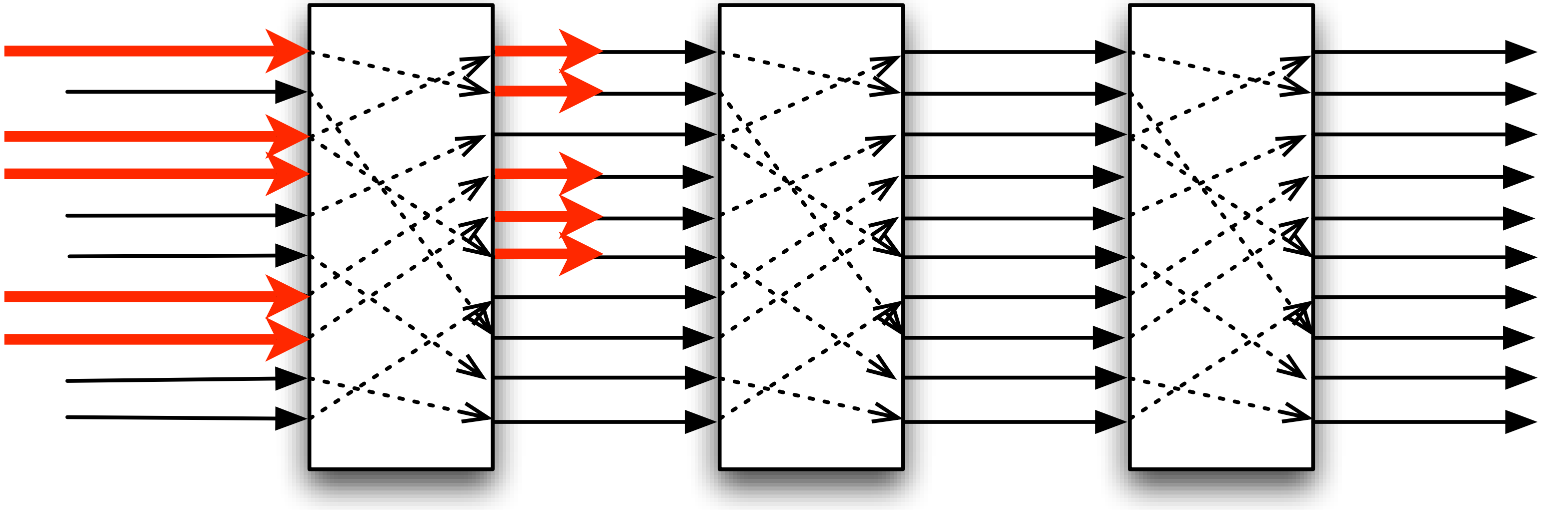
[JJR2002]

Verifying a Mixnet



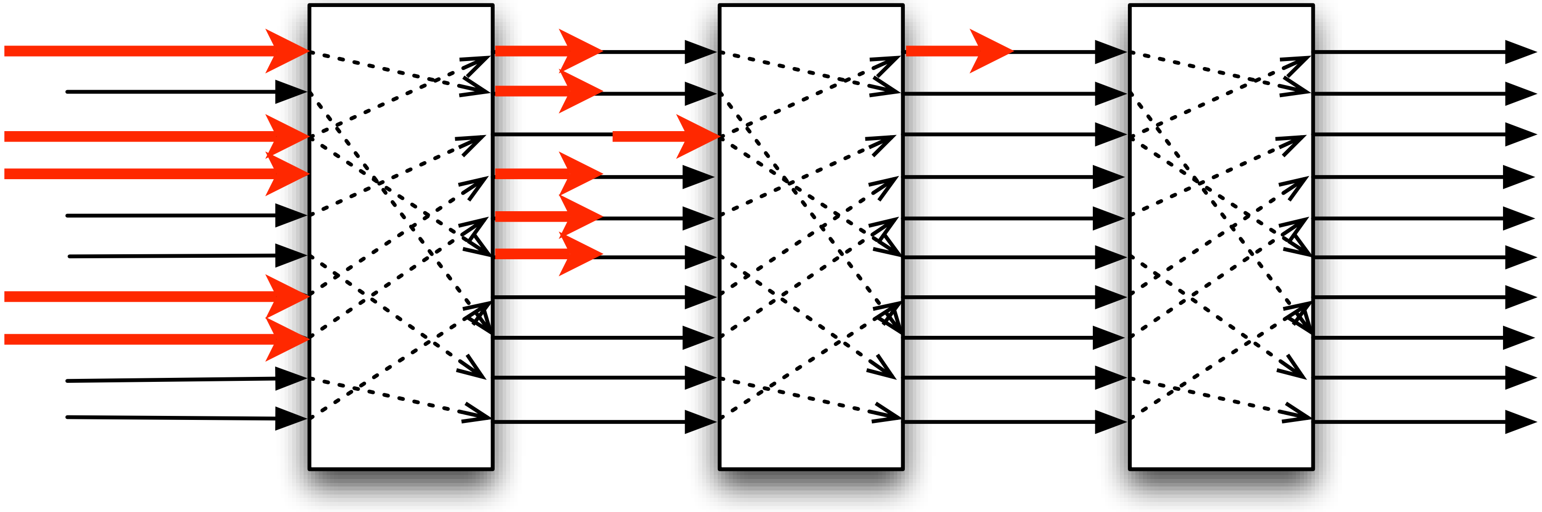
[JJR2002]

Verifying a Mixnet



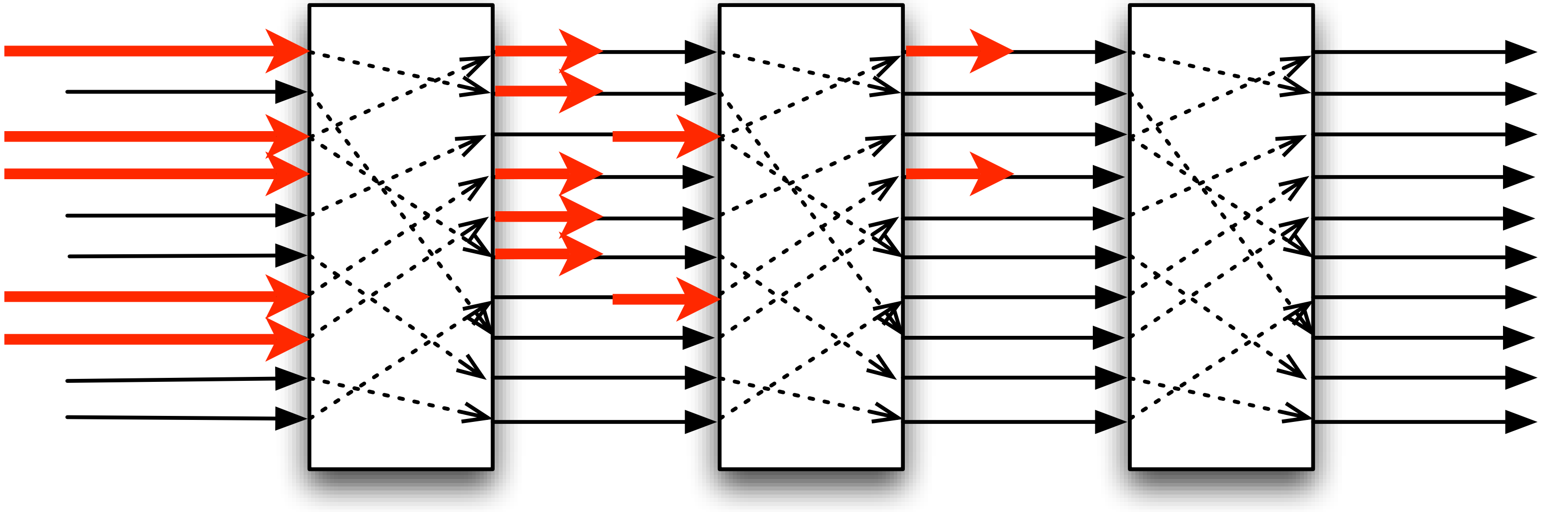
[JJR2002]

Verifying a Mixnet



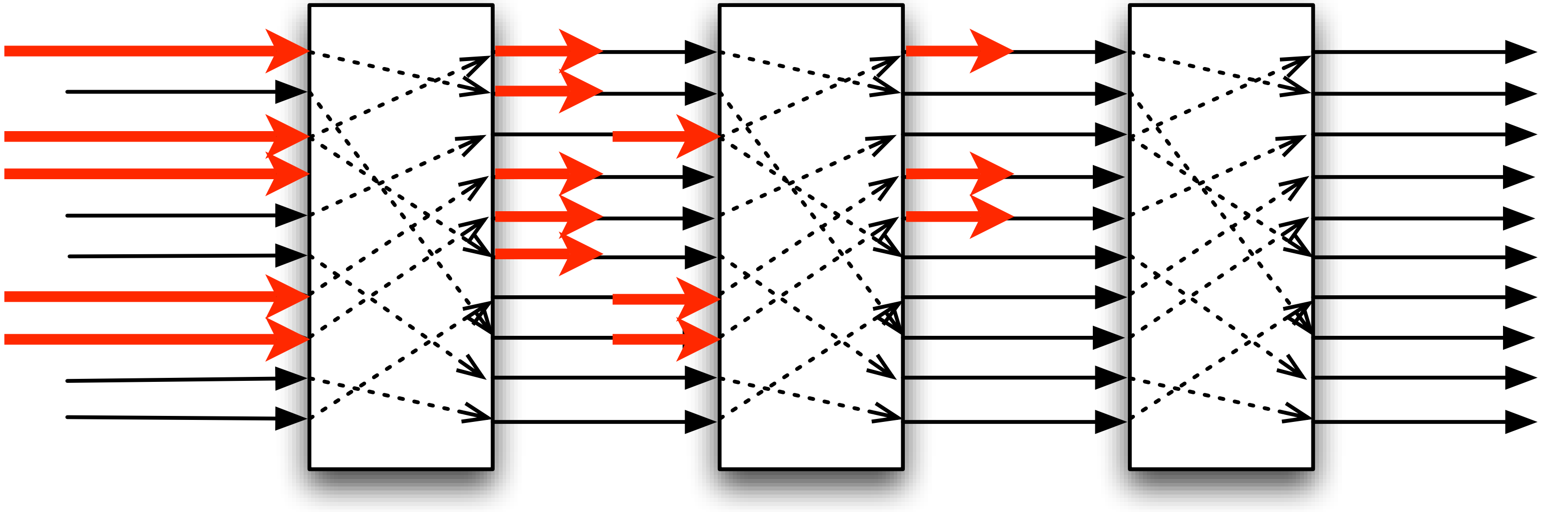
[JJR2002]

Verifying a Mixnet



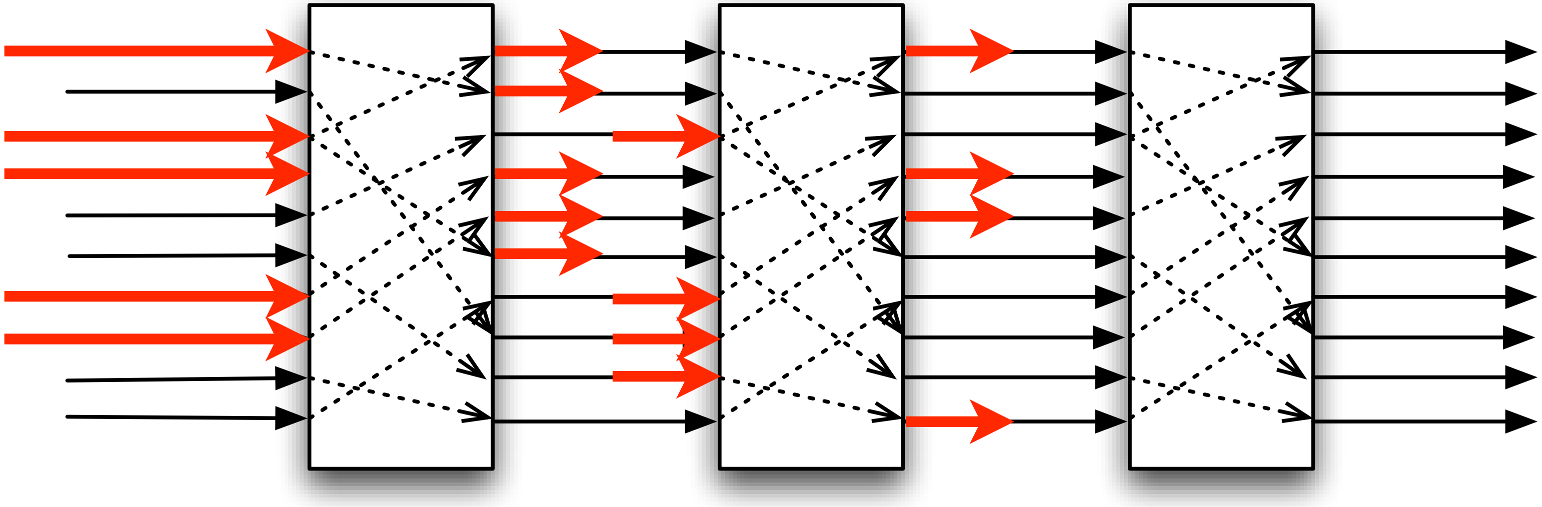
[JJR2002]

Verifying a Mixnet



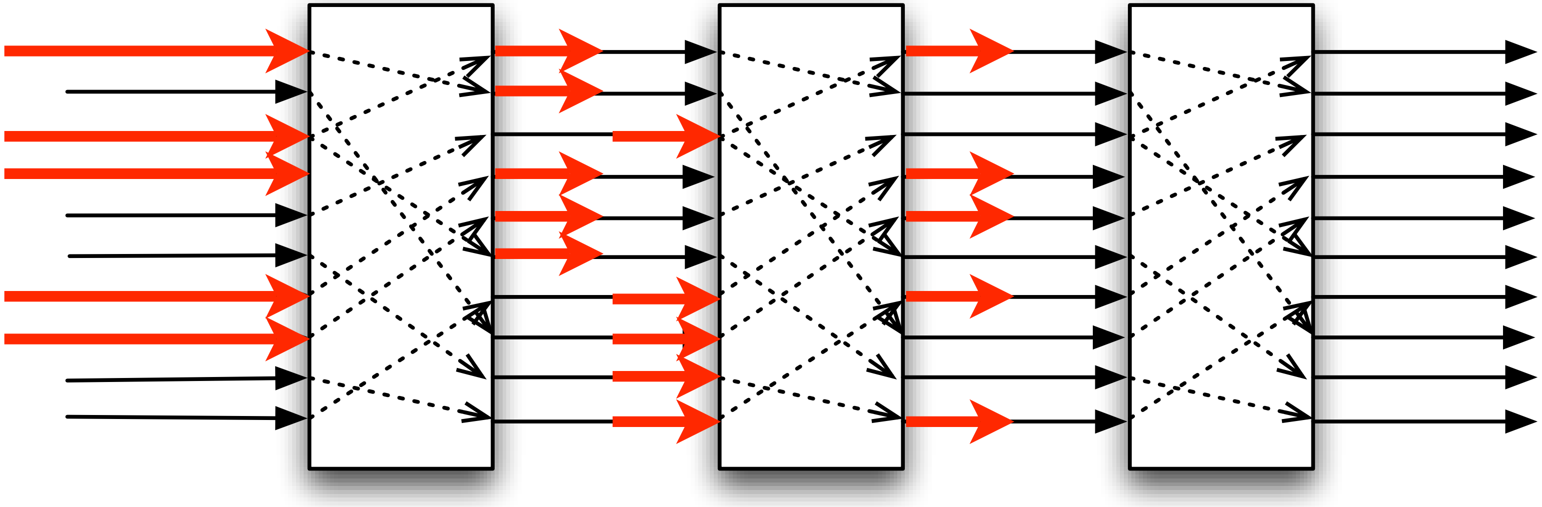
[JJR2002]

Verifying a Mixnet



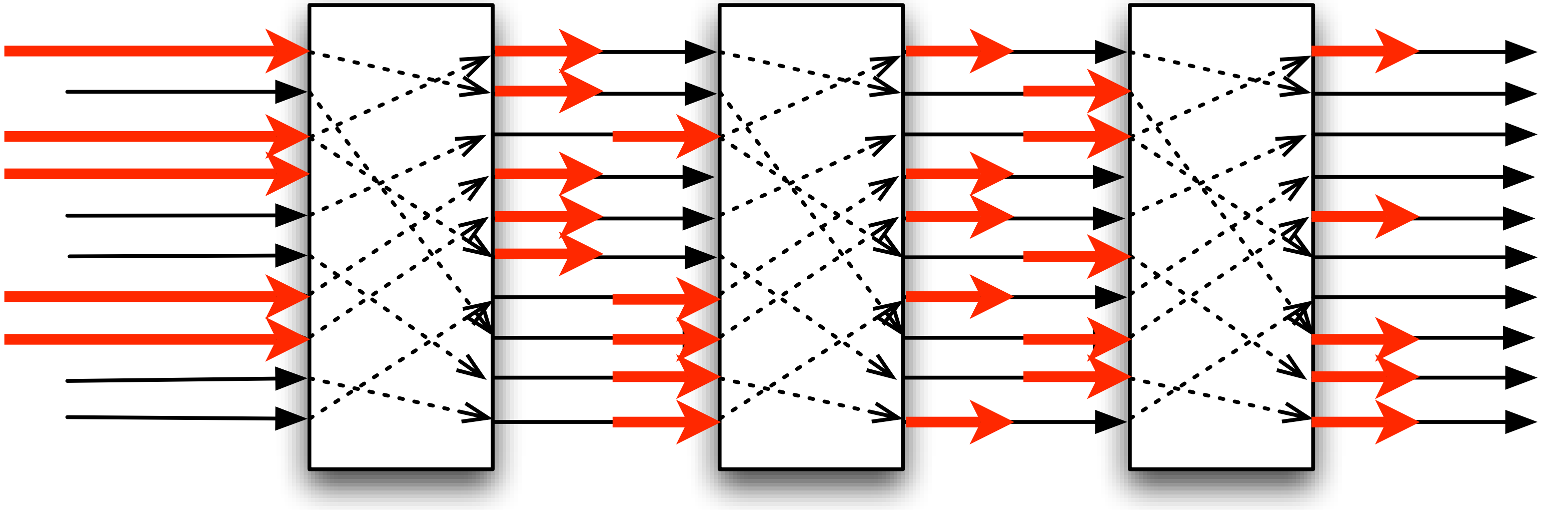
[JJR2002]

Verifying a Mixnet



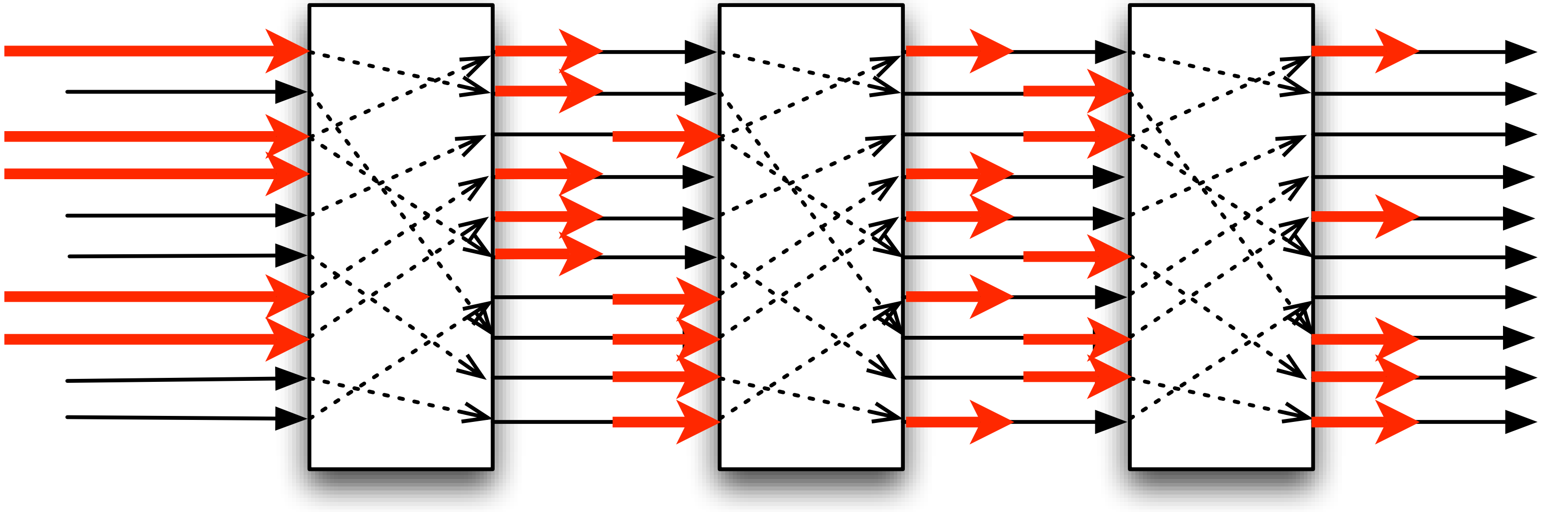
[JJR2002]

Verifying a Mixnet



[JJR2002]

Verifying a Mixnet



Tricks to ensure
no complete path is revealed.

[JJR2002]

El Gamal Reencryption

El Gamal Reencryption

$sk = x \ mod \ q \qquad pk = y = g^x \ mod \ p$

El Gamal Reencryption

$sk = x \; mod \; q \qquad\qquad pk = y = g^x \; mod \; p$

$\text{Enc}_{pk}(m; r) = (\alpha, \beta) = (g^r, m \cdot y^r)$

$\text{Dec}_{sk}(c) = \frac{\beta}{\alpha^x}$

El Gamal Reencryption

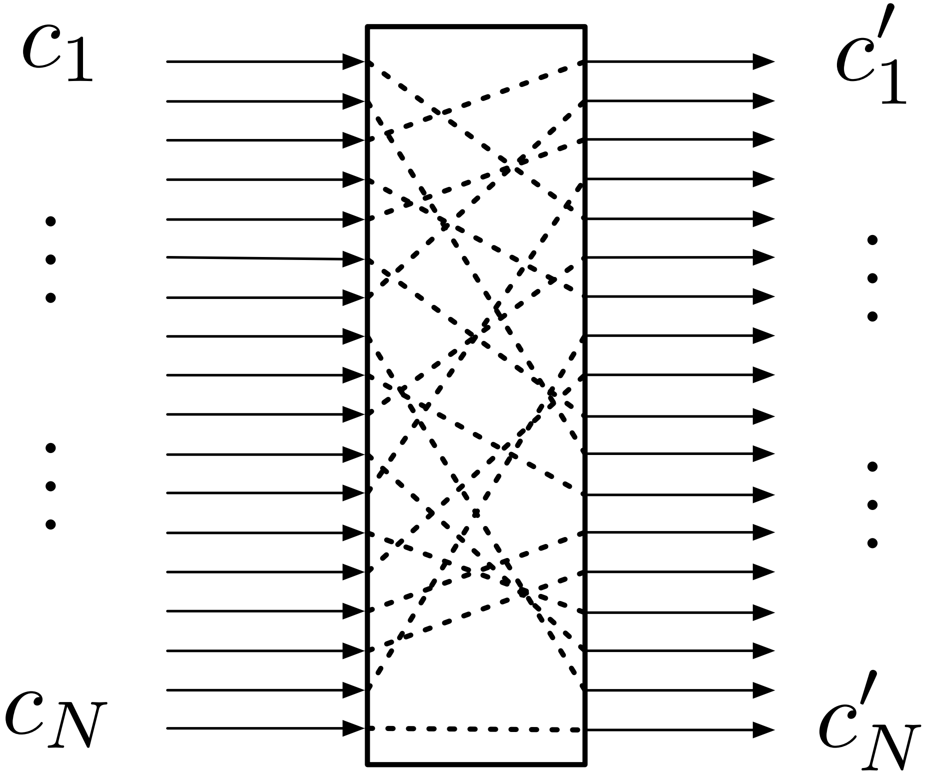
$sk = x \ mod \ q \qquad\qquad pk = y = g^x \ mod \ p$

$$\mathsf{Enc}_{pk}(m;r) = (\alpha, \beta) = (g^r, m \cdot y^r)$$

$$\mathsf{Dec}_{sk}(c) = \frac{\beta}{\alpha^x}$$

$$\begin{aligned}\mathsf{Reenc}_{pk}(c;r') &= c \cdot \mathsf{Enc}_{pk}(1, r') \\ &= (g^{r+r'}, m \cdot y^{r+r'})\end{aligned}$$

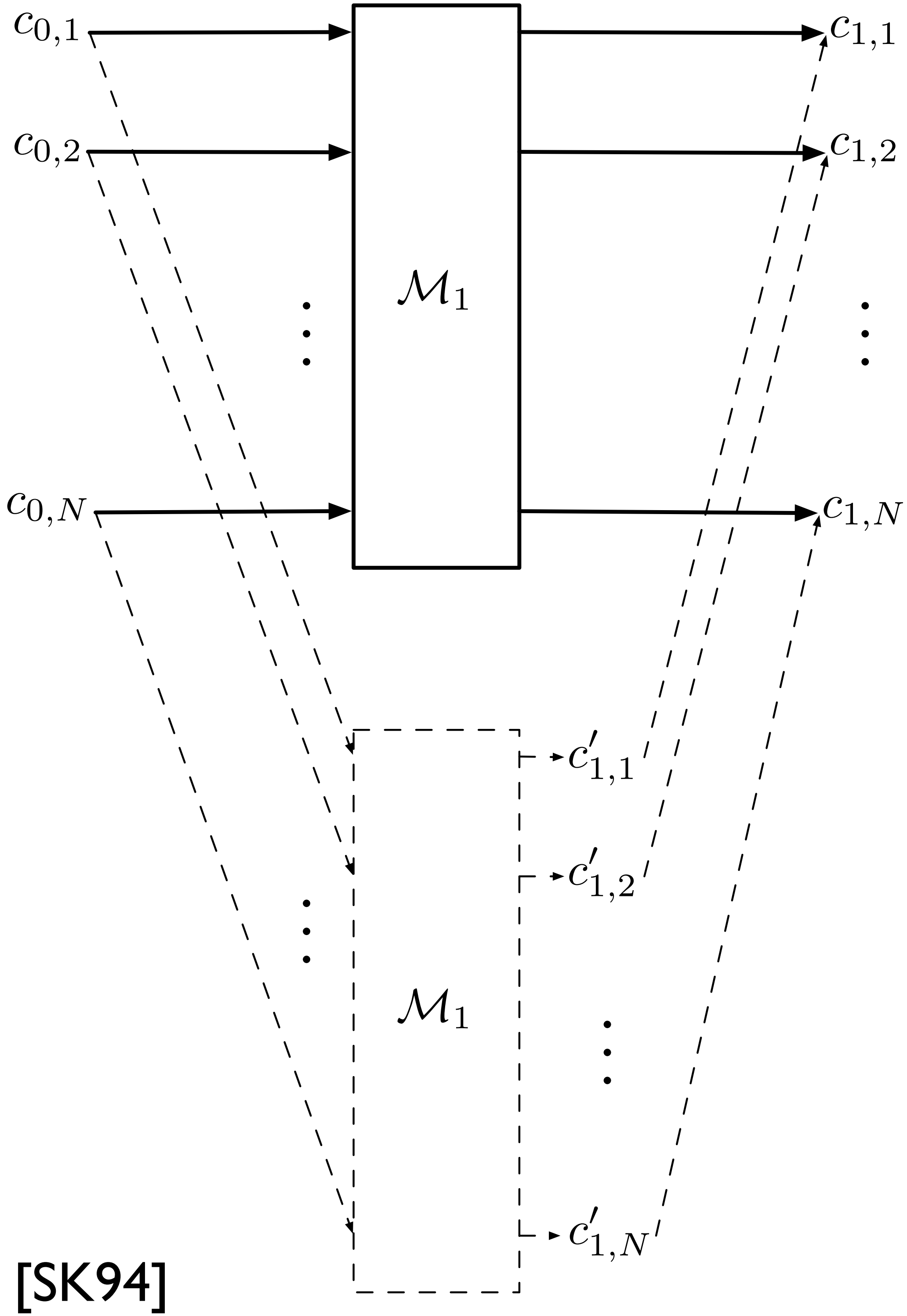
Re-encryption Mixnet



$$c'_{\pi(j)} = \text{Reenc}(c_j; r_j)$$

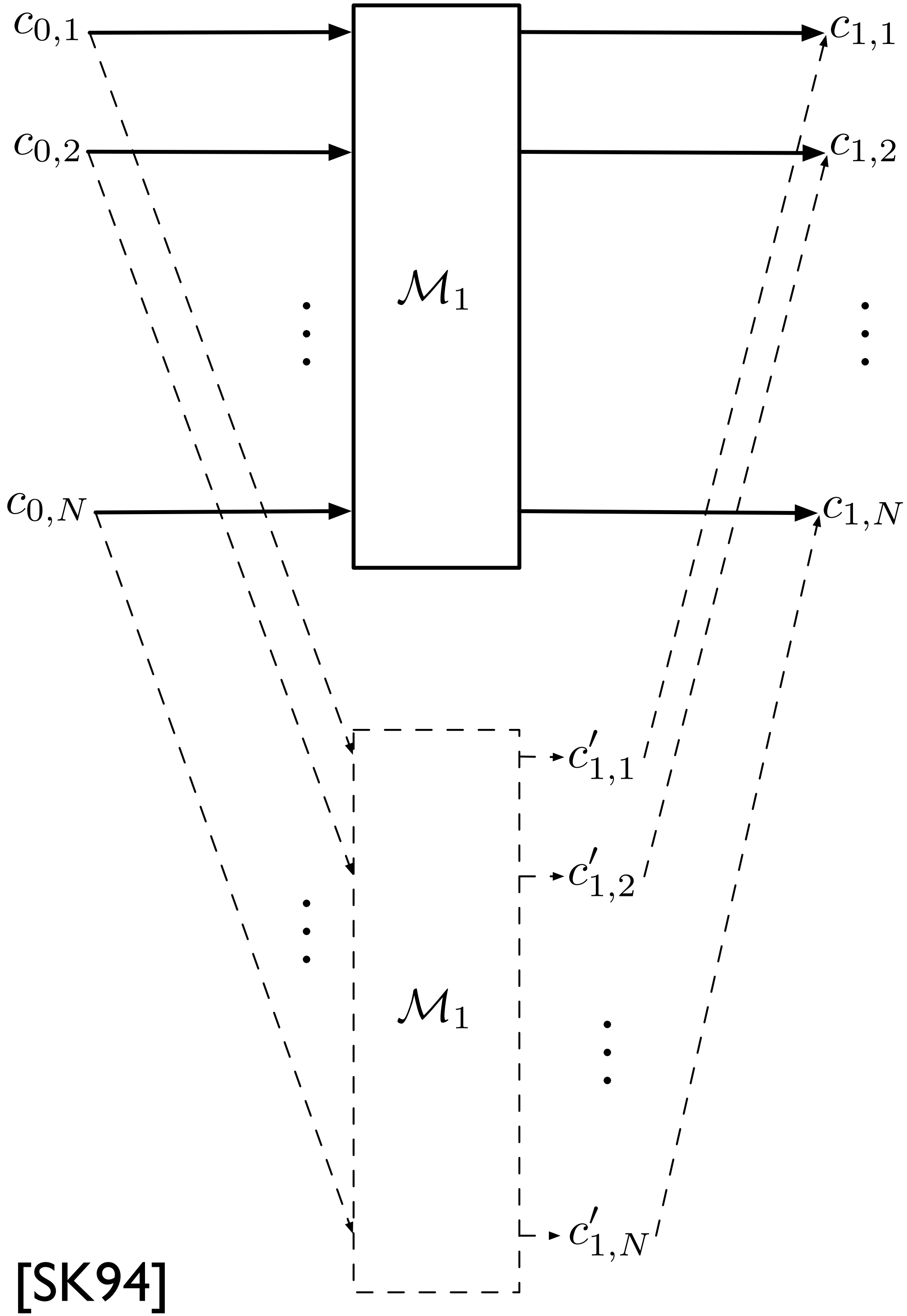
[PIK93]

Proof of Mixnet



[SK94]

Proof of Mixnet



Intermediate mix. Coin flip determines: reveal first or second.

[SK94]

Decryption

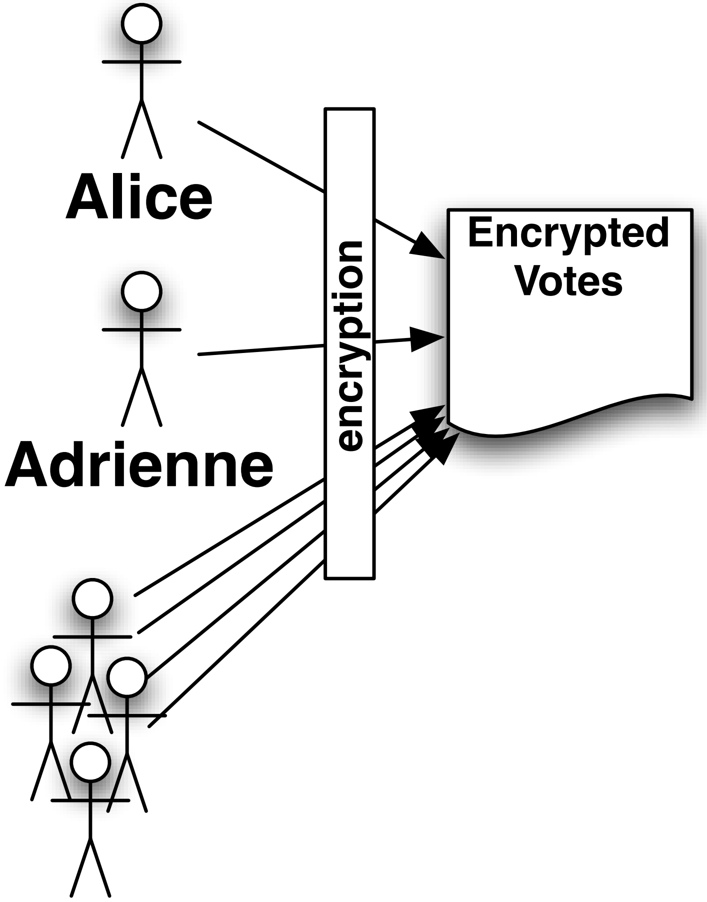
- **Threshold**
  multiple parties needed to decrypt
- **Provable**
  public proof of correct decryption

Crypto Voting Schemes

<- - - - - -> Verification

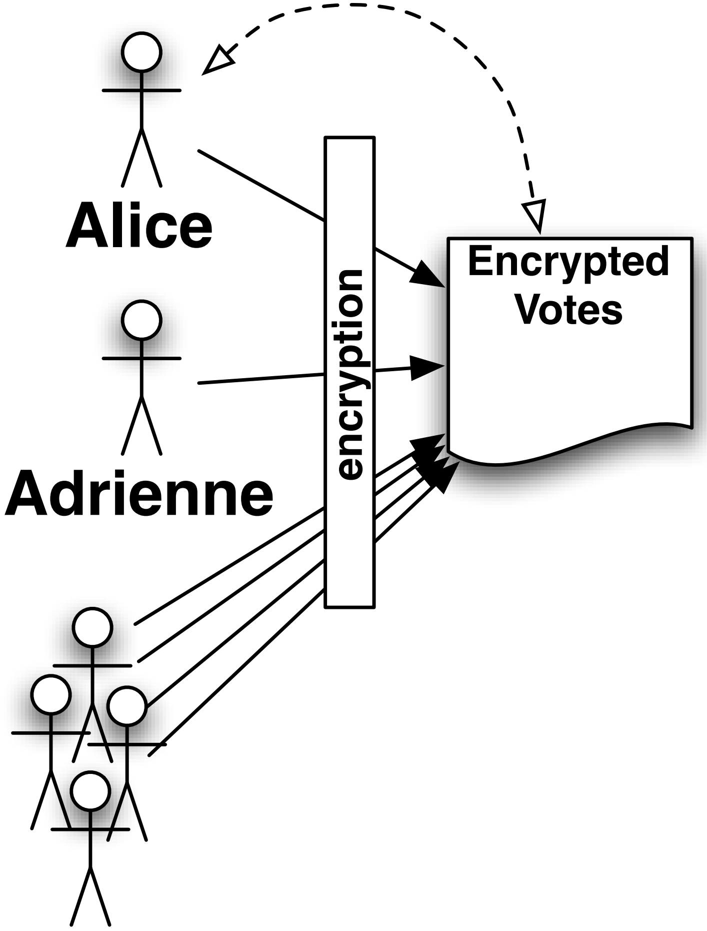
⟶ Ballot Data Flow

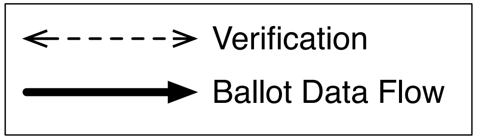
Crypto Voting Schemes



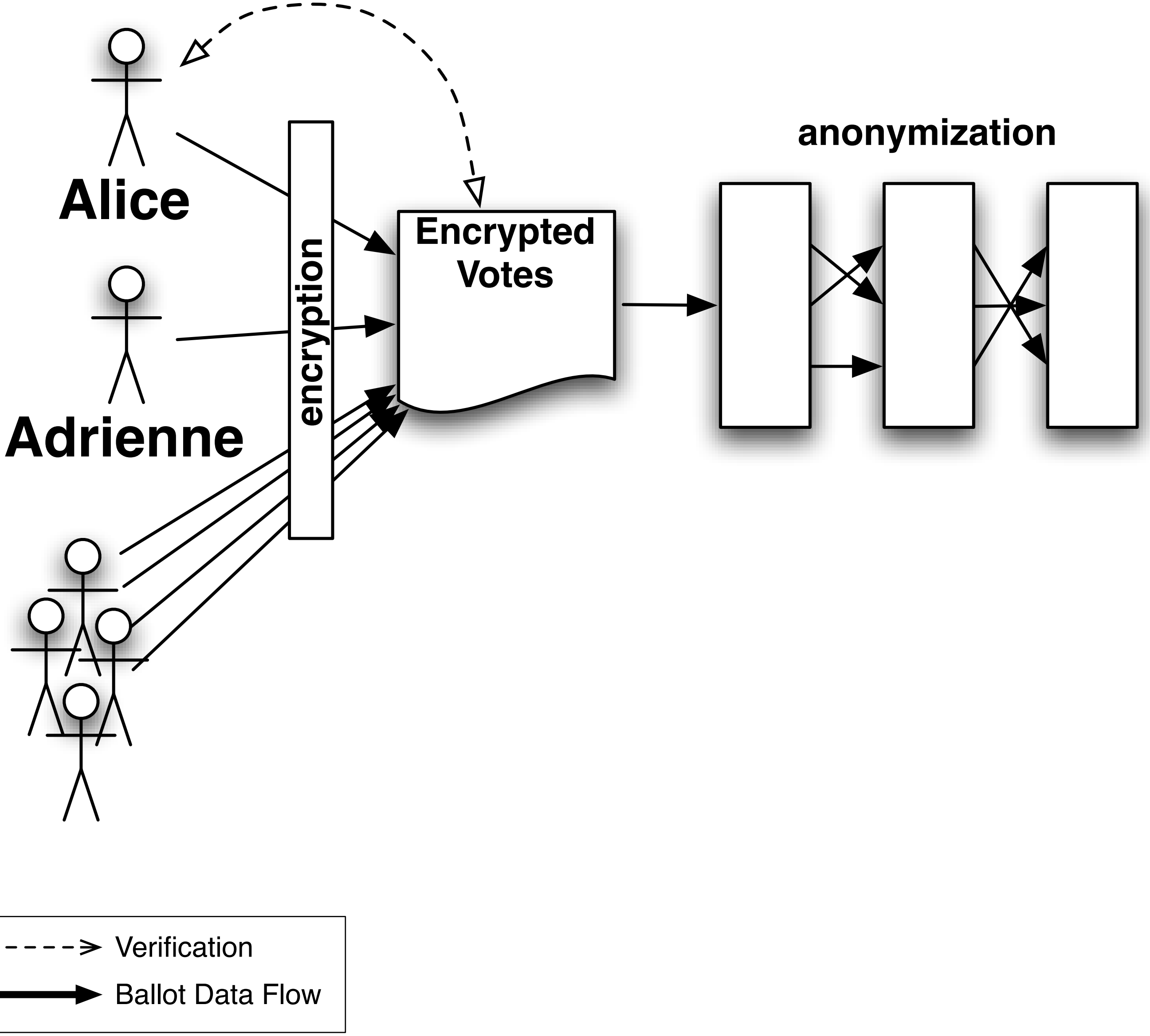
<-----> Verification
⟶ Ballot Data Flow

Crypto Voting Schemes

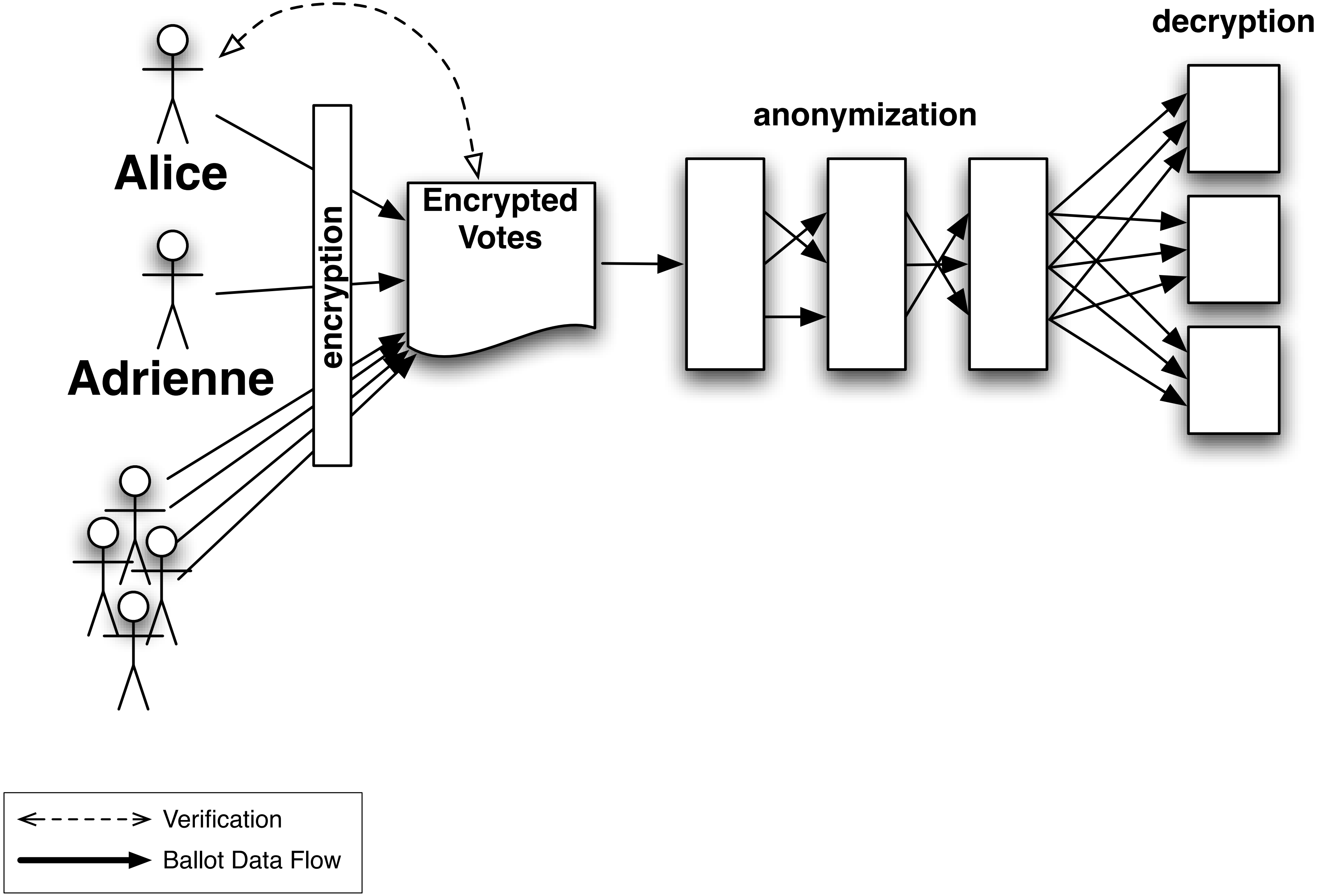




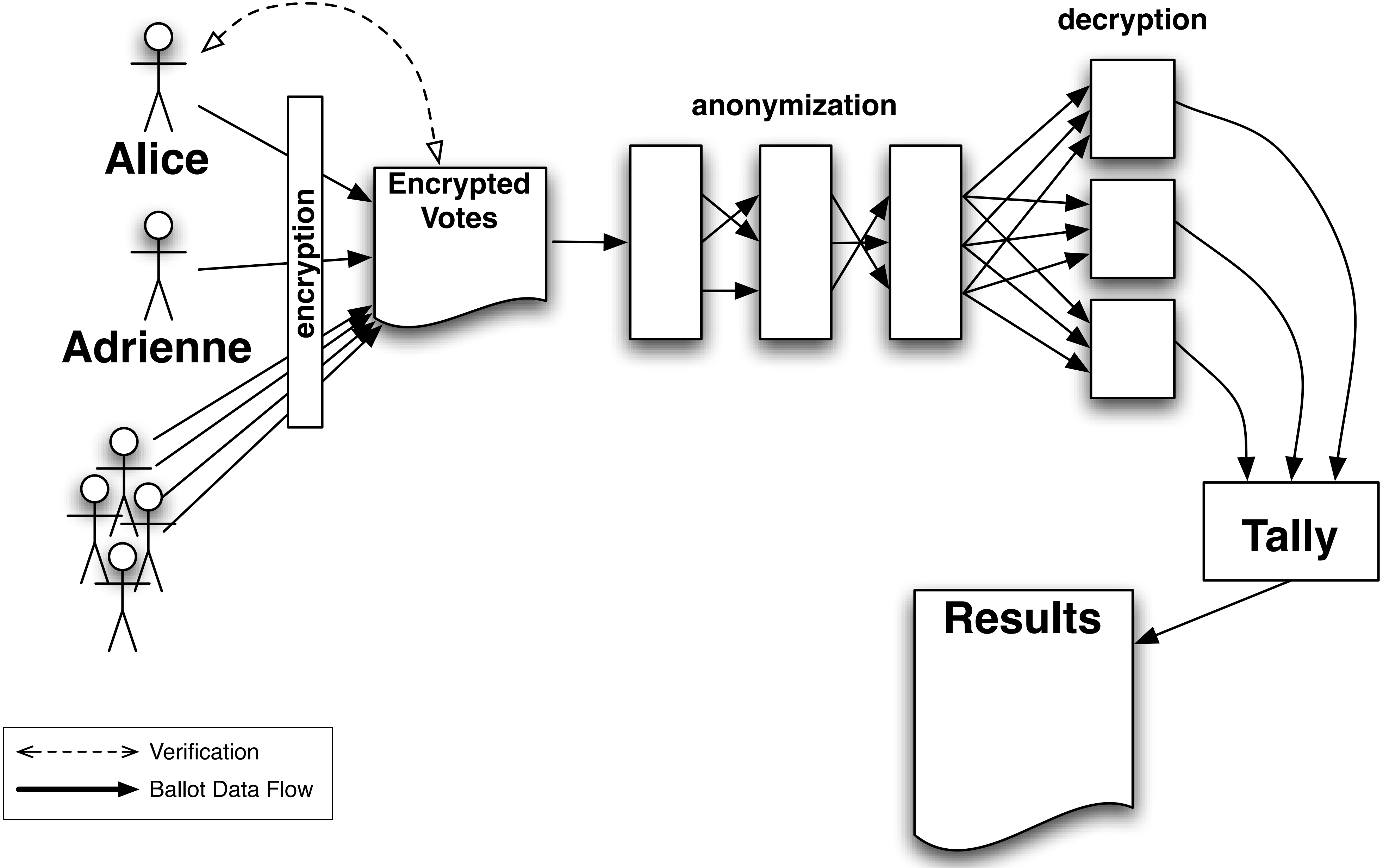
Crypto Voting Schemes



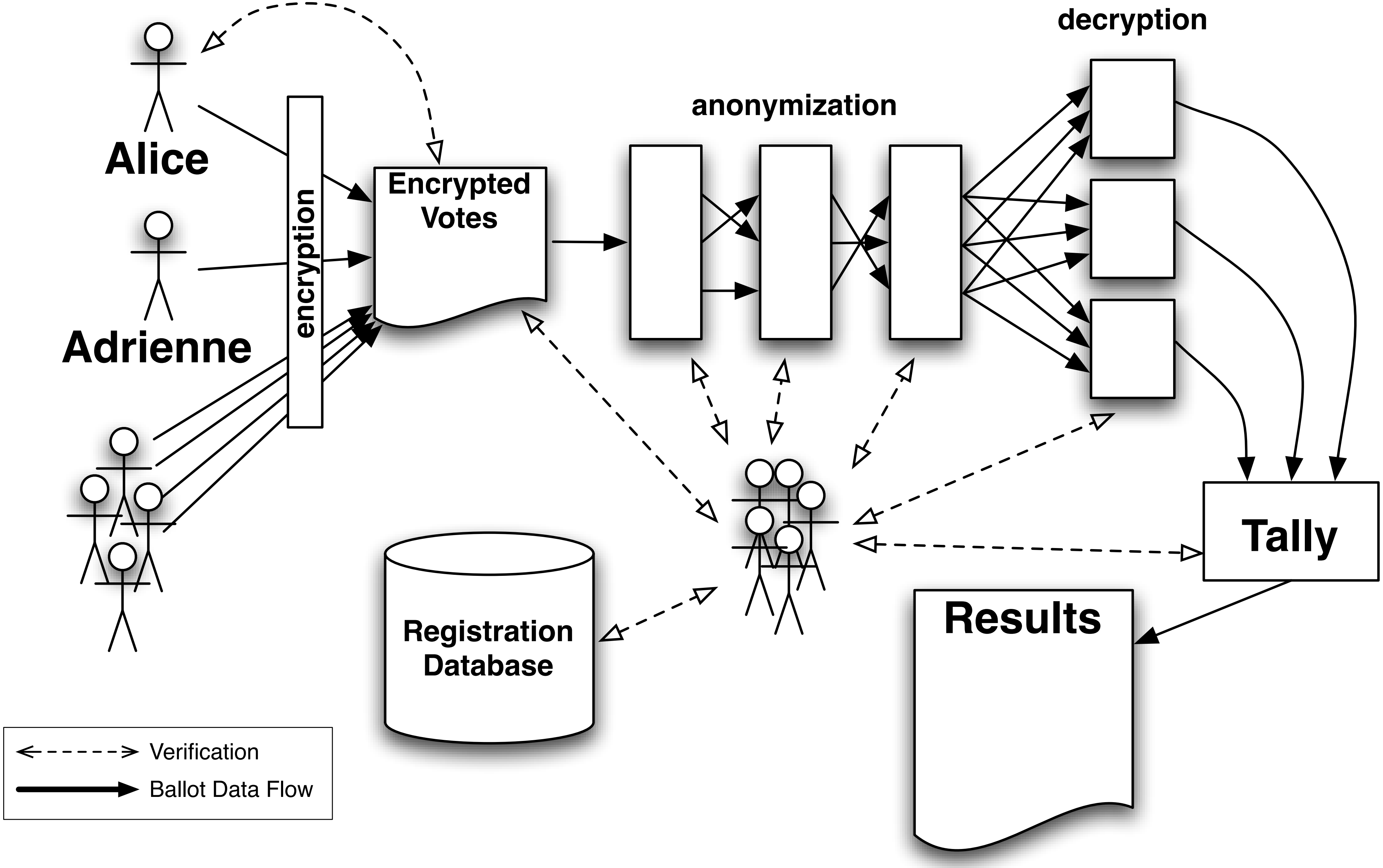
Crypto Voting Schemes



Crypto Voting Schemes



Crypto Voting Schemes



In Summary

In Summary

- End-to-End verification

In Summary

- End-to-End verification
- Secrecy and Verifiability ***are*** reconcilable

In Summary

- End-to-End verification
- Secrecy and Verifiability ***are*** reconcilable
- **Voting with Cryptography**:
  let *anyone* verify.

Questions?