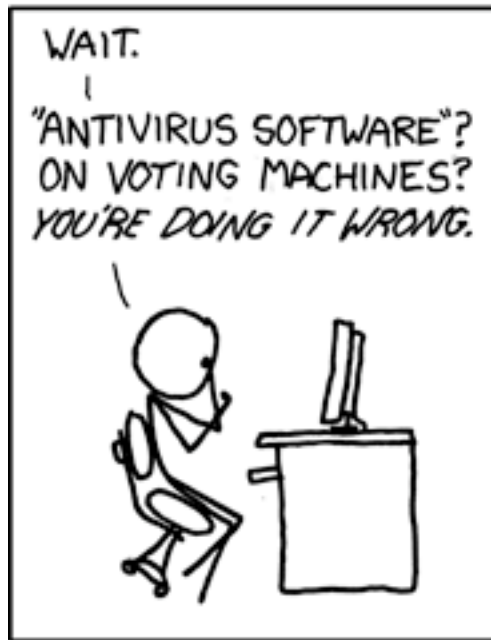
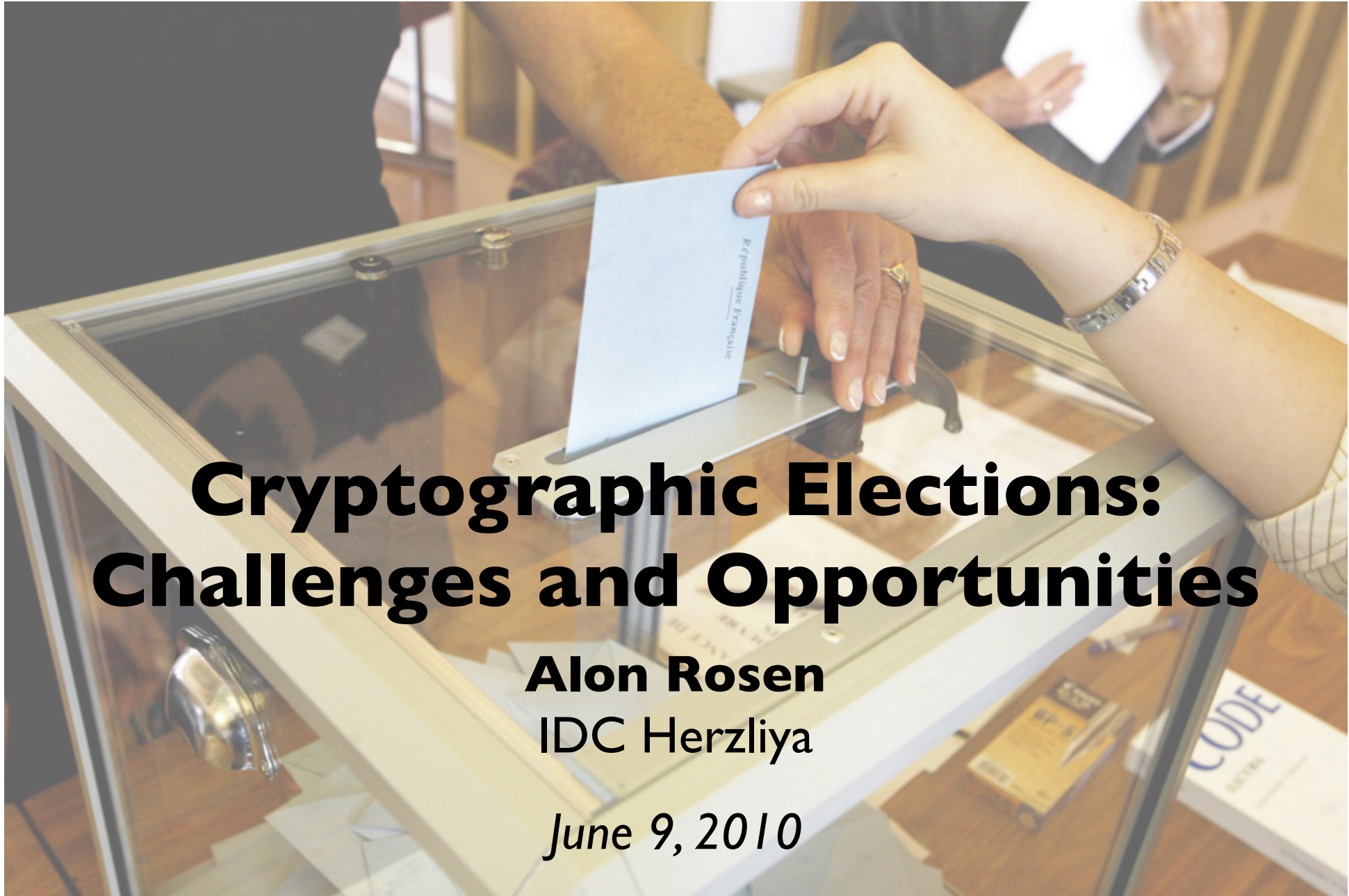


PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD)  
HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS  
WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.





# **Cryptographic Elections: Challenges and Opportunities**

**Alon Rosen**  
IDC Herzliya

*June 9, 2010*

# Thanks

- Ben Adida (Harvard University)
- Yuval Kedem (Gallileo)
- David Movshovitz (IDC Herzlyia)
- Shimon Schocken (IDC Herzlyia)
- Amnon Ta-Shma (Tel Aviv University)

# This Talk

## Part I

- ➡ Electronic voting in US
- ➡ The Israeli perspective

## Part II

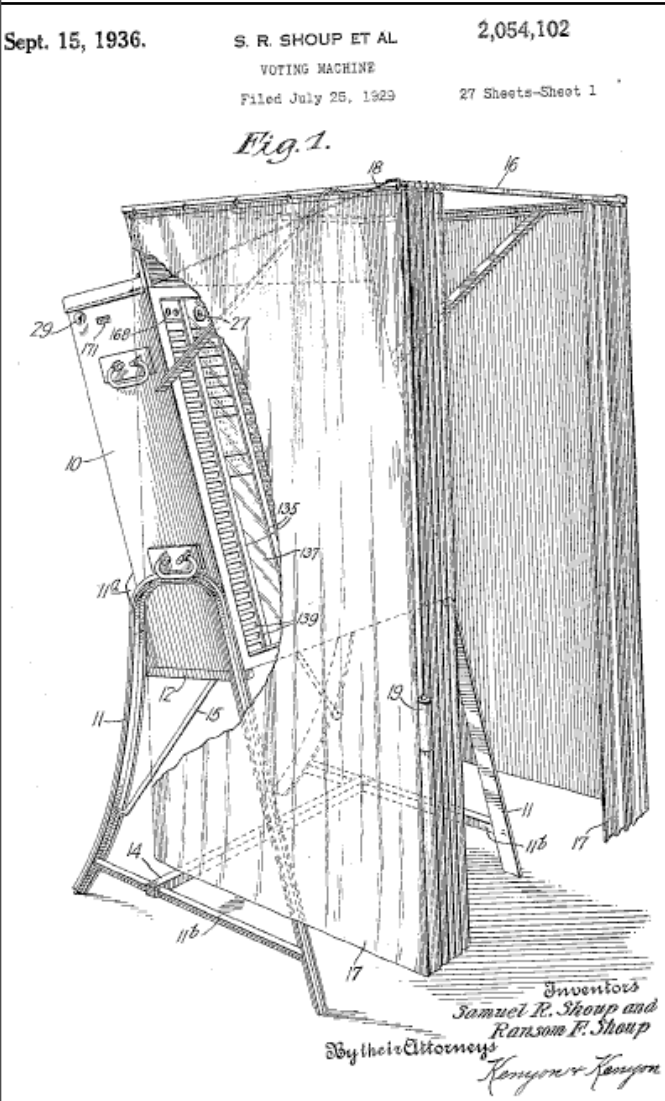
- ➡ Why is voting so hard?
- ➡ Cryptographic voting.



<http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html>

# Voting in the US

# Voting in the US



# Voting in the US

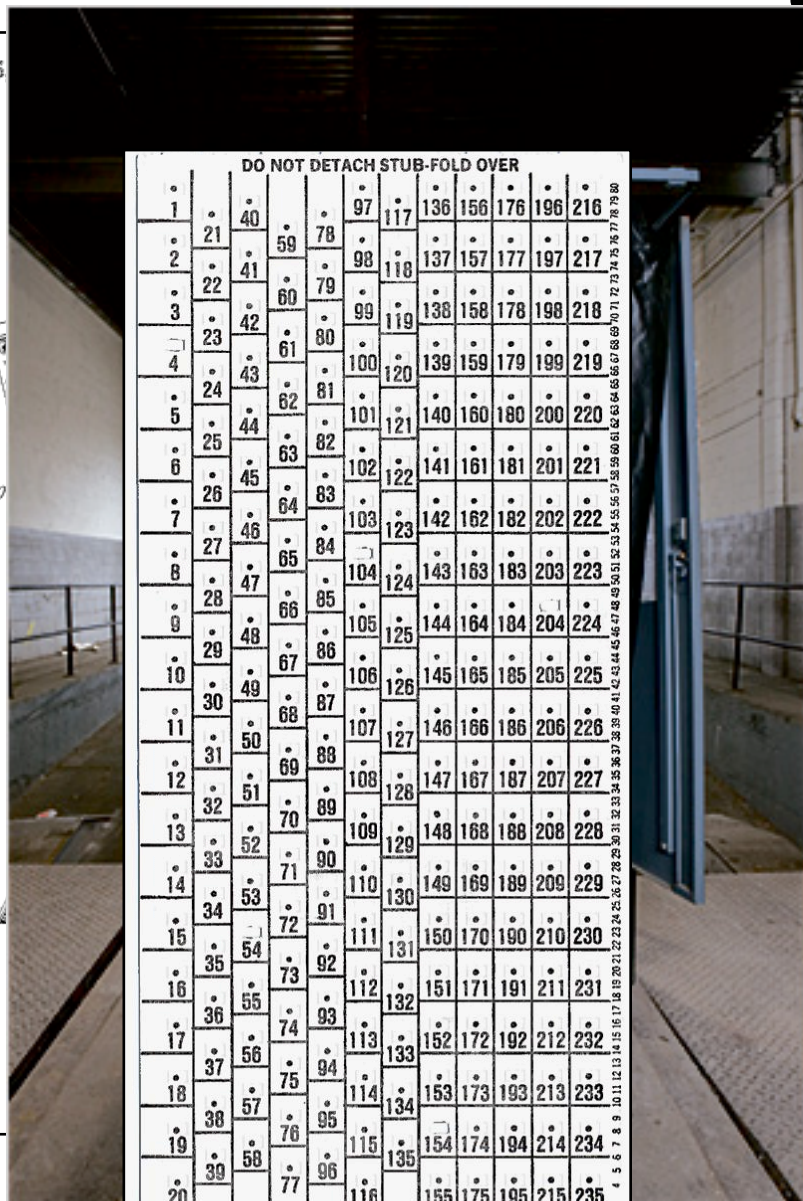


<http://www.cs.uiowa.edu/~jones/voting/pictures/>



# Voting in the US

Sept. 15



DO NOT DETACH STUB-FOLD OVER

|    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1  | 40 | 97 | 117 | 136 | 156 | 176 | 196 | 216 | 78  | 98  | 118 | 137 | 157 | 177 | 197 | 217 |     |     |     |
| 2  | 21 | 59 | 78  | 98  | 118 | 137 | 157 | 177 | 197 | 217 | 79  | 99  | 119 | 138 | 158 | 178 | 198 | 218 |     |
| 3  | 22 | 41 | 60  | 79  | 99  | 119 | 138 | 158 | 178 | 198 | 218 | 80  | 100 | 120 | 139 | 159 | 179 | 199 | 219 |
| 4  | 23 | 42 | 61  | 80  | 100 | 120 | 139 | 159 | 179 | 199 | 219 | 81  | 101 | 121 | 140 | 160 | 180 | 200 | 220 |
| 5  | 24 | 43 | 62  | 81  | 101 | 121 | 140 | 160 | 180 | 200 | 220 | 82  | 102 | 122 | 141 | 161 | 181 | 201 | 221 |
| 6  | 25 | 44 | 63  | 82  | 102 | 122 | 141 | 161 | 181 | 201 | 221 | 83  | 103 | 123 | 142 | 162 | 182 | 202 | 222 |
| 7  | 26 | 45 | 64  | 83  | 103 | 123 | 142 | 162 | 182 | 202 | 222 | 84  | 104 | 124 | 143 | 163 | 183 | 203 | 223 |
| 8  | 27 | 46 | 65  | 84  | 104 | 124 | 143 | 163 | 183 | 203 | 223 | 85  | 105 | 125 | 144 | 164 | 184 | 204 | 224 |
| 9  | 28 | 47 | 66  | 85  | 105 | 125 | 144 | 164 | 184 | 204 | 224 | 86  | 106 | 126 | 145 | 165 | 185 | 205 | 225 |
| 10 | 29 | 48 | 67  | 86  | 106 | 126 | 145 | 165 | 185 | 205 | 225 | 87  | 107 | 127 | 146 | 166 | 186 | 206 | 226 |
| 11 | 30 | 49 | 68  | 87  | 107 | 127 | 146 | 166 | 186 | 206 | 226 | 88  | 108 | 128 | 147 | 167 | 187 | 207 | 227 |
| 12 | 31 | 50 | 69  | 88  | 108 | 128 | 147 | 167 | 187 | 207 | 227 | 89  | 109 | 129 | 148 | 168 | 188 | 208 | 228 |
| 13 | 32 | 51 | 70  | 89  | 109 | 129 | 148 | 168 | 188 | 208 | 228 | 90  | 110 | 130 | 149 | 169 | 189 | 209 | 229 |
| 14 | 33 | 52 | 71  | 90  | 110 | 130 | 149 | 169 | 189 | 209 | 229 | 91  | 111 | 131 | 150 | 170 | 190 | 210 | 230 |
| 15 | 34 | 53 | 72  | 91  | 111 | 131 | 150 | 170 | 190 | 210 | 230 | 92  | 112 | 132 | 151 | 171 | 191 | 211 | 231 |
| 16 | 35 | 54 | 73  | 92  | 112 | 132 | 151 | 171 | 191 | 211 | 231 | 93  | 113 | 133 | 152 | 172 | 192 | 212 | 232 |
| 17 | 36 | 55 | 74  | 93  | 113 | 133 | 152 | 172 | 192 | 212 | 232 | 94  | 114 | 134 | 153 | 173 | 193 | 213 | 233 |
| 18 | 37 | 56 | 75  | 94  | 114 | 134 | 153 | 173 | 193 | 213 | 233 | 95  | 115 | 135 | 154 | 174 | 194 | 214 | 234 |
| 19 | 38 | 57 | 76  | 95  | 115 | 135 | 154 | 174 | 194 | 214 | 234 | 96  | 116 | 136 | 155 | 175 | 195 | 215 | 235 |
| 20 | 39 | 58 | 77  | 96  | 116 | 136 | 155 | 175 | 195 | 215 | 235 |     |     |     |     |     |     |     |     |

TO BE FILLED IN BY COUNTING BOARD ONLY  
 PRECINCT NO. \_\_\_\_\_ WRITE IN NO. \_\_\_\_\_

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

# Voting in the US

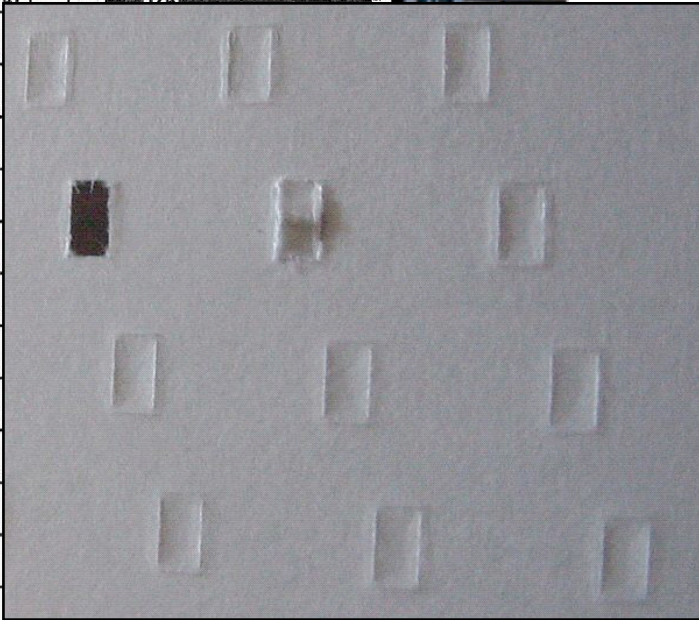
Sept. 15



DO NOT DETACH STUB-FOLD OVER

|    |    |    |     |     |     |     |     |     |     |     |     |
|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1  | 40 | 97 | 117 | 136 | 156 | 176 | 196 | 216 |     |     |     |
| 2  | 21 | 59 | 78  | 98  | 118 | 137 | 157 | 177 | 197 | 217 |     |
| 3  | 22 | 41 | 60  | 79  | 99  | 119 | 138 | 158 | 178 | 198 | 218 |
| 4  | 23 | 42 | 61  | 80  | 100 | 120 | 139 | 159 | 179 | 199 | 219 |
| 5  | 24 | 43 | 62  | 81  | 101 | 121 | 140 | 160 | 180 | 200 | 220 |
| 6  | 25 | 44 | 63  | 82  | 102 | 122 | 141 | 161 | 181 | 201 | 221 |
| 7  | 26 | 45 | 64  | 83  | 103 | 123 | 142 | 162 | 182 | 202 | 222 |
| 8  | 27 | 46 | 65  | 84  | 104 | 124 | 143 | 163 | 183 | 203 | 223 |
| 9  | 28 | 47 |     |     |     |     |     |     |     |     |     |
| 10 | 29 |    |     |     |     |     |     |     |     |     |     |
| 11 | 30 |    |     |     |     |     |     |     |     |     |     |
| 12 | 31 |    |     |     |     |     |     |     |     |     |     |
| 13 | 32 |    |     |     |     |     |     |     |     |     |     |
| 14 | 33 |    |     |     |     |     |     |     |     |     |     |
| 15 | 34 |    |     |     |     |     |     |     |     |     |     |
| 16 | 35 |    |     |     |     |     |     |     |     |     |     |
| 17 | 36 |    |     |     |     |     |     |     |     |     |     |
| 18 | 37 |    |     |     |     |     |     |     |     |     |     |
| 19 | 38 |    |     |     |     |     |     |     |     |     |     |
| 20 | 39 |    |     |     |     |     |     |     |     |     |     |

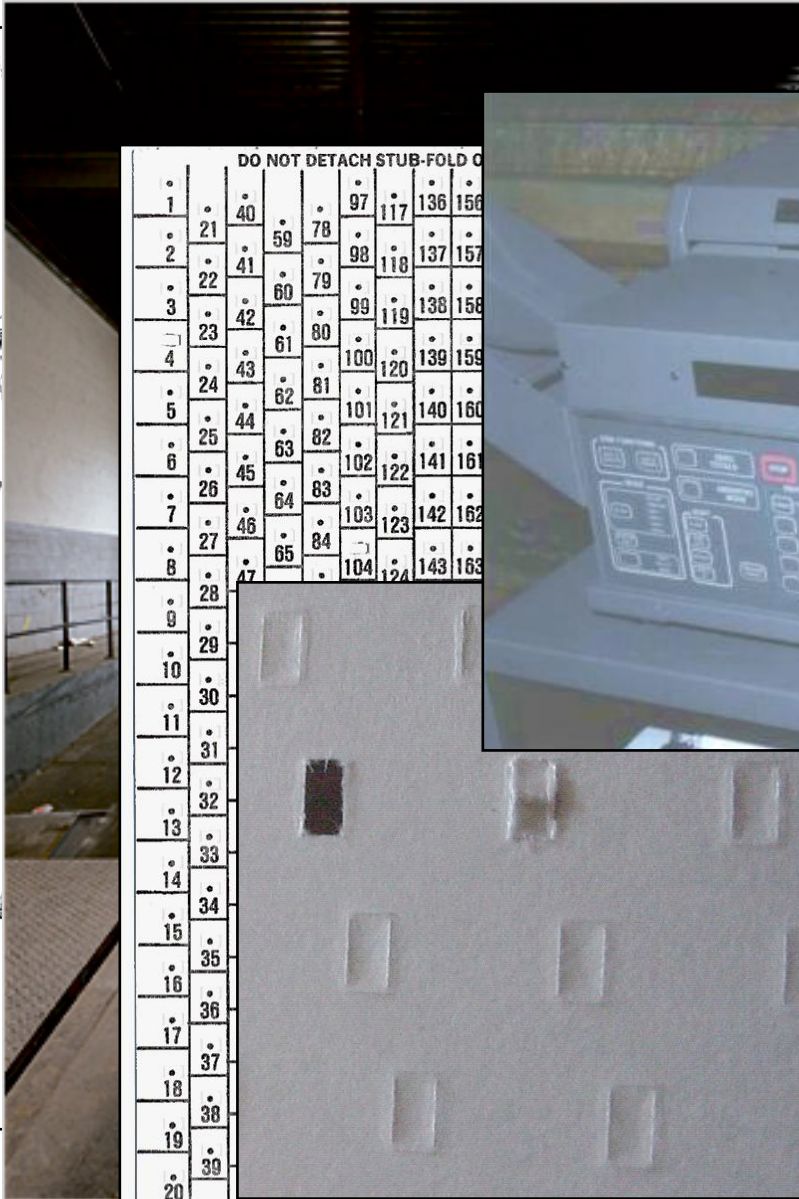
TO BE FILLED IN BY COUNTING BOARD ONLY  
 PRECINCT NO. \_\_\_\_\_ WRITE-IN NO. \_\_\_\_\_



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

# Voting in the US

Sept. 15



DO NOT DETACH STUB-FOLD OVER

|    |    |    |     |     |     |     |     |     |
|----|----|----|-----|-----|-----|-----|-----|-----|
| 1  | 40 | 97 | 117 | 136 | 156 |     |     |     |
| 2  | 21 | 59 | 78  | 98  | 118 | 137 | 157 |     |
| 3  | 22 | 41 | 60  | 79  | 99  | 119 | 138 | 158 |
| 4  | 23 | 42 | 61  | 80  | 100 | 120 | 139 | 159 |
| 5  | 24 | 43 | 62  | 81  | 101 | 121 | 140 | 160 |
| 6  | 25 | 44 | 63  | 82  | 102 | 122 | 141 | 161 |
| 7  | 26 | 45 | 64  | 83  | 103 | 123 | 142 | 162 |
| 8  | 27 | 46 | 65  | 84  | 104 | 124 | 143 | 163 |
| 9  | 28 |    |     |     |     |     |     |     |
| 10 | 29 |    |     |     |     |     |     |     |
| 11 | 30 |    |     |     |     |     |     |     |
| 12 | 31 |    |     |     |     |     |     |     |
| 13 | 32 |    |     |     |     |     |     |     |
| 14 | 33 |    |     |     |     |     |     |     |
| 15 | 34 |    |     |     |     |     |     |     |
| 16 | 35 |    |     |     |     |     |     |     |
| 17 | 36 |    |     |     |     |     |     |     |
| 18 | 37 |    |     |     |     |     |     |     |
| 19 | 38 |    |     |     |     |     |     |     |
| 20 | 39 |    |     |     |     |     |     |     |



TO BE FILLED IN BY COUNTING BOARD ONLY  
 PRECINCT NO. \_\_\_\_\_ WRITE-IN NO. \_\_\_\_\_

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

# Voting in the US

Sept. 15



DO NOT DETACH STUB-FOLD OVER

|    |    |    |     |     |     |     |     |     |
|----|----|----|-----|-----|-----|-----|-----|-----|
| 1  | 40 | 97 | 117 | 136 | 156 |     |     |     |
| 2  | 21 | 59 | 78  | 98  | 118 | 137 | 157 |     |
| 3  | 22 | 41 | 60  | 79  | 99  | 119 | 138 | 158 |
| 4  | 23 | 42 | 61  | 80  | 100 | 120 | 139 | 159 |
| 5  | 24 | 43 | 62  | 81  | 101 | 121 | 140 | 160 |
| 6  | 25 | 44 | 63  | 82  | 102 | 122 | 141 | 161 |
| 7  | 26 | 45 | 64  | 83  | 103 | 123 | 142 | 162 |
| 8  | 27 | 46 | 65  | 84  | 104 | 124 | 143 | 163 |
| 9  | 28 |    |     |     |     |     |     |     |
| 10 | 29 |    |     |     |     |     |     |     |
| 11 | 30 |    |     |     |     |     |     |     |
| 12 | 31 |    |     |     |     |     |     |     |
| 13 | 32 |    |     |     |     |     |     |     |
| 14 | 33 |    |     |     |     |     |     |     |
| 15 | 34 |    |     |     |     |     |     |     |
| 16 | 35 |    |     |     |     |     |     |     |
| 17 | 36 |    |     |     |     |     |     |     |
| 18 | 37 |    |     |     |     |     |     |     |
| 19 | 38 |    |     |     |     |     |     |     |
| 20 | 39 |    |     |     |     |     |     |     |

TO BE FILLED IN BY COUNTING BOARD **ONLY**  
PRECINCT NO. \_\_\_\_\_ WRITE-IN NO. \_\_\_\_\_

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

# Confusion over Palm Beach County ballot

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform Party.

|  |      |      |   |
|--|------|------|---|
| (REPUBLICAN)<br>GEORGE W. BUSH - PRESIDENT<br>DICK CHENEY - VICE PRESIDENT         | 3 →  |      |   |
| (DEMOCRATIC)<br>AL GORE - PRESIDENT<br>JOE LIEBERMAN - VICE PRESIDENT              | 5 →  | ← 4  | (REFORM)<br>PAT BUCHANAN - PRESIDENT<br>EZOLA FOSTER - VICE PRESIDENT   |
| (LIBERTARIAN)<br>HARRY BROWNE - PRESIDENT<br>ART OLIVIER - VICE PRESIDENT          | 7 →  | ← 6  | (SOCIALIST)<br>DAVID McREYNOLDS - PRESIDENT<br>MARY CAL HOLLIS - VICE PRESIDENT                                     |
| (GREEN)<br>RALPH NADER - PRESIDENT<br>WINDA LaDUKE - VICE PRESIDENT                | 9 →  | ← 8  | (CONSTITUTION)<br>HOWARD PHILLIPS - PRESIDENT<br>J. CURTIS FRAZIER - VICE PRESIDENT                                 |
| (SOCIALIST WORKERS)<br>JAMES HARRIS - PRESIDENT<br>MARGARET TROWE - VICE PRESIDENT | 11 → | ← 10 | (WORKERS WORLD)<br>MONICA MOOREHEAD - PRESIDENT<br>GLORIA La RIVA - VICE PRESIDENT                                  |
| (NATURAL LAW)<br>JOHN HAGELIN - PRESIDENT<br>NAT GOLDHABER - VICE PRESIDENT        | 13 → |      | WRITE-IN CANDIDATE<br>To vote for a write-in candidate, follow the directions on the long stub of your ballot card. |



Sun-Sentinel graphic/Daniel Niblock

## Confusion over Palm Beach County ballot

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

|  |      |   |
|--|------|---|
| (REPUBLICAN)<br>GEORGE W. BUSH - PRESIDENT<br>DICK CHENEY - VICE PRESIDENT         | 3 →  |   |
| (DEMOCRATIC)<br>AL GORE - PRESIDENT<br>JOE LIEBERMAN - VICE PRESIDENT              | 5 →  | ← 4 (REFORM)<br>PAT BUCHANAN - PRESIDENT<br>EZOLA FOSTER - VICE PRESIDENT   |
| (LIBERTARIAN)<br>HARRY BROWNE - PRESIDENT<br>ART OLIVIER - VICE PRESIDENT          | 7 →  | ← 6 (SOCIALIST)<br>DAVID McREYNOLDS - PRESIDENT<br>MARY CAL HOLLIS - VICE PRESIDENT                                 |
| (GREEN)<br>RALPH NADER - PRESIDENT<br>WINDNA LaDUKE - VICE PRESIDENT               | 9 →  | ← 8 (CONSTITUTION)<br>HOWARD PHILLIPS - PRESIDENT<br>J. CURTIS FRAZIER - VICE PRESIDENT                             |
| (SOCIALIST WORKERS)<br>JAMES HARRIS - PRESIDENT<br>MARGARET TROWE - VICE PRESIDENT | 11 → | ← 10 (WORKERS WORLD)<br>MONICA MOOREHEAD - PRESIDENT<br>GLORIA La RIVA - VICE PRESIDENT                             |
| (NATURAL LAW)<br>JOHN HAGELIN - PRESIDENT<br>NAT GOLDHABER - VICE PRESIDENT        | 13 → | WRITE-IN CANDIDATE<br>To vote for a write-in candidate, follow the directions on the long stub of your ballot card. |

Sun-Sentinel graphic/Daniel Niblock



- HAVA - Help America Vote Act
- 4 Billion dollars allocated
- Mostly to replace voting machines



- HAVA - Help America Vote Act
- 4 Billion dollars allocated
- Mostly to replace voting machines

# The 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%

OK Cancel

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

[FHF2006]



- New Mexico (March 2006)
- California (August 2007)
- Florida (December 2007)
- Ohio (January 2008)
- Iowa (March 2008)
- ...
  
- States that mandate paper trail.

# State of California



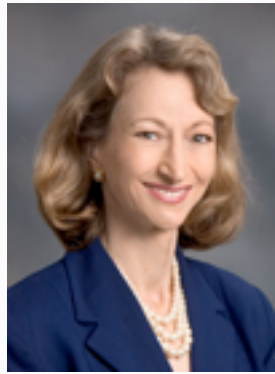
## SECRETARY OF STATE

**WITHDRAWAL OF APPROVAL OF  
DIEBOLD ELECTION SYSTEMS, INC.,  
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS  
DRE & OPTICAL SCAN VOTING SYSTEM  
AND CONDITIONAL RE-APPROVAL OF  
USE OF DIEBOLD ELECTION SYSTEMS, INC.,  
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS  
DRE & OPTICAL SCAN VOTING SYSTEM**

# State of California



**SECRETARY OF STATE**



**Debra Bowen**

**WITHDRAWAL OF APPROVAL OF  
DIEBOLD ELECTION SYSTEMS, INC.,  
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS  
DRE & OPTICAL SCAN VOTING SYSTEM  
AND CONDITIONAL RE-APPROVAL OF  
USE OF DIEBOLD ELECTION SYSTEMS, INC.,  
GEMS 1.18.24/AccuVote-TSX/AccuVote-OS  
DRE & OPTICAL SCAN VOTING SYSTEM**

# What does Everbody Want?

- Simple and reliable system
- Voter secrecy
- Quick count
  
- And in addition: transparency (open audit).

# What is Transparency?

Anyone can verify that:

- their vote was cast as intended
- the votes were count as cast



# Paper vs. Electronic

## Paper elections:

- Local attacks
- No transparency

## Electronic elections today:

- Global attacks
- Undetectable
- Unrecoverable
- No transparency

# Paper vs. Electronic

## Paper elections:

- Local attacks
- No transparency

## Electronic elections today:

- Global attacks
- Undetectable
- Unrecoverable
- No transparency

## Ideally:

- No local/global attacks
- Full transparency

# Aviation and Banking?

<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>



# Aviation and Banking?



<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Aviation and Banking?



- Little defense against insiders

<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Aviation and Banking?



- Little defense against insiders
- Failures are obvious

<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Aviation and Banking?



- Little defense against insiders
- Failures are obvious



<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Aviation and Banking?



- Little defense against insiders
- Failures are obvious



- Complete audit logs

<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Aviation and Banking?



- Little defense against insiders
- Failures are obvious



- Complete audit logs
- Transferability of claims

<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Aviation and Banking?



- Little defense against insiders
- Failures are obvious



- Complete audit logs
- Transferability of claims

These are poor analogies.

<http://commons.wikimedia.org/wiki/Image:738100.jpg>

<http://www.sxc.hu/photo/206579>

# Open-Source?



EXCLUSIVE EVENT  
BY INVITATION ONLY

THE HOLLYWOOD HILL

Invites you to

## TOWARDS "WE.GOV"

RESTORING TRUST IN OUR ELECTIONS SYSTEMS

an exclusive presentation and discussion with the  
**OPEN SOURCE DIGITAL VOTING FOUNDATION**  
and special guests

California Secretary of State Debra Bowen

Technology Entrepreneur Mitch Kapor

RockTheVote Exec Director Heather Smith

Registrar-Recorder for L.A County Dean Logan

**Wednesday, October 21st, 2009 | 7:00 – 10:00 pm**

Residence of Film Producer Lawrence Bender in Bel Air, CA.

**By Invitation Only.** Cocktails, Hors D'oeuvres, Valet Parking.  
For special requests, email [Paris@hhill.org](mailto:Paris@hhill.org)



# Software Independence

## [Rivest, Wack'06]

“A voting system is software independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome”

# Examples



<http://www.youtube.com/watch?v=zeHmsrLc4jc>

# Examples



<http://www.youtube.com/watch?v=zeHmsrLc4jc>

# Non-example





# The Israeli Perspective



- Nov '07: Pilot of electronic voting with touch screens in several municipalities.
- Nov '07: Minister of interior announces plan to move to electronic elections
- Apr '08: TEHILA are given mandate to run pilot in 3 municipalities.
- Sep'08 - today: Legislation underway to accommodate pilot.

## The process:

- No public scrutiny
- No open design

## The result:

- No paper trail
- No software independence

**Why is Voting  
so Hard?**

# 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.



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

# **Secret Ballot vs. Verifiability**

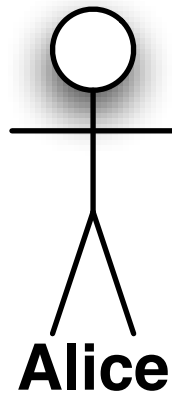
# Secret Ballot vs. Verifiability

Voting System

# Secret Ballot vs. Verifiability

Voting System

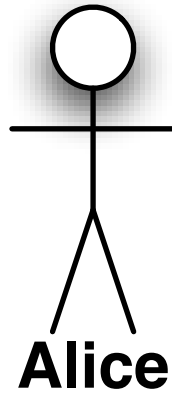
convince



# Secret Ballot vs. Verifiability

Voting System

convince

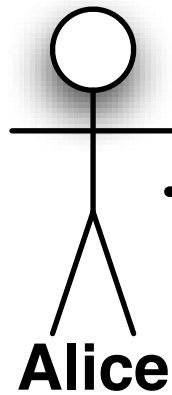


**Carl the Coercer**

# Secret Ballot vs. Verifiability

Voting System

convince



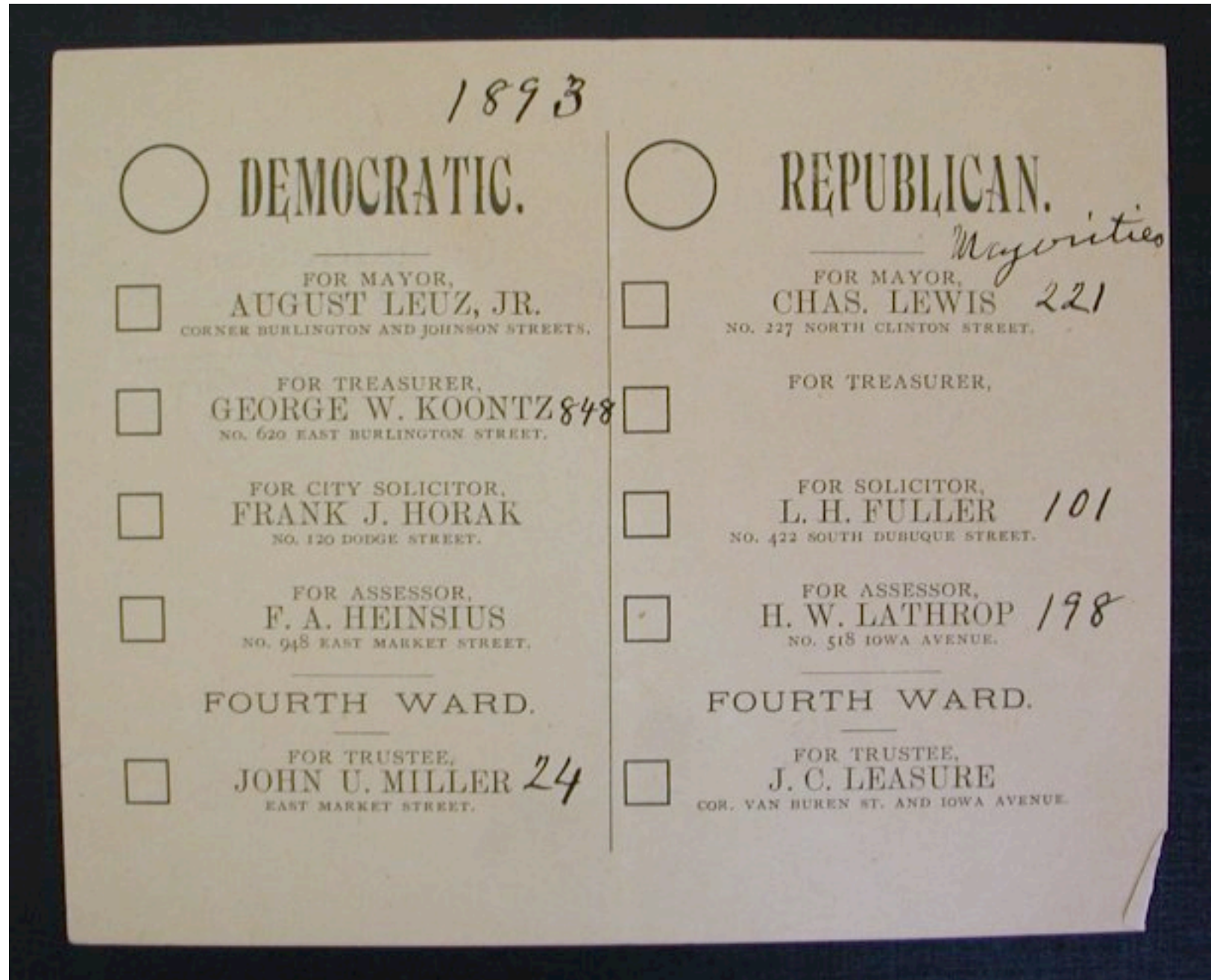
**Carl the Coercer**

# Desired Properties

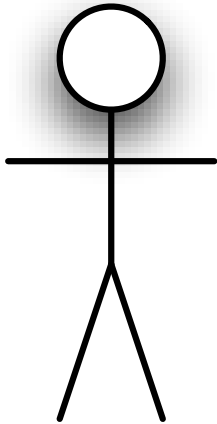
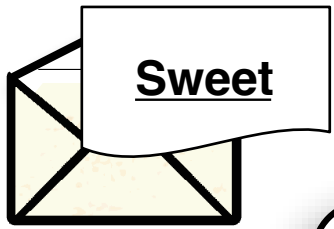
- (1) **Alice** verifies **her vote**.
- (2) **Everyone** verifies **tallying**.
- (3) Alice **cannot be coerced** by Eve.



# 1892 - Australian Ballot

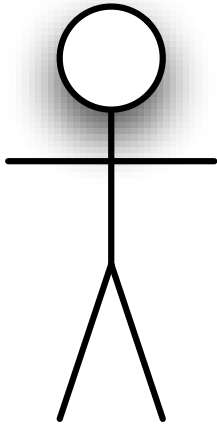
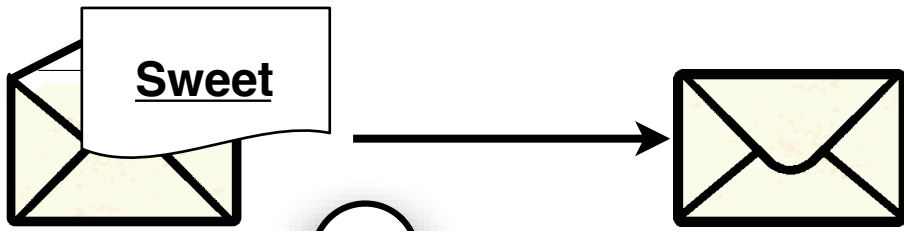


# The Ballot Handoff



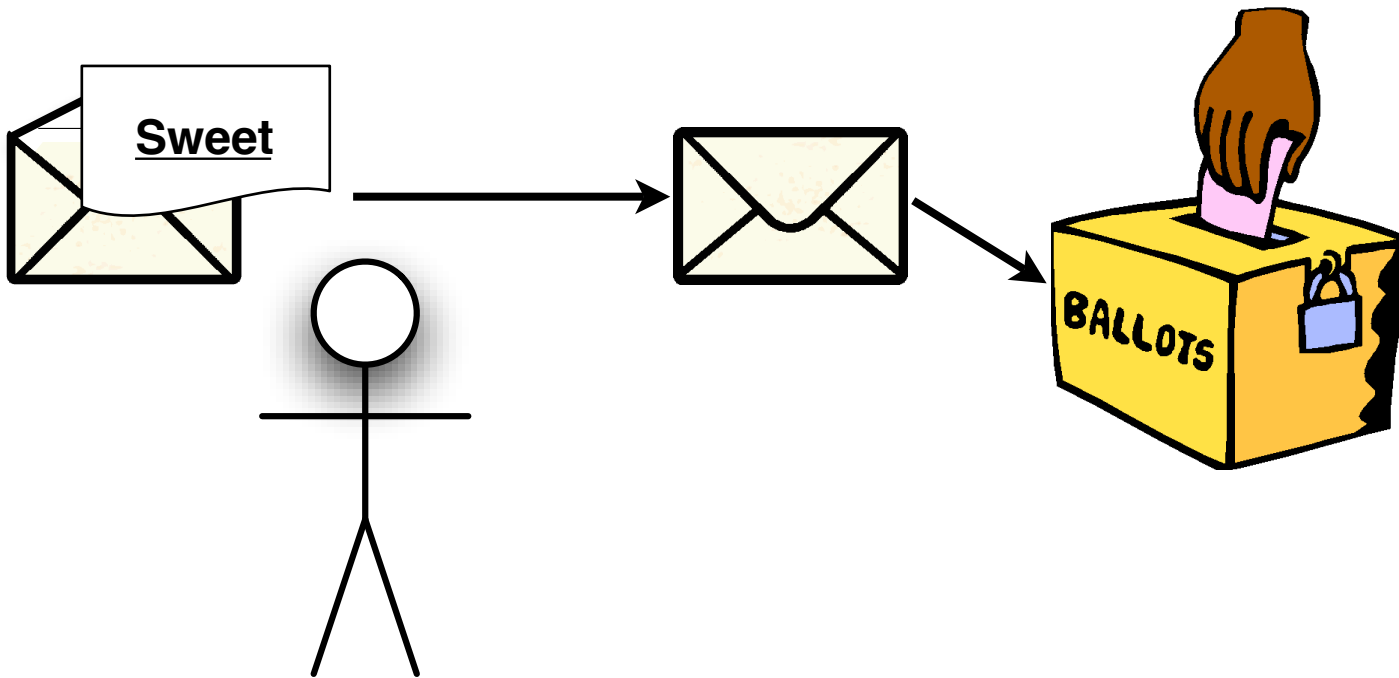
**Alice the Voter**

# The Ballot Handoff



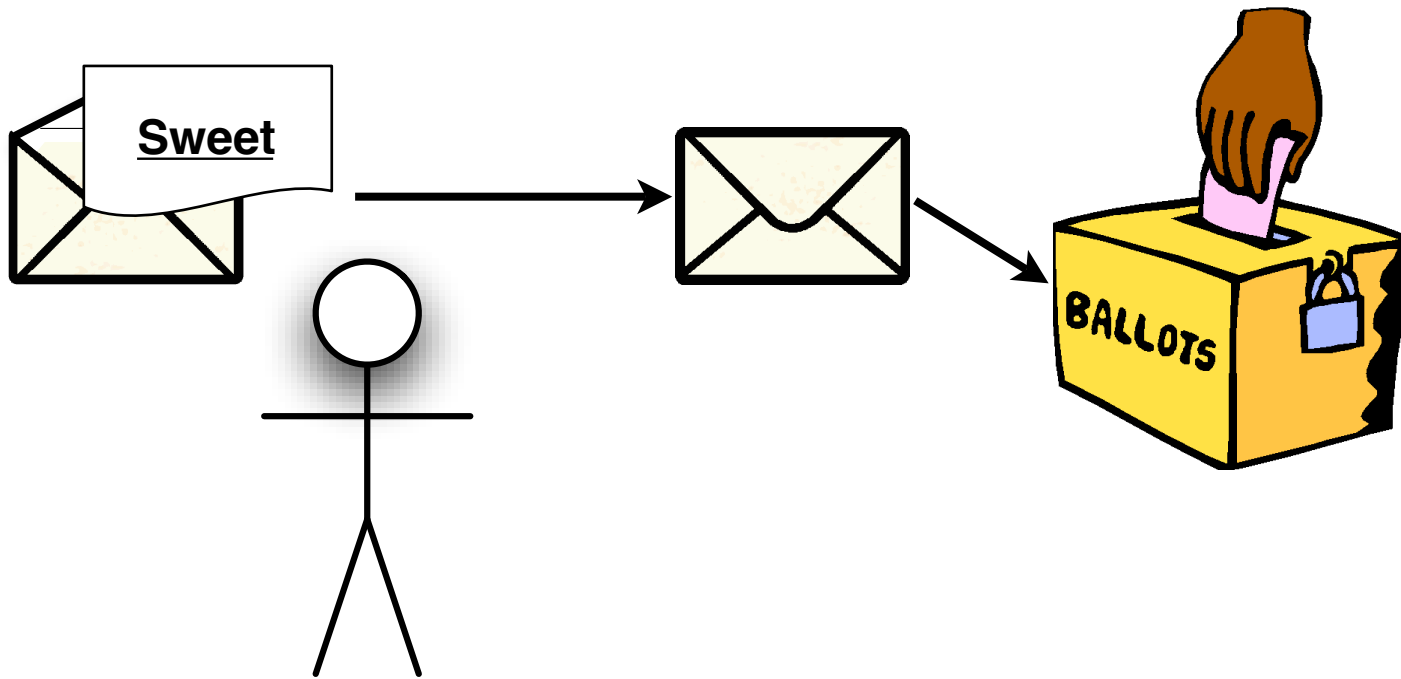
**Alice the Voter**

# The Ballot Handoff



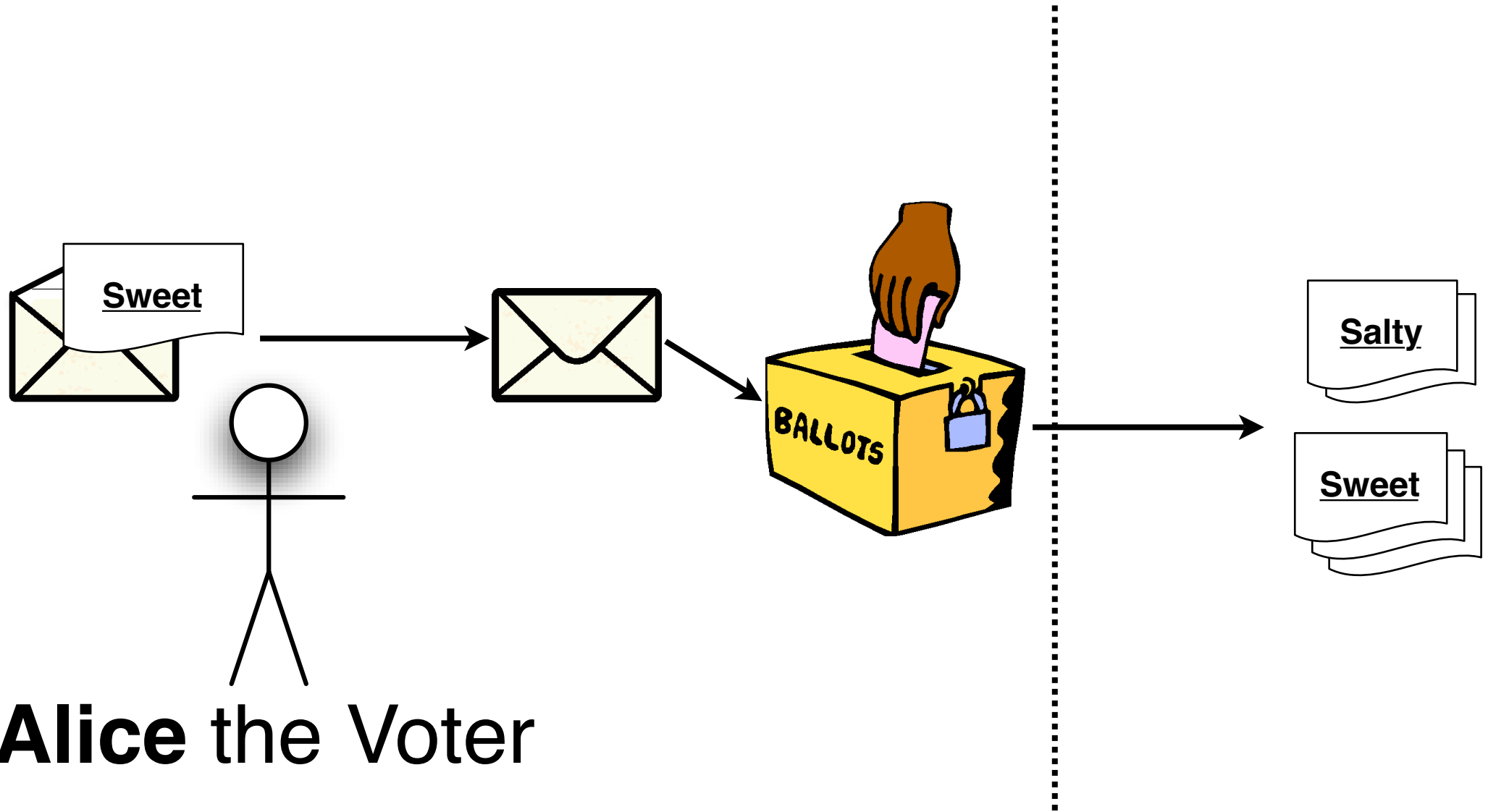
**Alice the Voter**

# The Ballot Handoff

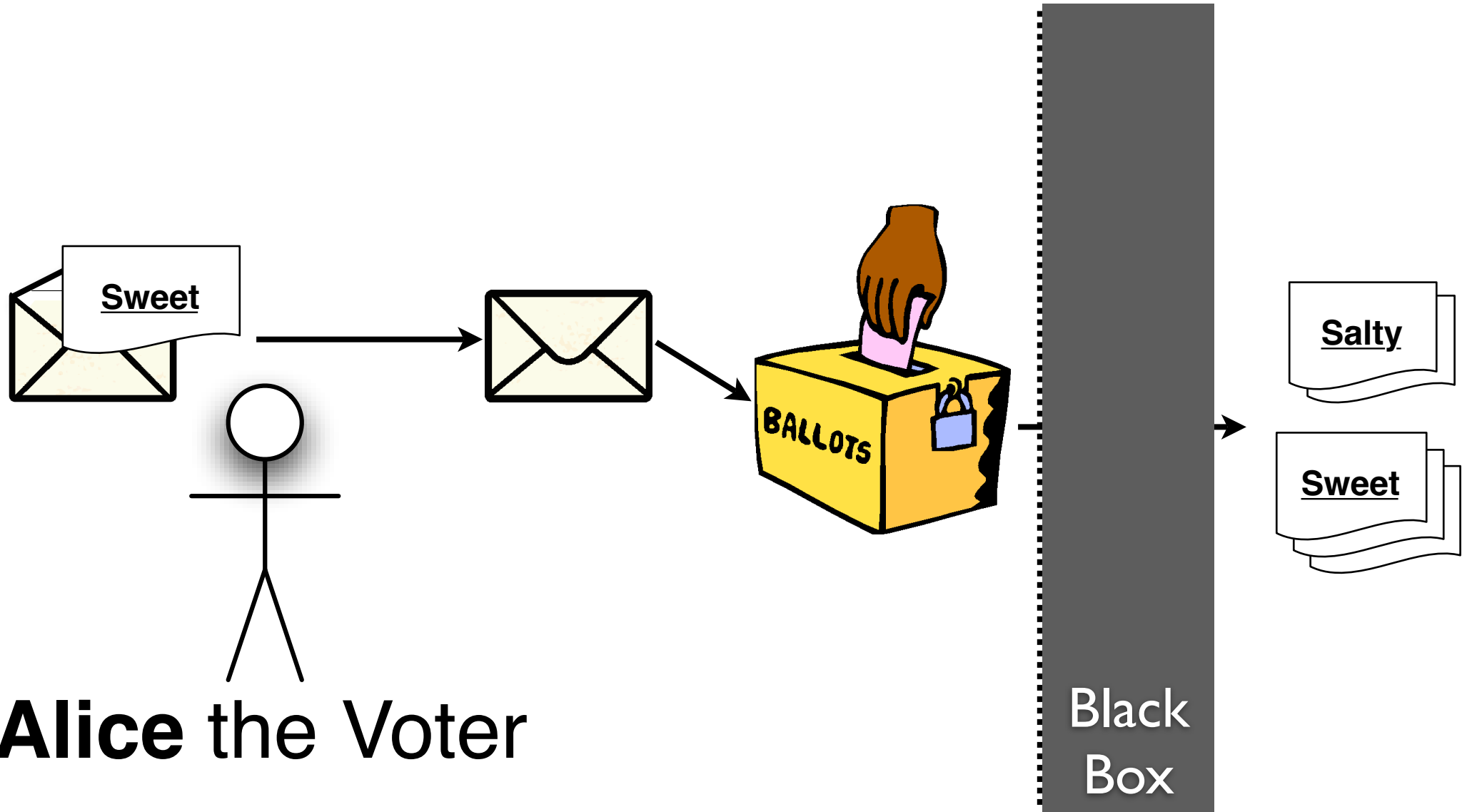


**Alice the Voter**

# The Ballot Handoff



# The Ballot Handoff



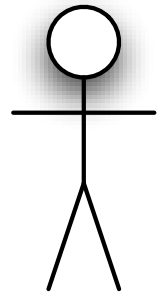
# Chain of Custody



# Chain of Custody

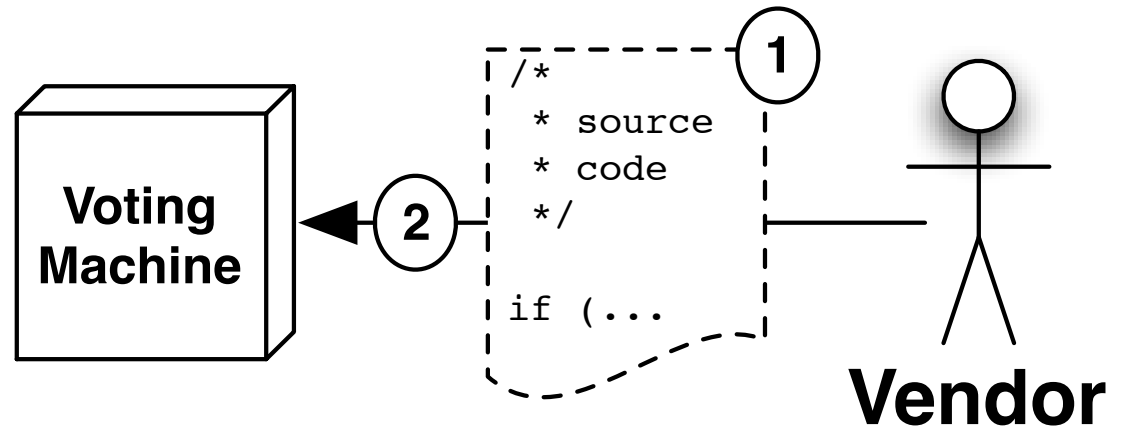
```
/*  
 * source  
 * code  
 */  
if (...
```

1

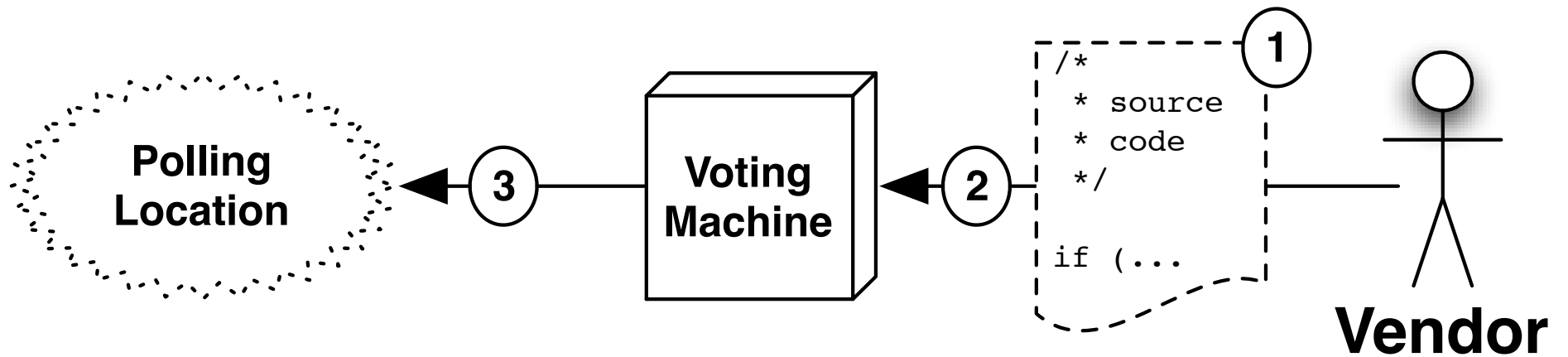


**Vendor**

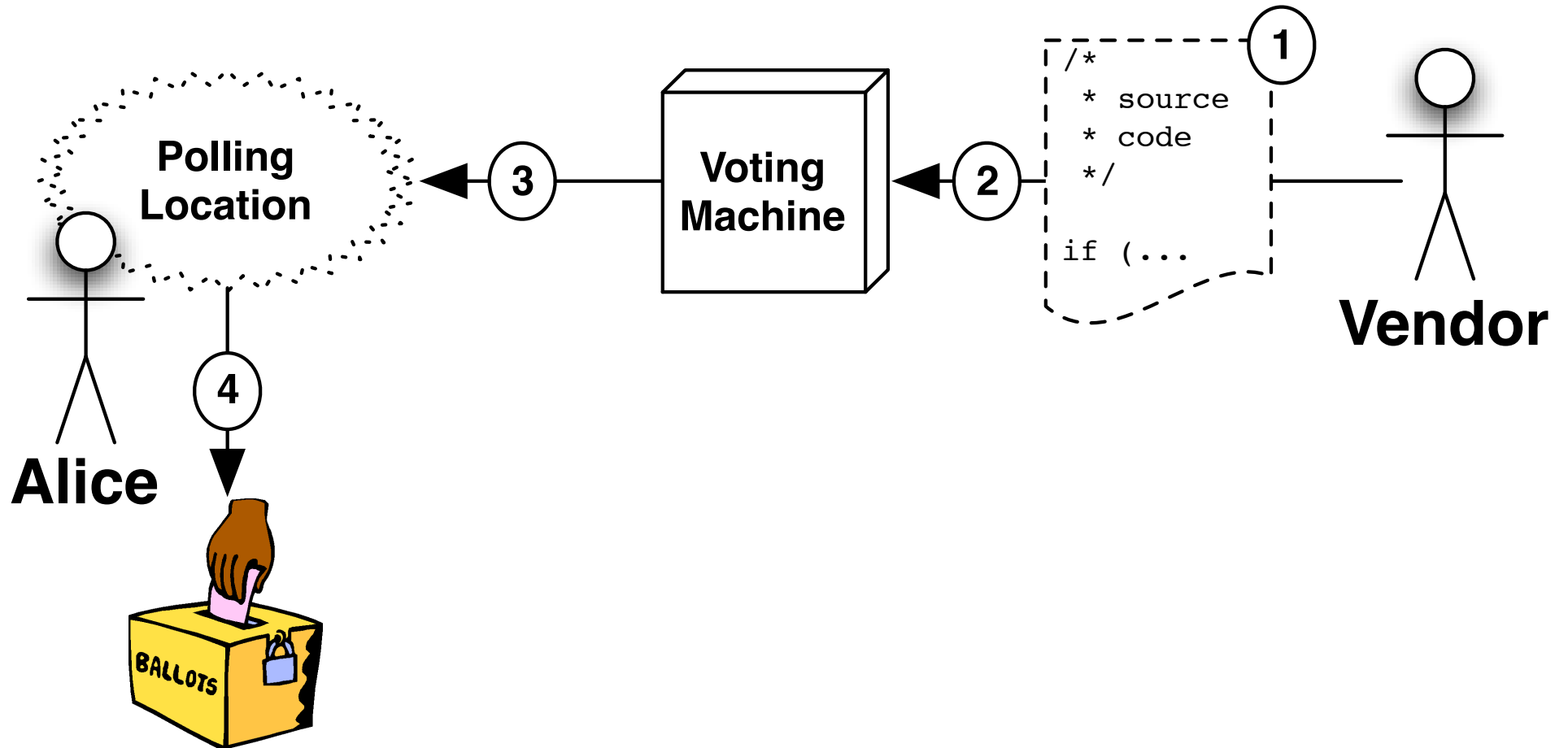
# Chain of Custody



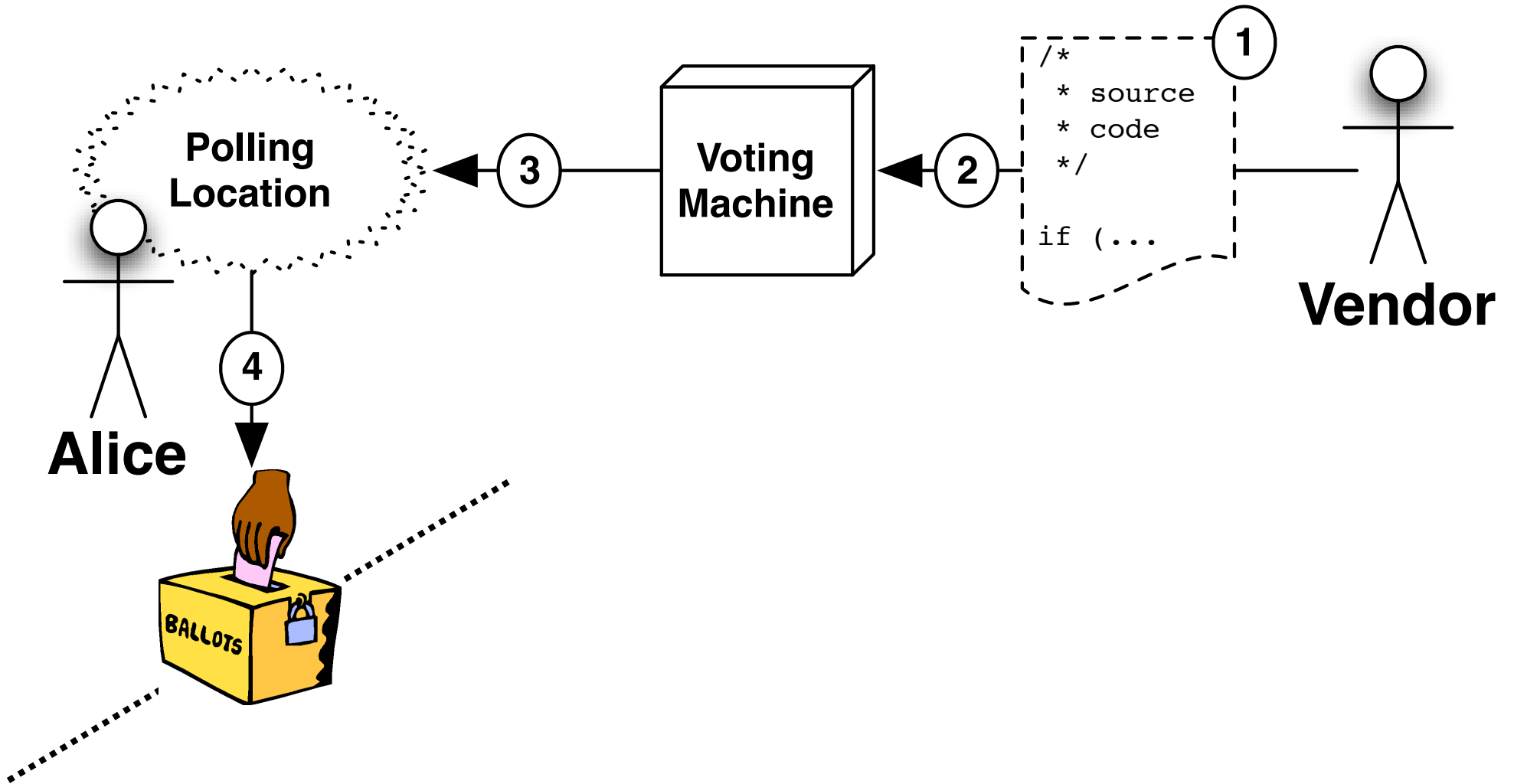
# Chain of Custody



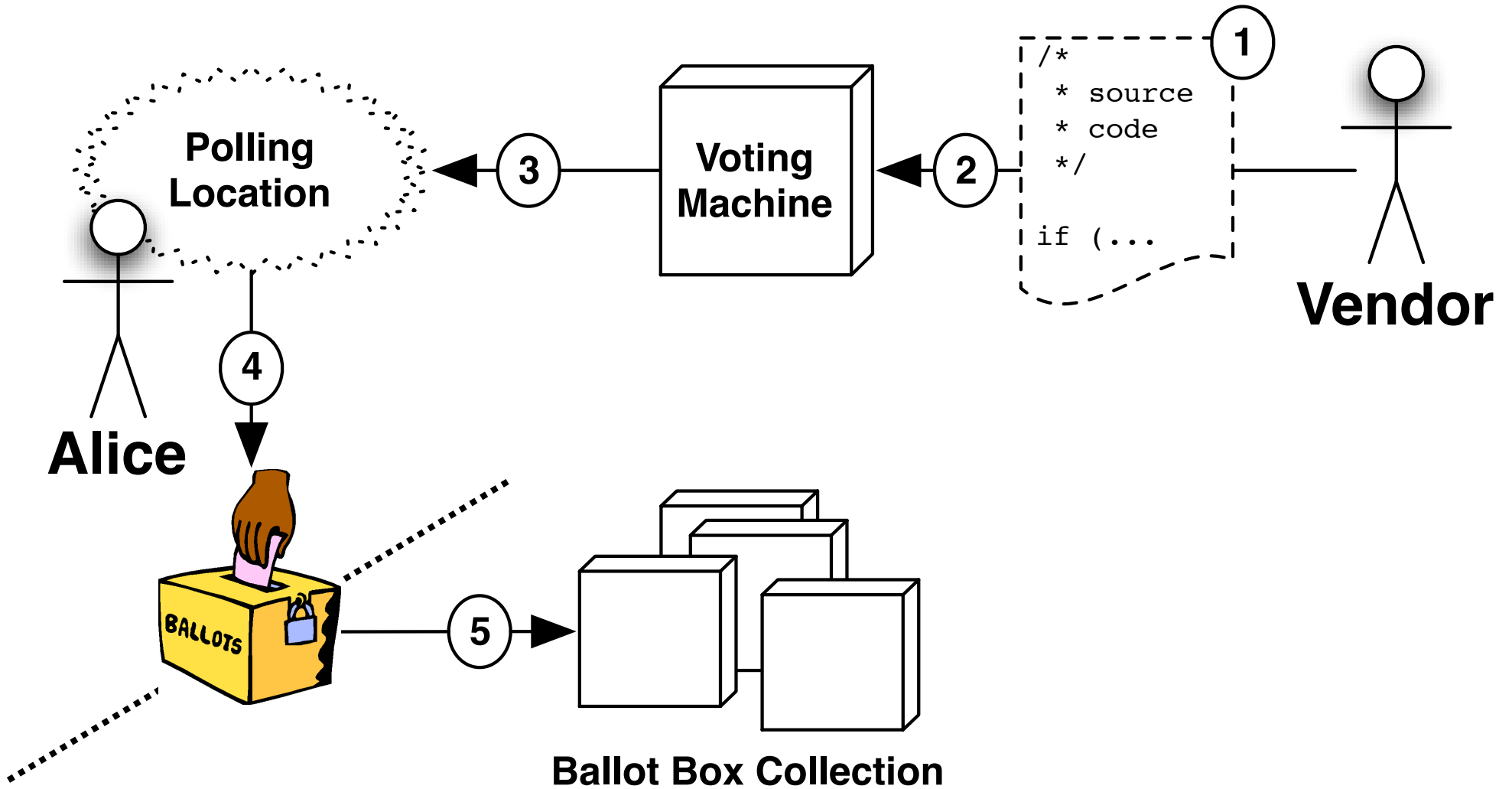
# Chain of Custody



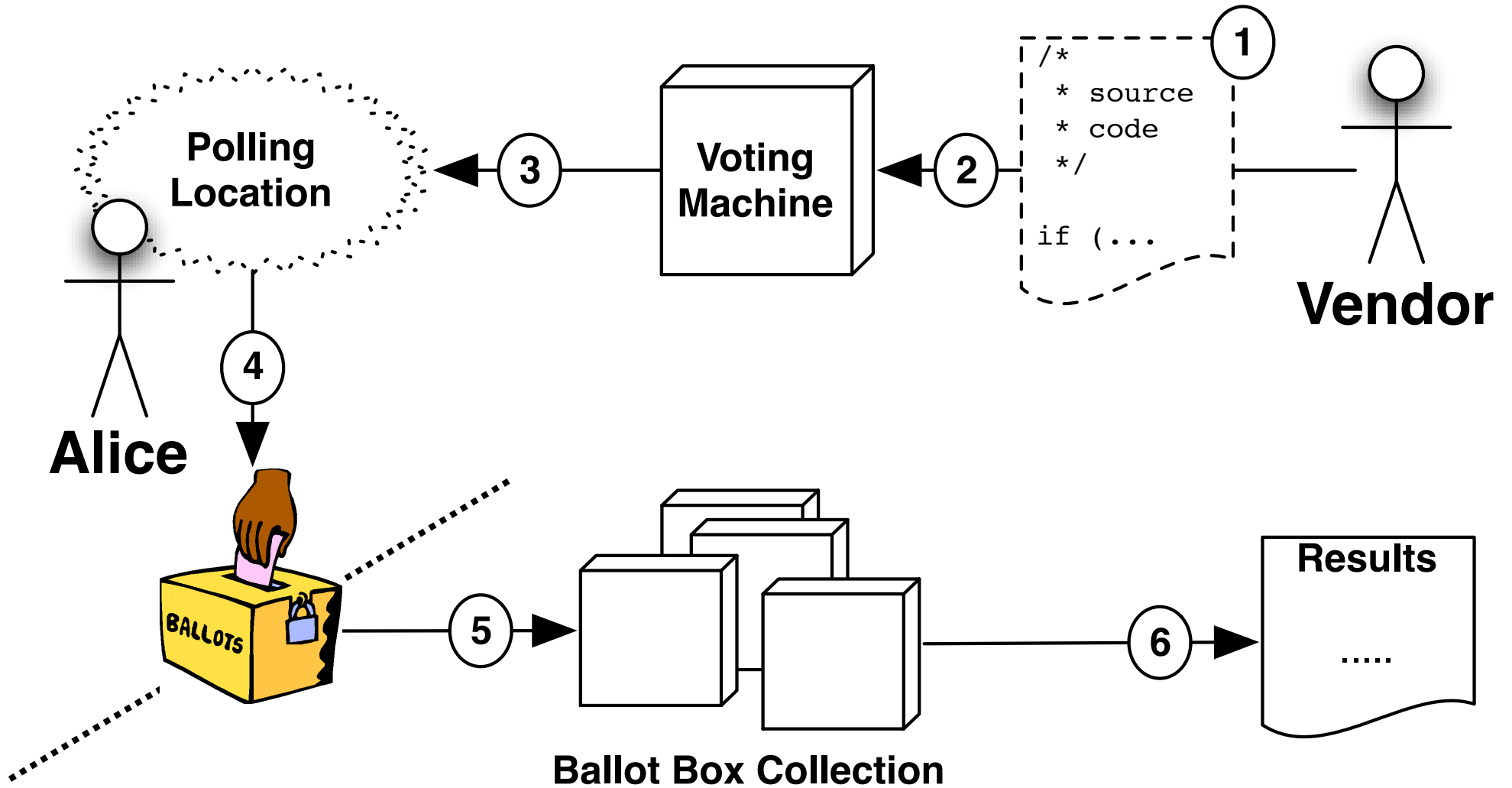
# Chain of Custody



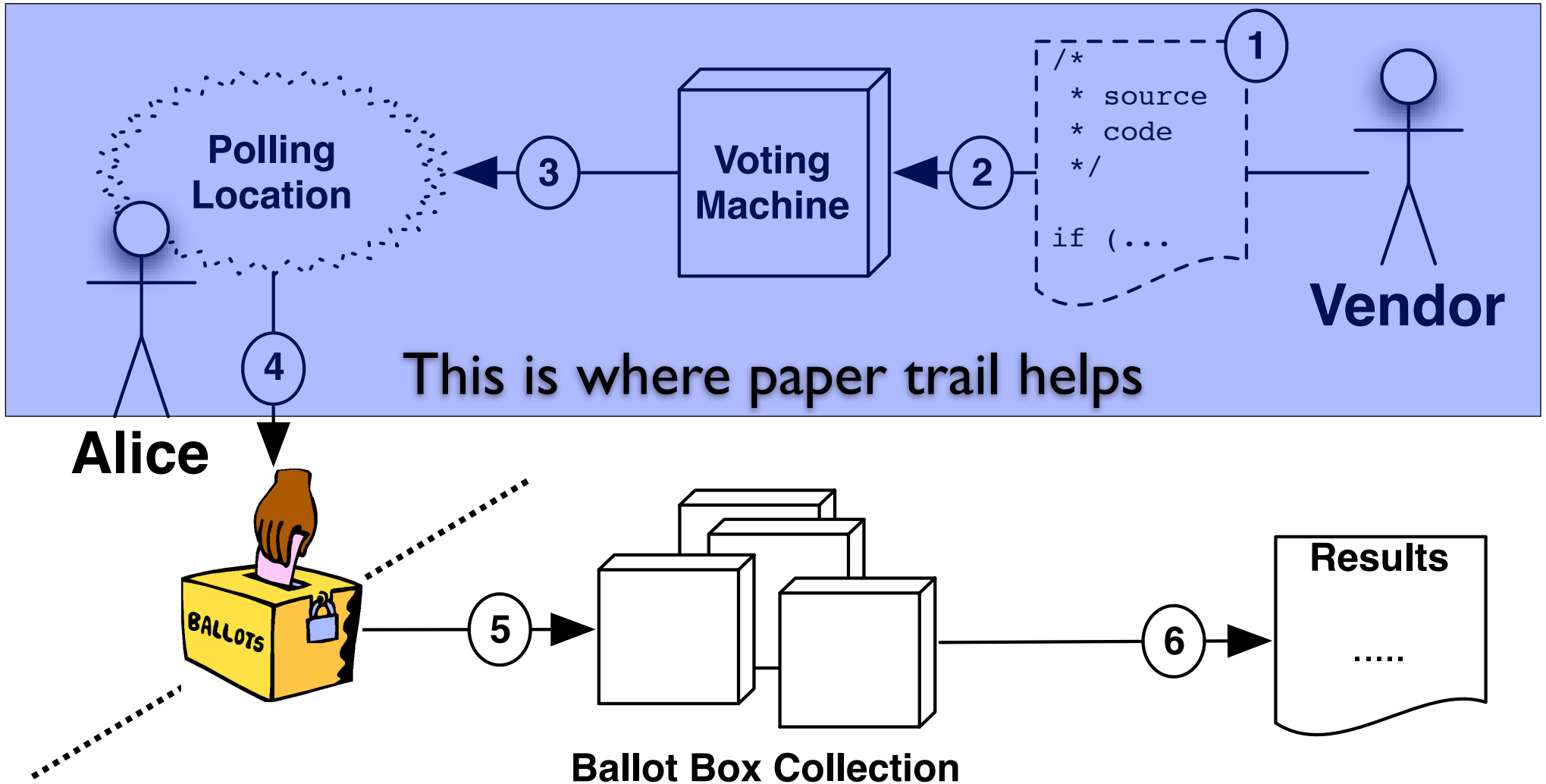
# Chain of Custody



# Chain of Custody

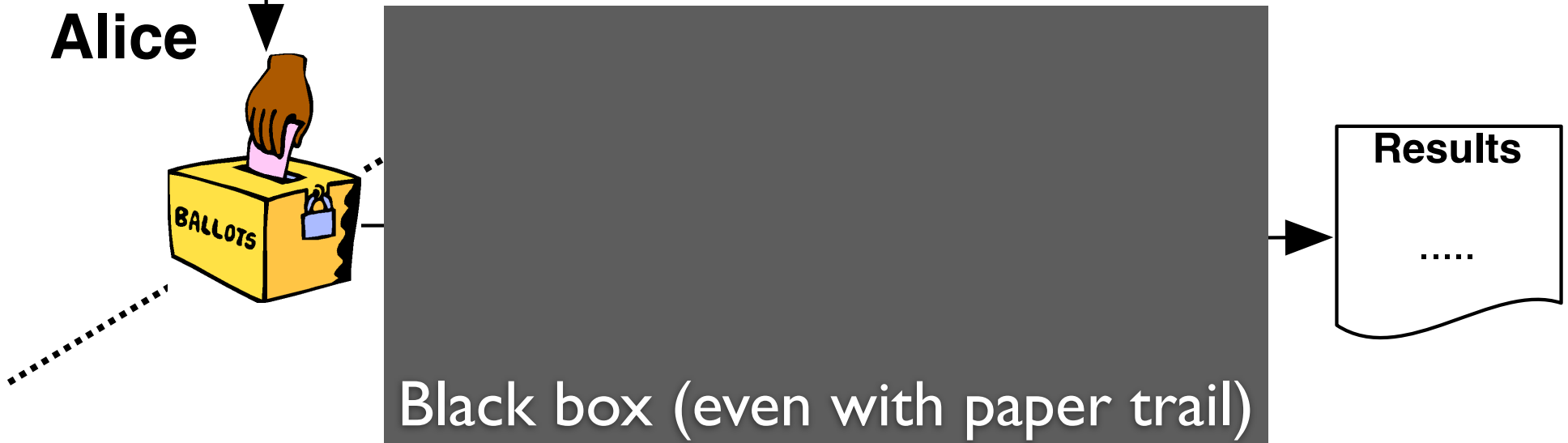
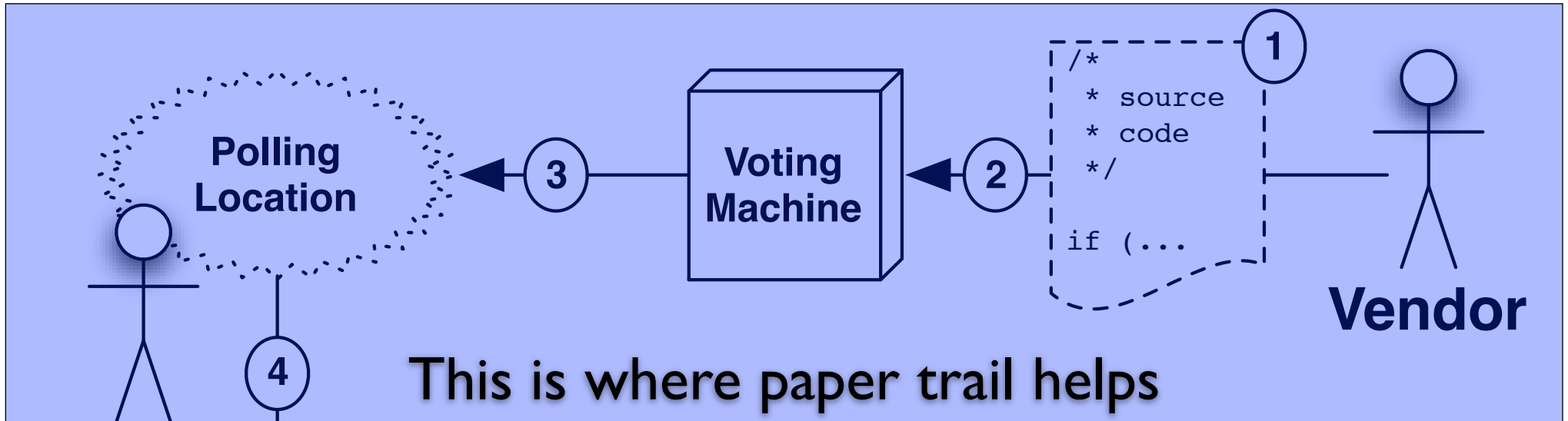


# Chain of Custody





# Chain of Custody



# Threat Model

# Threat Model

**Who is the attacker?**

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

# Threat Model

## **Who is the attacker?**

- administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

# Threat Model

## **Who is the attacker?**

- administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

## **How will the attacks be carried out?**



# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

## **How will the attacks be carried out?**

- ➔ corruption of input, ballot box, transport, tallying

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

## **How will the attacks be carried out?**

- ➔ corruption of input, ballot box, transport, tallying
- ➔ coercion of voters

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

## **How will the attacks be carried out?**

- ➔ corruption of input, ballot box, transport, tallying
- ➔ coercion of voters

## **Where will the attacks be hidden?**

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

## **How will the attacks be carried out?**

- ➔ corruption of input, ballot box, transport, tallying
- ➔ coercion of voters

## **Where will the attacks be hidden?**

- ➔ honest mistakes: randomly distributed in the process

# Threat Model

## **Who is the attacker?**

- ➔ administration officials, candidates, poll workers, even voters

## **What is the Benefit?**

## **How will the attacks be carried out?**

- ➔ corruption of input, ballot box, transport, tallying
- ➔ coercion of voters

## **Where will the attacks be hidden?**

- ➔ honest mistakes: randomly distributed in the process
- ➔ malicious intent: hiding where you least defend

**So what can we do?**

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 local bar.

# Open audit elections

Cryptography provides more than confidentiality.

Cryptography can provide both **verifiability** *and* **ballot secrecy**

Anyone can audit!

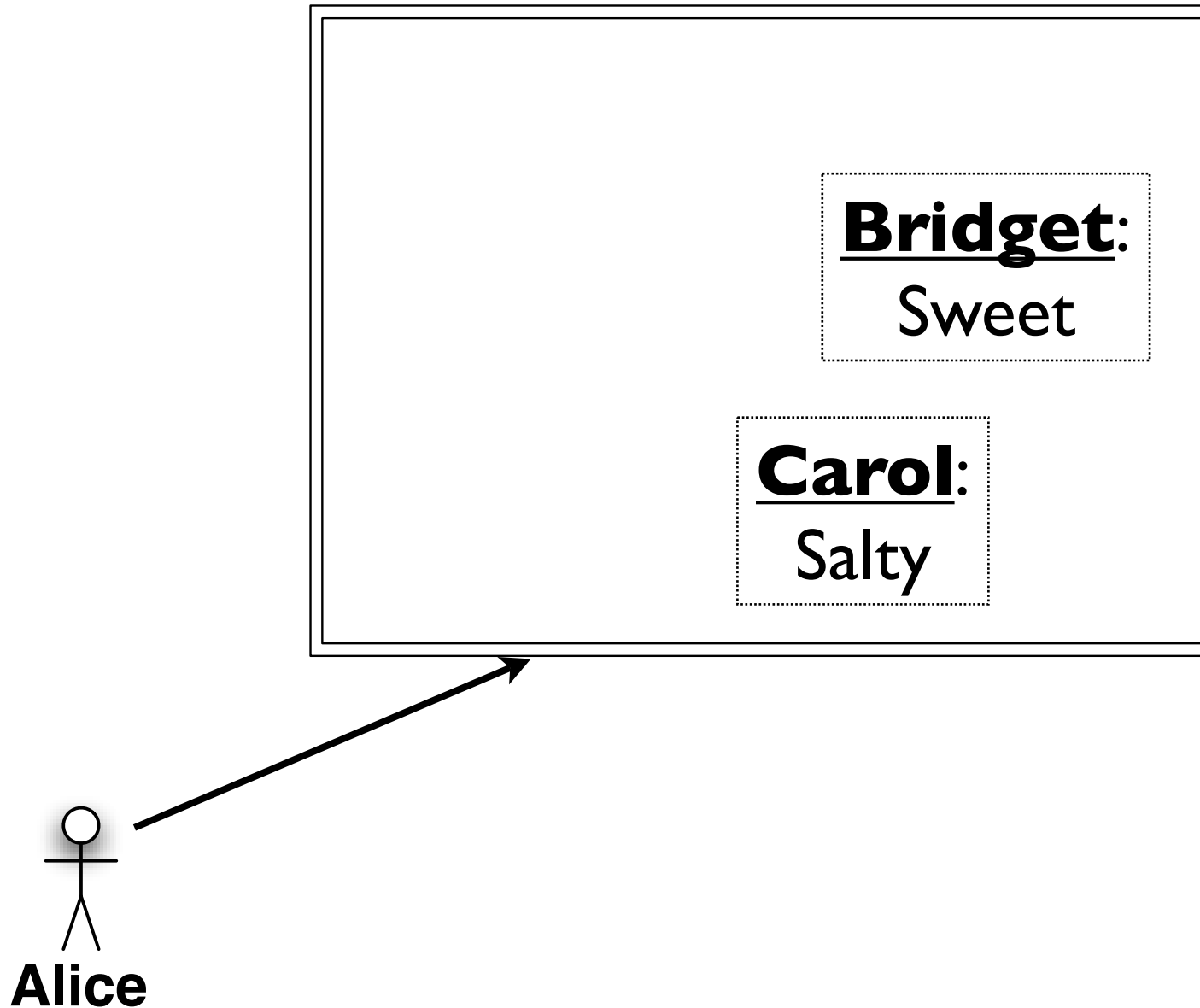


# Public Ballots

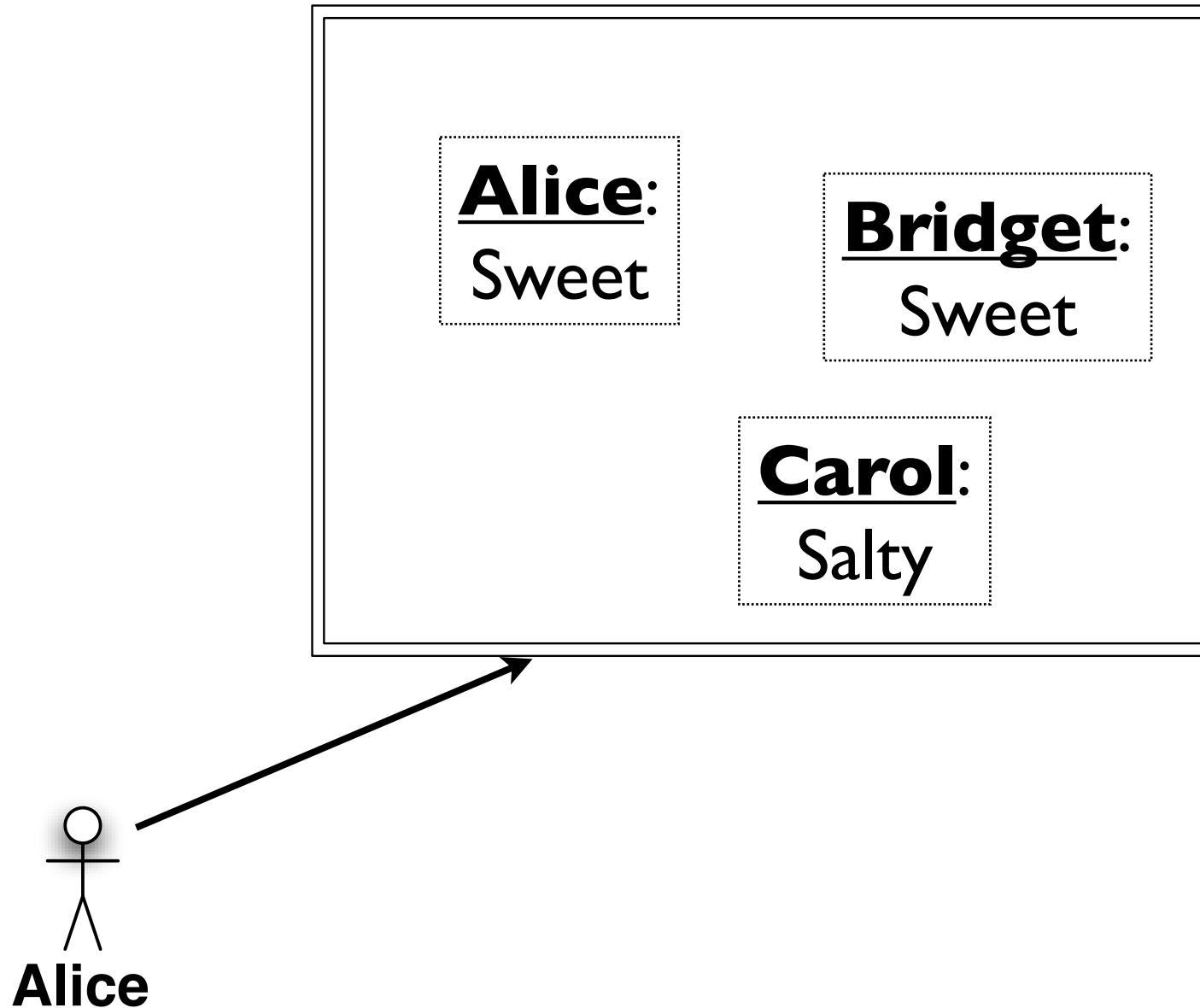
**Bridget:**  
Sweet

**Carol:**  
Salty

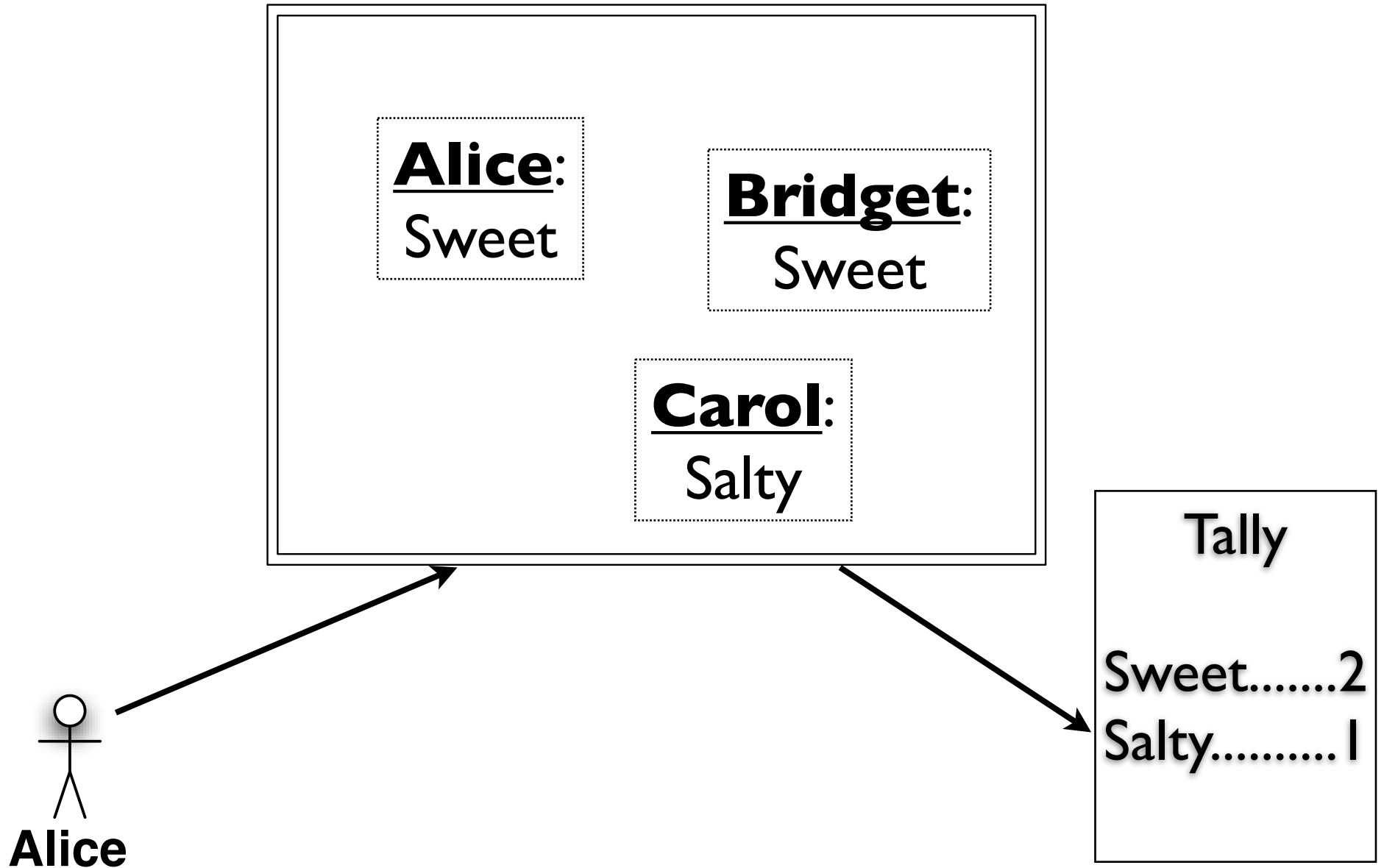
# Public Ballots



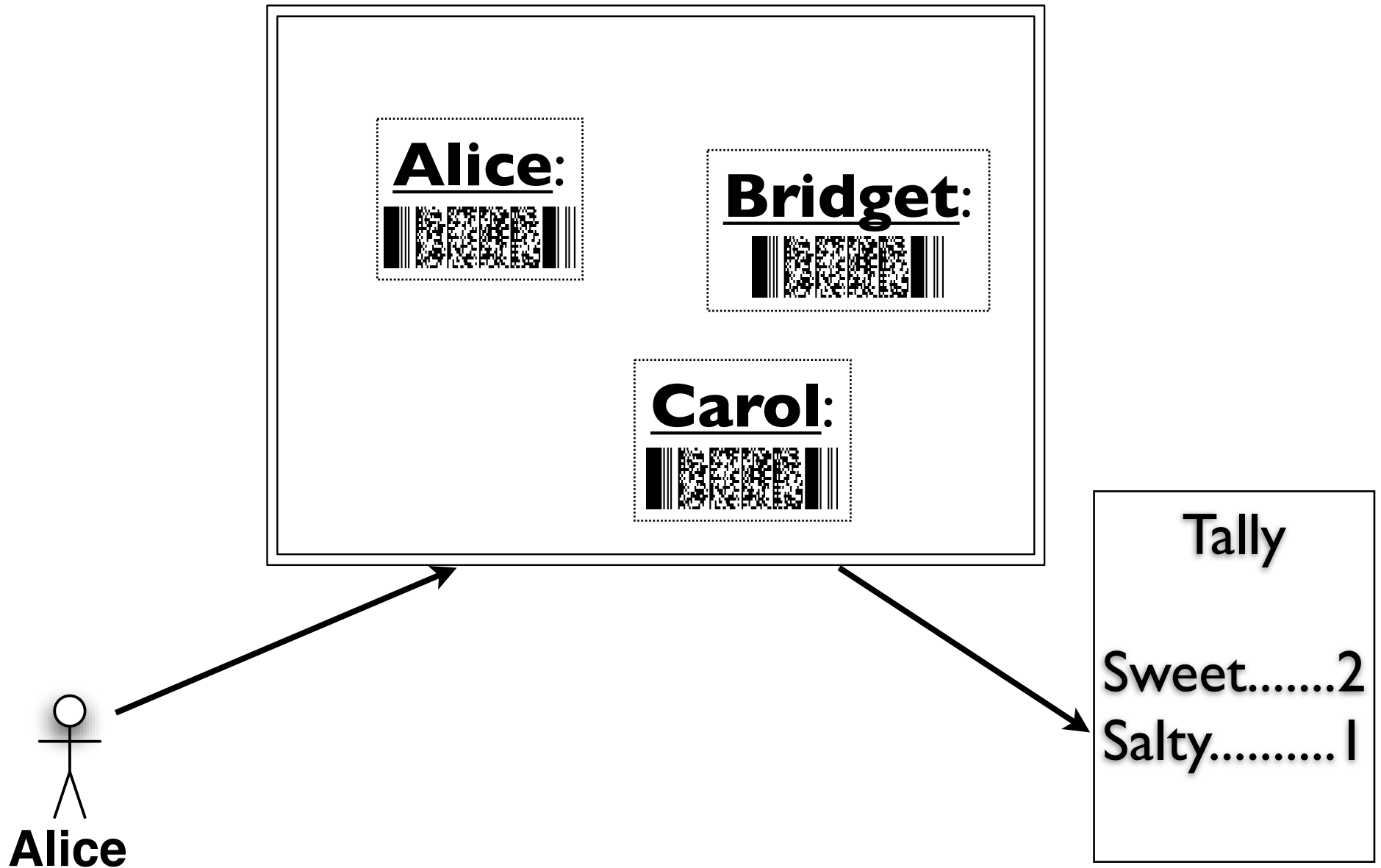
# Public Ballots



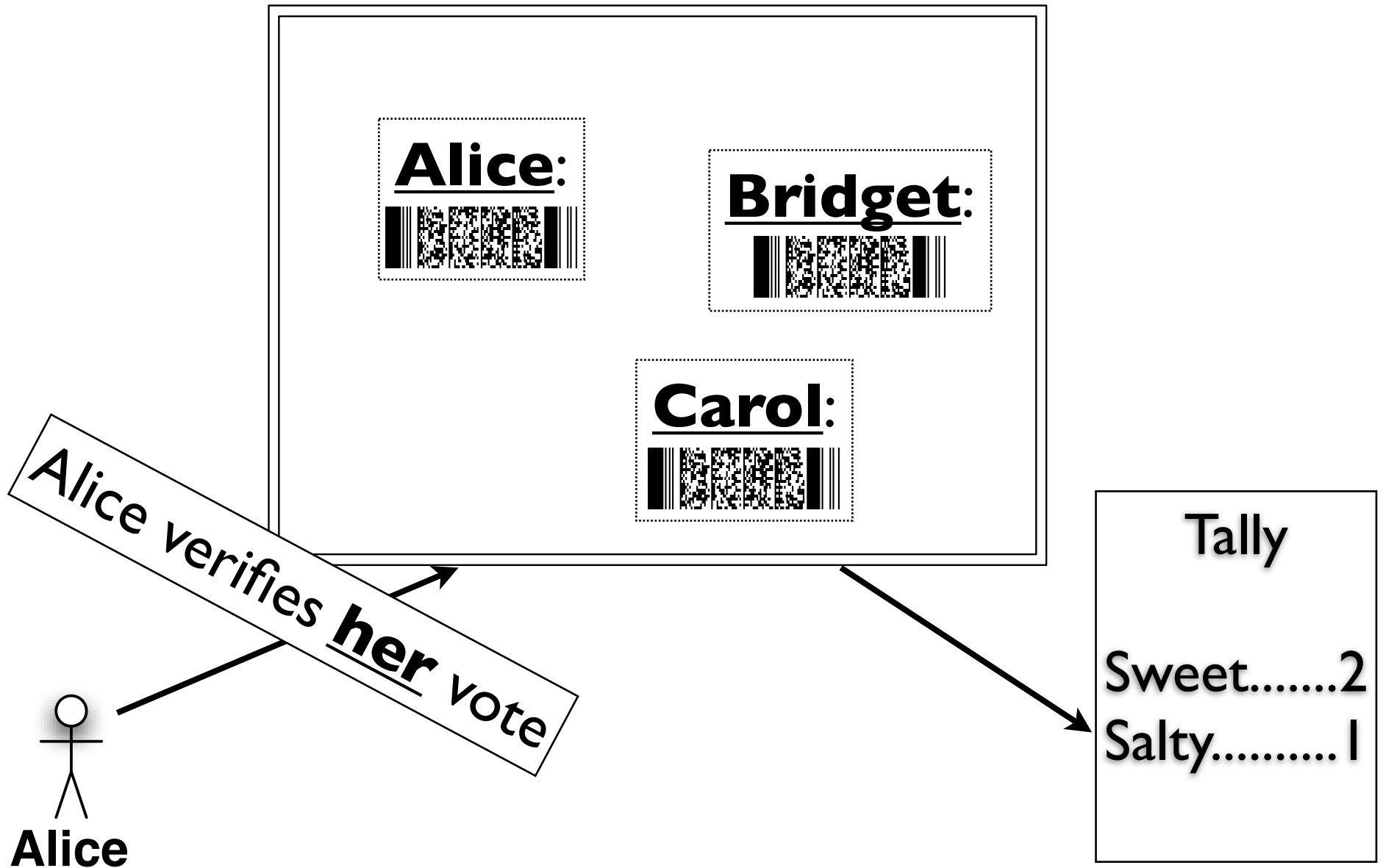
# Public Ballots



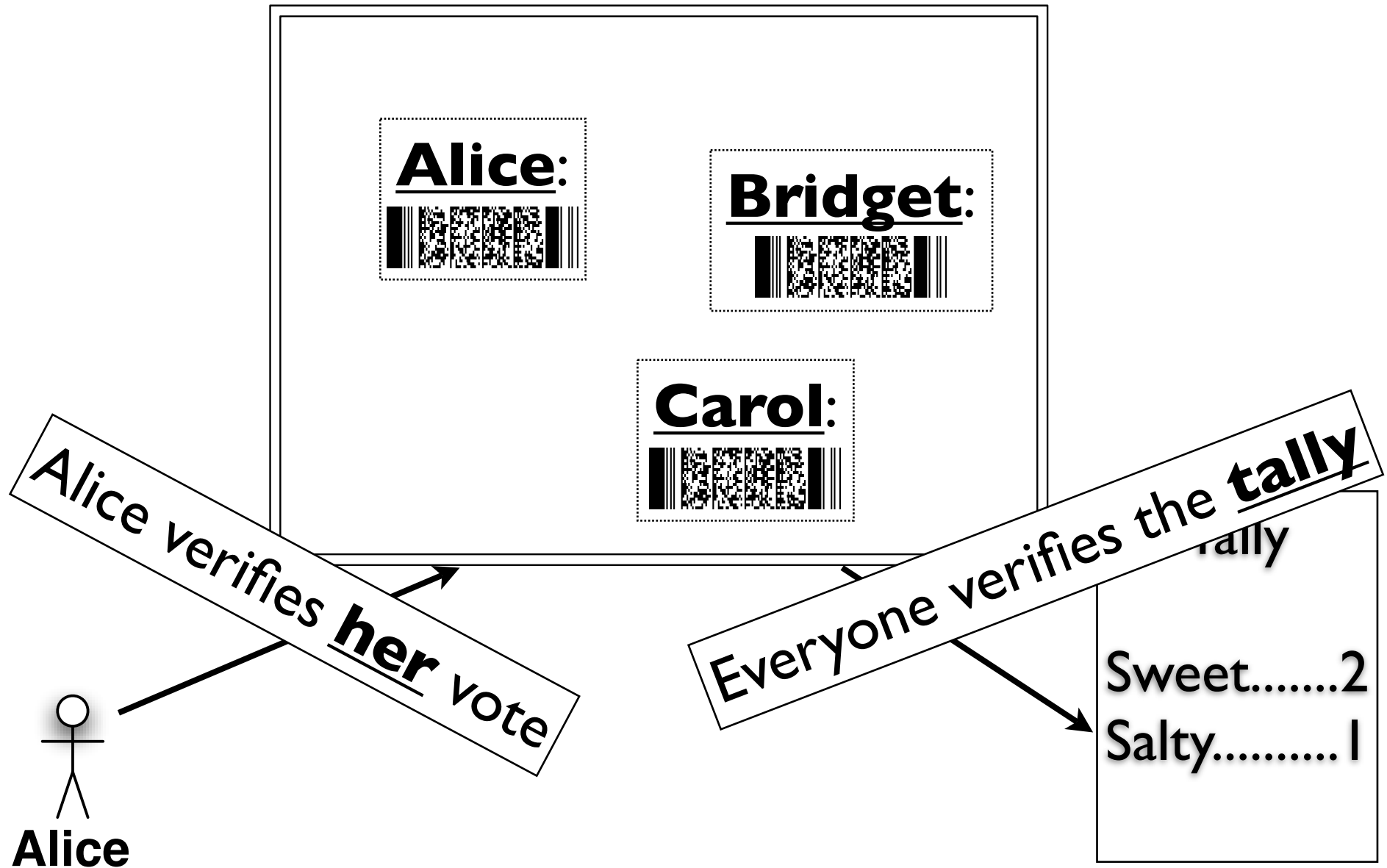
# Encrypted Public Ballots



# Encrypted Public Ballots



# Encrypted Public Ballots



# Public-Key Encryption



# Public-Key Encryption

Keypair consists of a public key  $pk$  and a secret key  $sk$ .

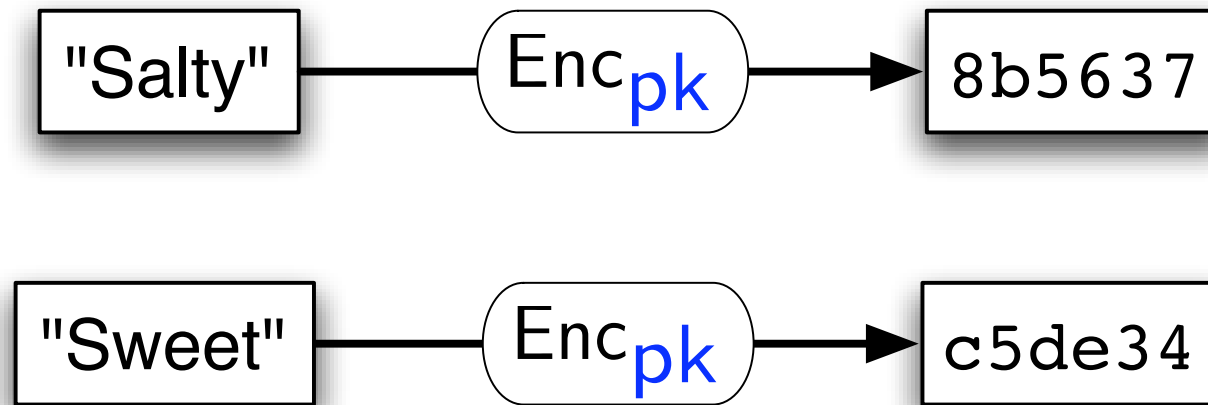
# Public-Key Encryption

Keypair consists of a public key  $pk$  and a secret key  $sk$ .



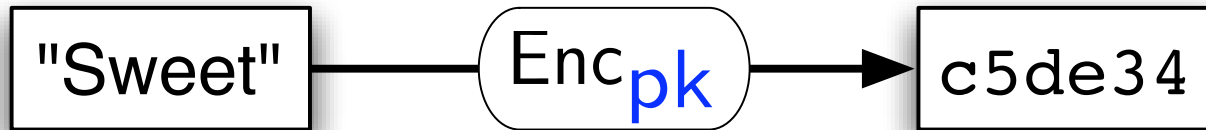
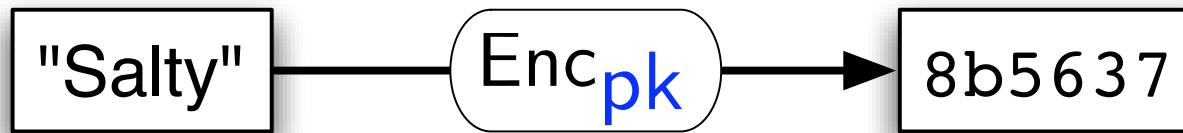
# Public-Key Encryption

Keypair consists of a public key  $pk$  and a secret key  $sk$ .



# Public-Key Encryption

Keypair consists of a public key  $pk$  and a secret key  $sk$ .



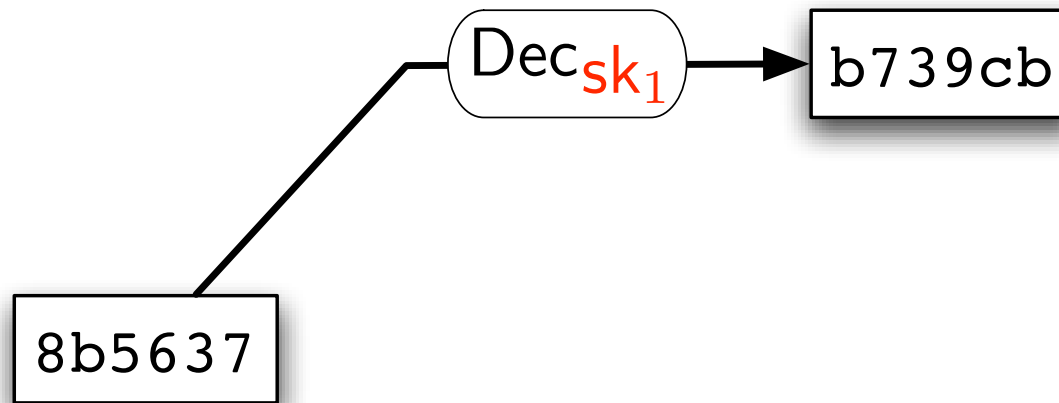
# Threshold Decryption

Secret key is shared amongst multiple parties:  
all (or at least a quorum) need to cooperate to decrypt.

8b5637

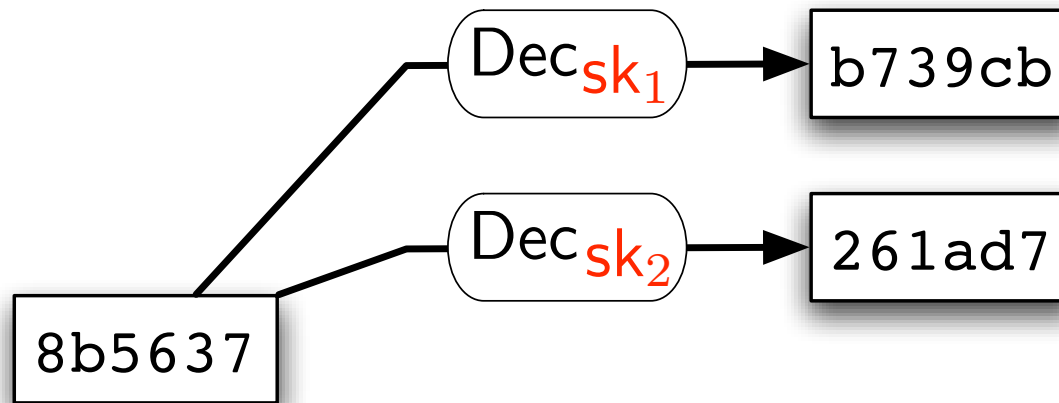
# Threshold Decryption

Secret key is shared amongst multiple parties:  
all (or at least a quorum) need to cooperate to decrypt.



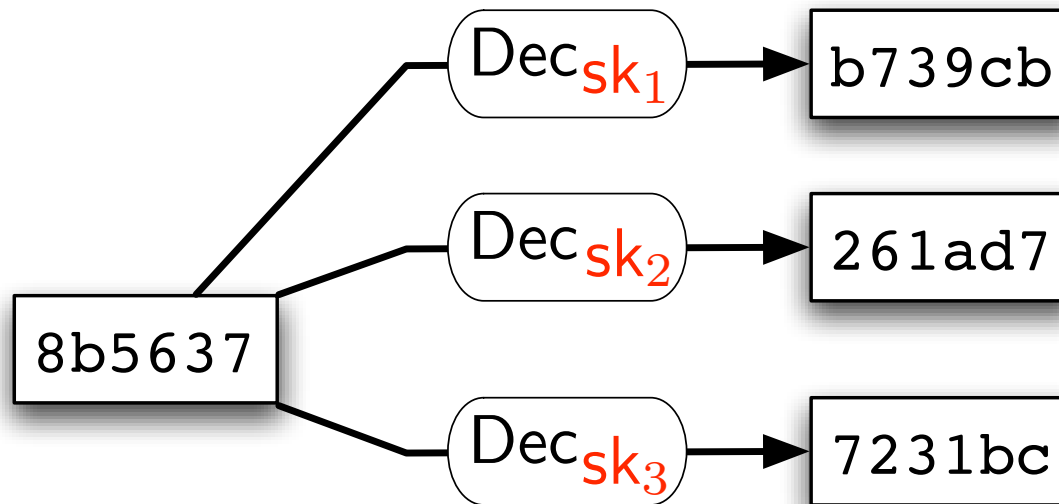
# Threshold Decryption

Secret key is shared amongst multiple parties:  
all (or at least a quorum) need to cooperate to decrypt.



# Threshold Decryption

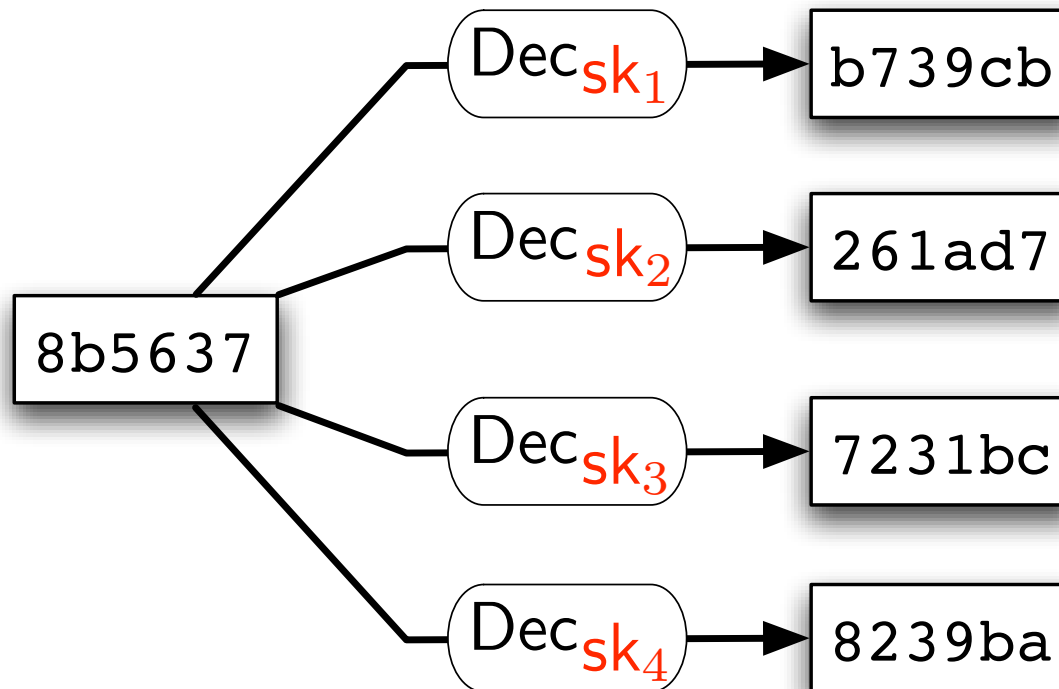
Secret key is shared amongst multiple parties:  
all (or at least a quorum) need to cooperate to decrypt.





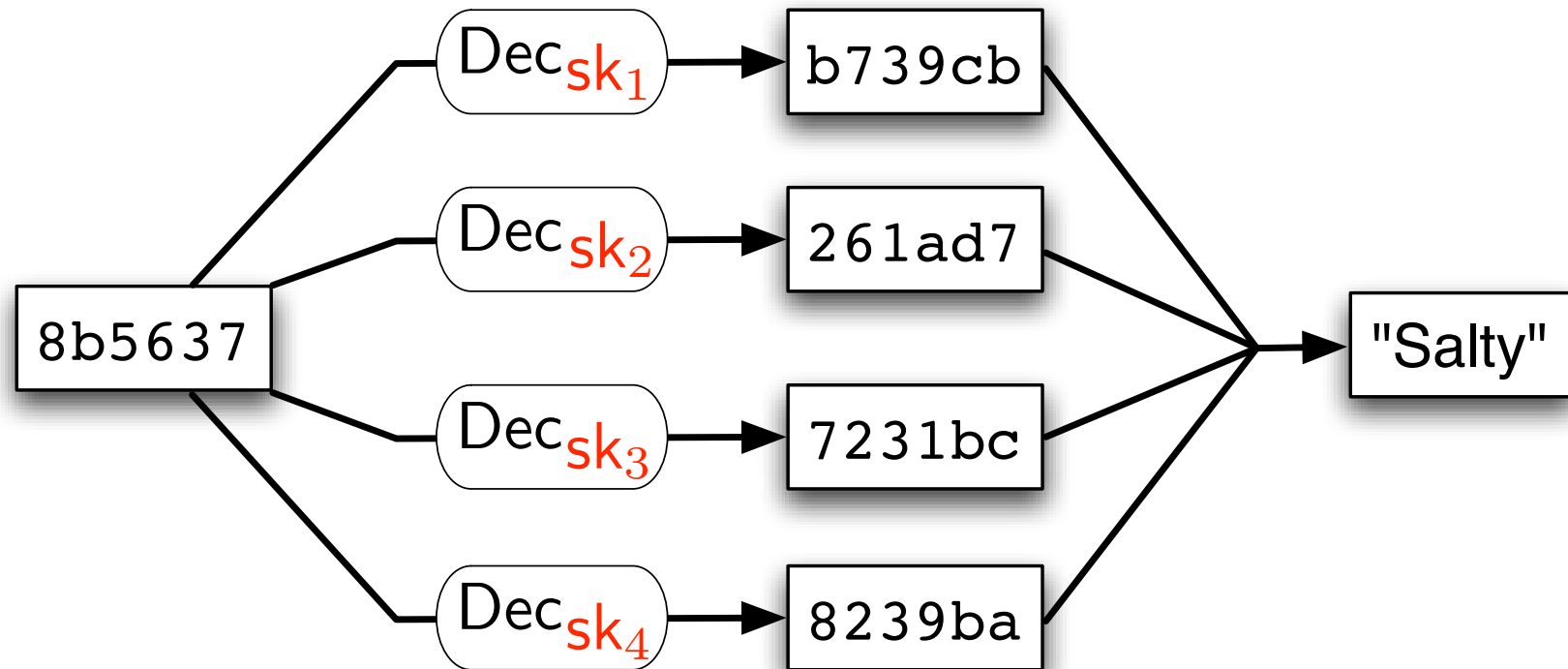
# Threshold Decryption

Secret key is shared amongst multiple parties:  
all (or at least a quorum) need to cooperate to decrypt.



# Threshold Decryption

Secret key is shared amongst multiple parties:  
all (or at least a quorum) need to cooperate to decrypt.



# Tallying Method I: Homomorphic Tabulation [Benaloh'87]

$$\begin{aligned} \text{Enc}(m_1) \times \text{Enc}(m_2) \\ = \text{Enc}(m_1 + m_2) \end{aligned}$$

# Tallying Method I: Homomorphic Tabulation [Benaloh'87]

$$\text{Enc}(m_1) \times \text{Enc}(m_2) \\ = \text{Enc}(m_1 + m_2)$$

$$\text{Yes} = \text{Enc}(1)$$

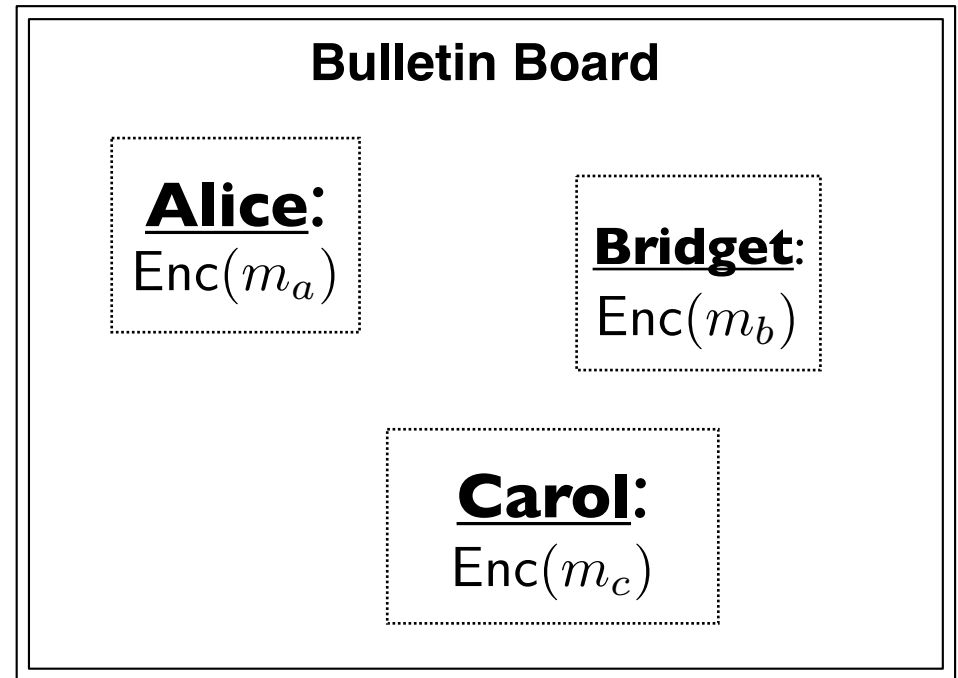
$$\text{No} = \text{Enc}(0)$$

# Tallying Method I: Homomorphic Tabulation [Benaloh'87]

$$\text{Enc}(m_1) \times \text{Enc}(m_2) \\ = \text{Enc}(m_1 + m_2)$$

$$\text{Yes} = \text{Enc}(1)$$

$$\text{No} = \text{Enc}(0)$$

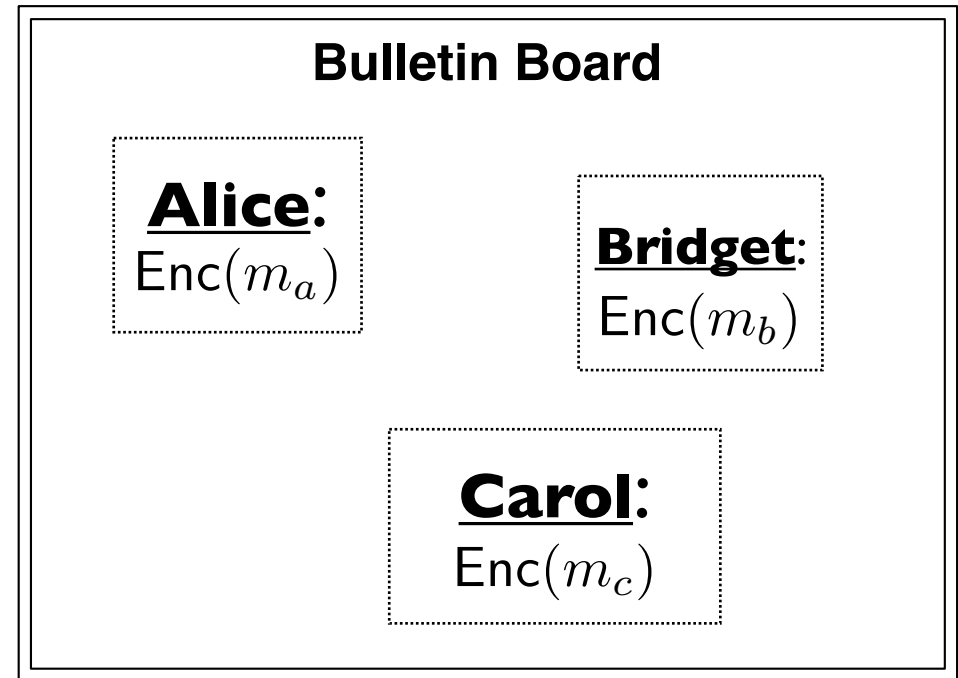


# Tallying Method I: Homomorphic Tabulation [Benaloh'87]

$$\text{Enc}(m_1) \times \text{Enc}(m_2) \\ = \text{Enc}(m_1 + m_2)$$

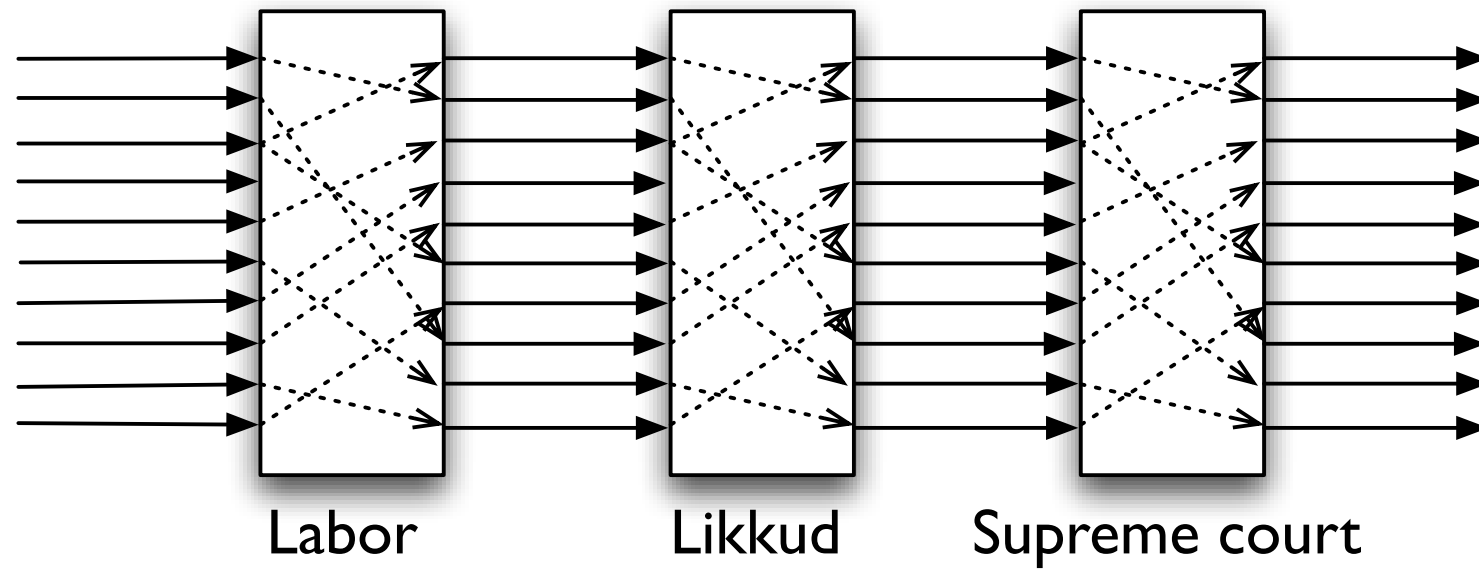
$$\text{Yes} = \text{Enc}(1)$$

$$\text{No} = \text{Enc}(0)$$

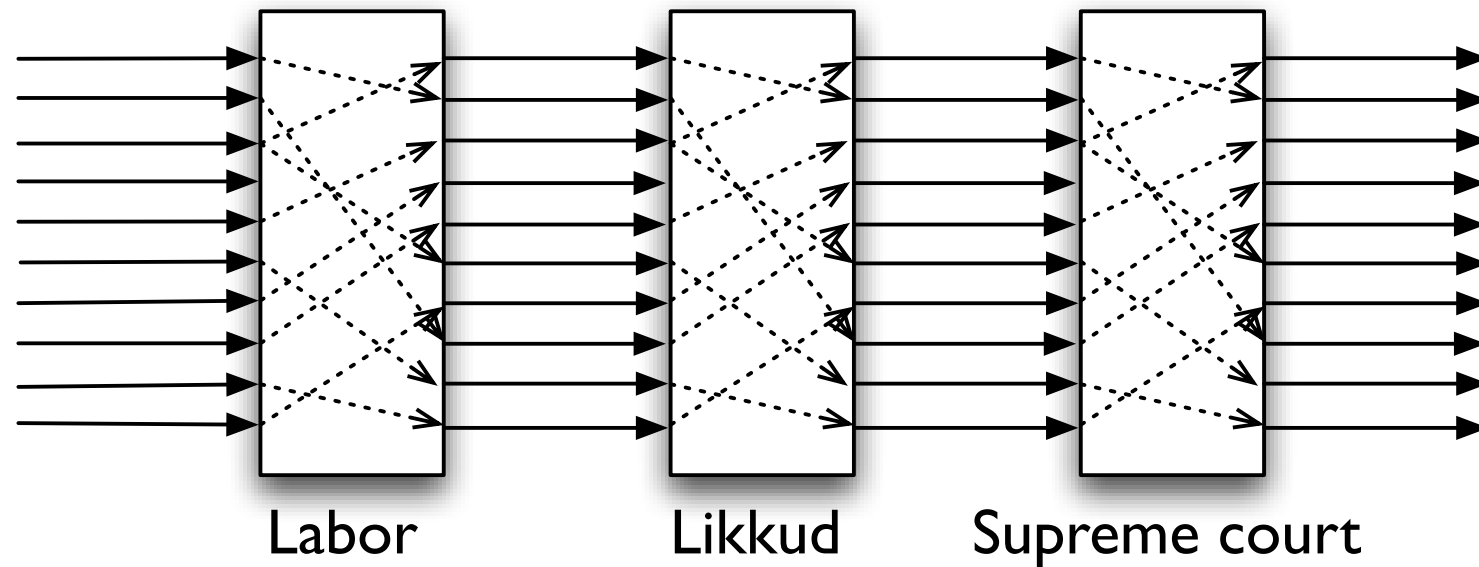


$$\text{Encrypted Tally} = \text{Enc}(m_a) \times \text{Enc}(m_b) \times \text{Enc}(m_c) \\ = \text{Enc}(m_a + m_b + m_c)$$

# Tallying Method II: Mixnet [Chaum'81]



# Tallying Method II: Mixnet [Chaum'81]



Each mix server shuffles  
the encrypted votes.



How can we verify  
operations on  
encrypted data?

# Verifying Validity of Encryption/Mixing

Given  $\text{Enc}(m)$  How can I verify:

1. that it is not an encryption of more than one vote?
2. that the encryption of my vote wasn't "dropped"?

**Zero-Knowledge proofs:** Can prove validity of  $\text{Enc}(m)$  without revealing anything else!

**The crucial point:** only need to verify that machine is computing right functionality...

# Verifying Validity of Encryption/Mixing

Given  $\text{Enc}(m)$  How can I verify:

1. that it is not an encryption of more than one vote?
2. that the encryption of my vote wasn't "dropped"?

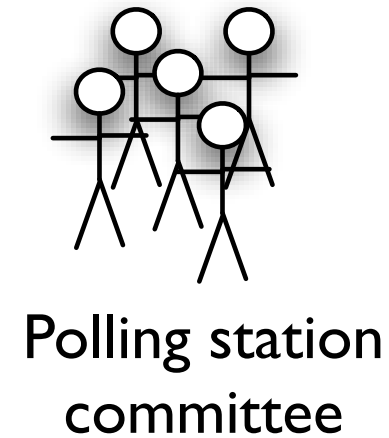
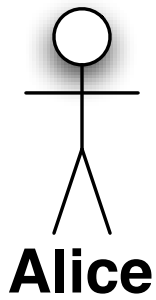
**Zero-Knowledge proofs:** Can prove validity of  $\text{Enc}(m)$  without revealing anything else!

**The crucial point:** only need to verify that machine is computing right functionality...

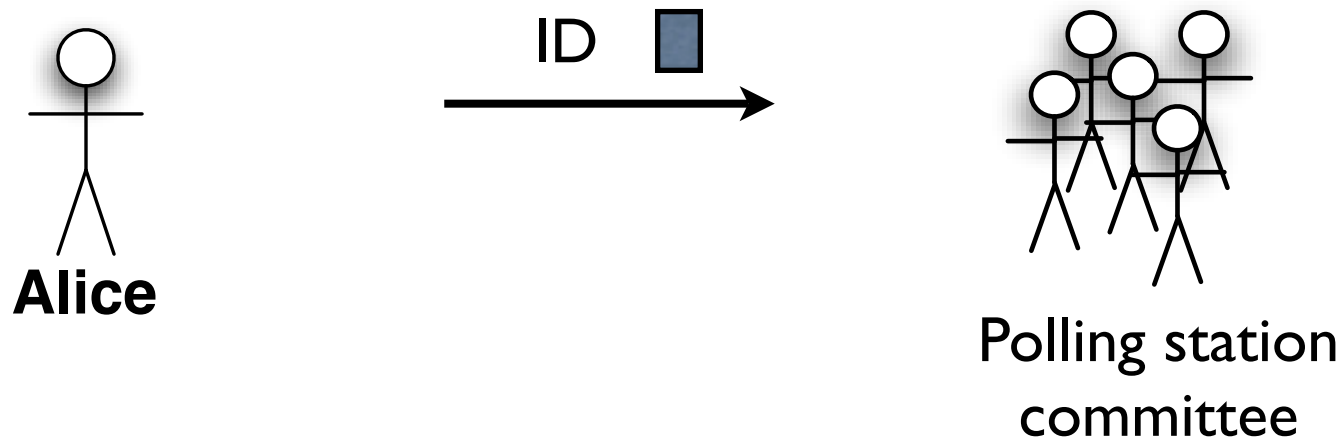
# Voting Process Example

[Chaum'81, Sako-Kilian'95, Neff'04,  
Chaum'04, etc...]

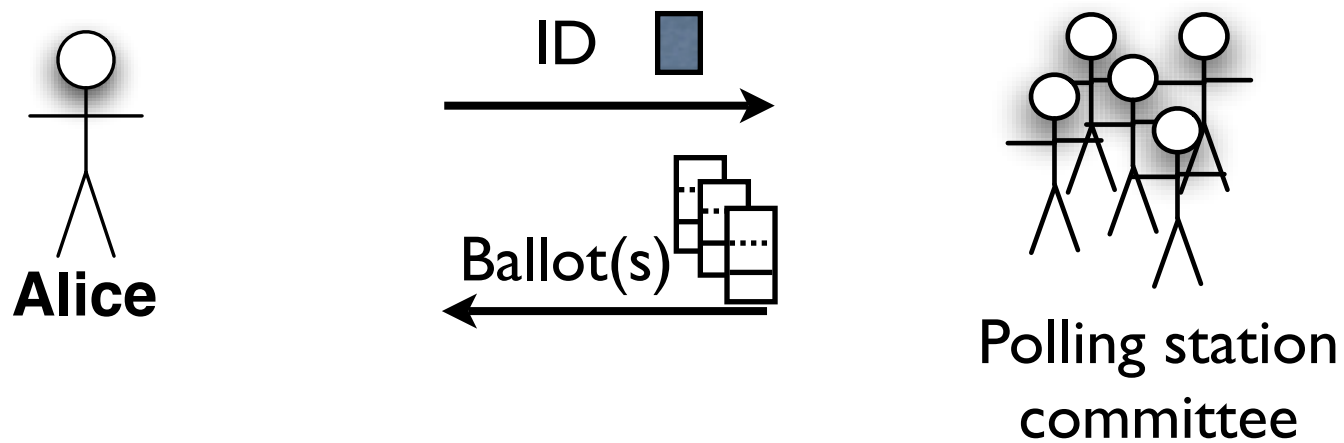
# Identification



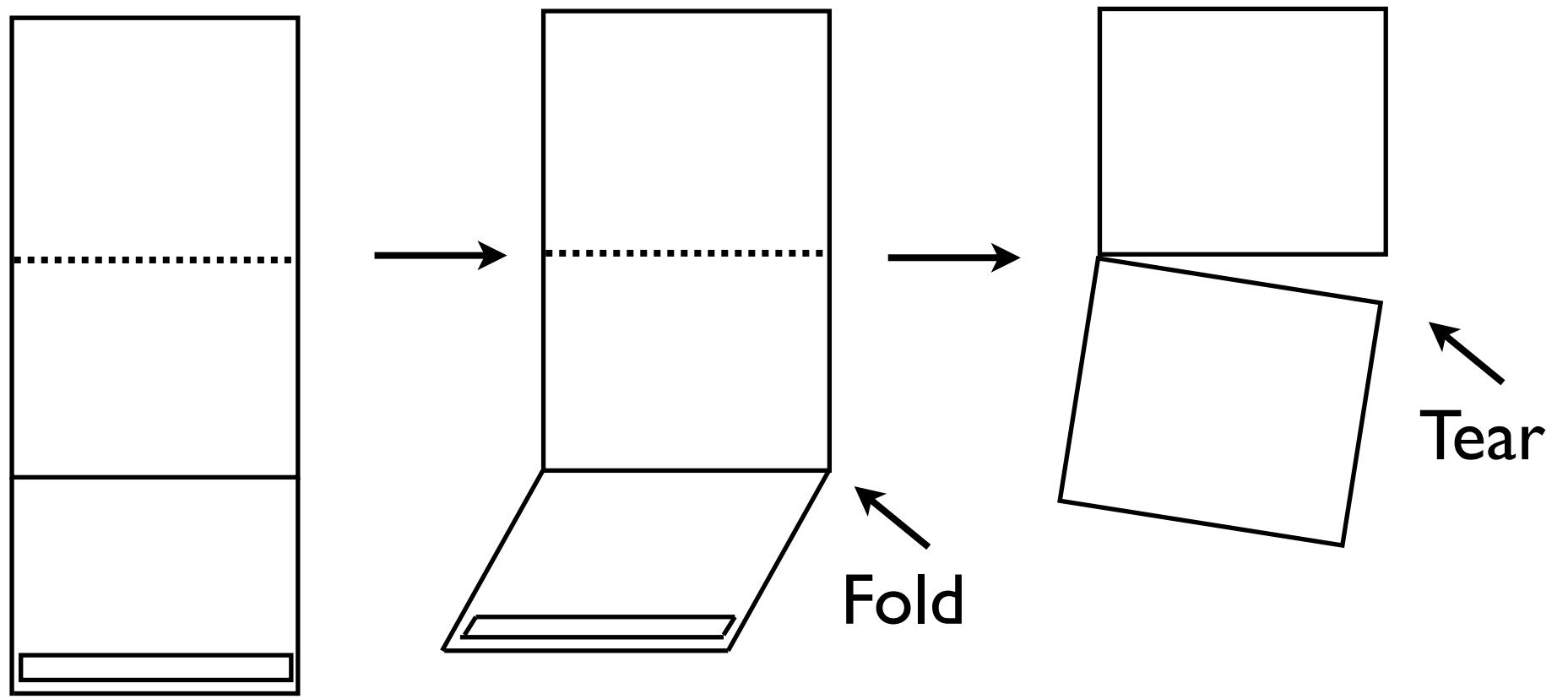
# Identification



# Identification

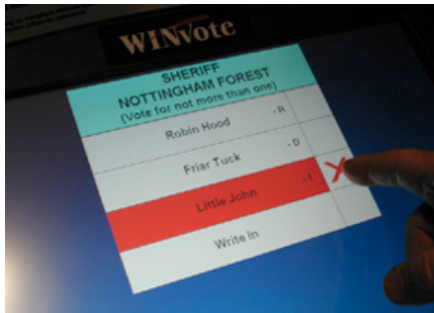


# The Ballot

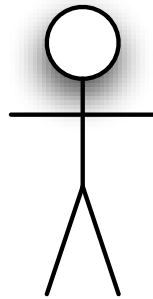




# Producing Encrypted Ballot

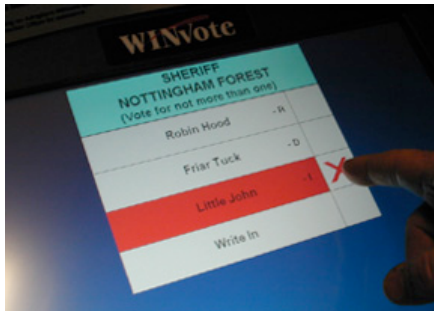


+

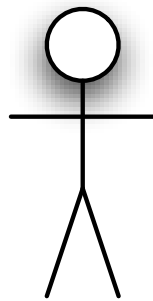


**Alice**

# Producing Encrypted Ballot

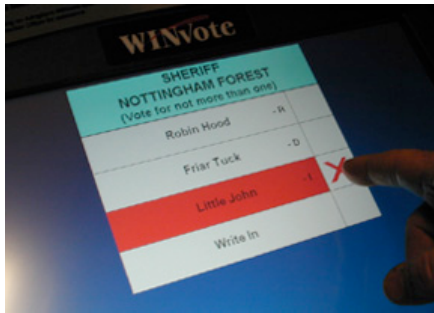


+

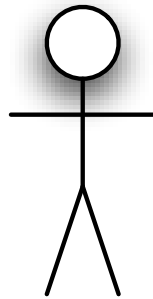


**Alice**

# Producing Encrypted Ballot

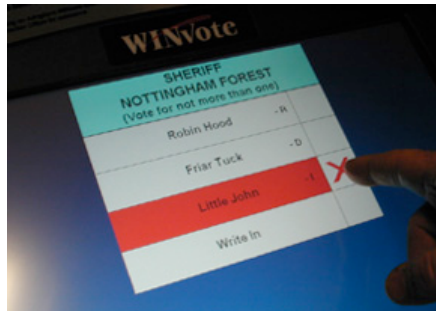


+



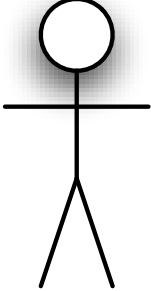
**Alice**

# Producing Encrypted Ballot

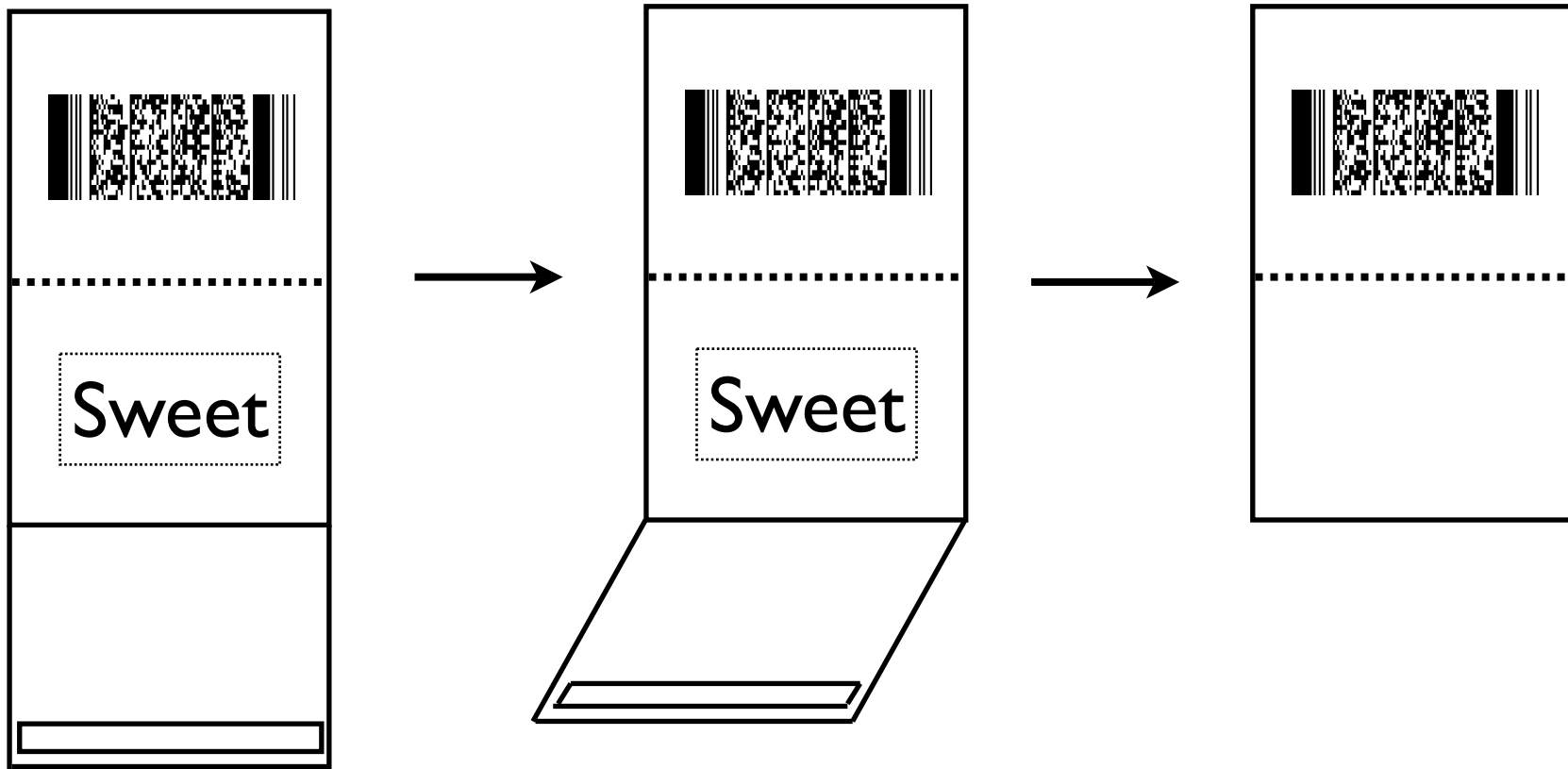


+

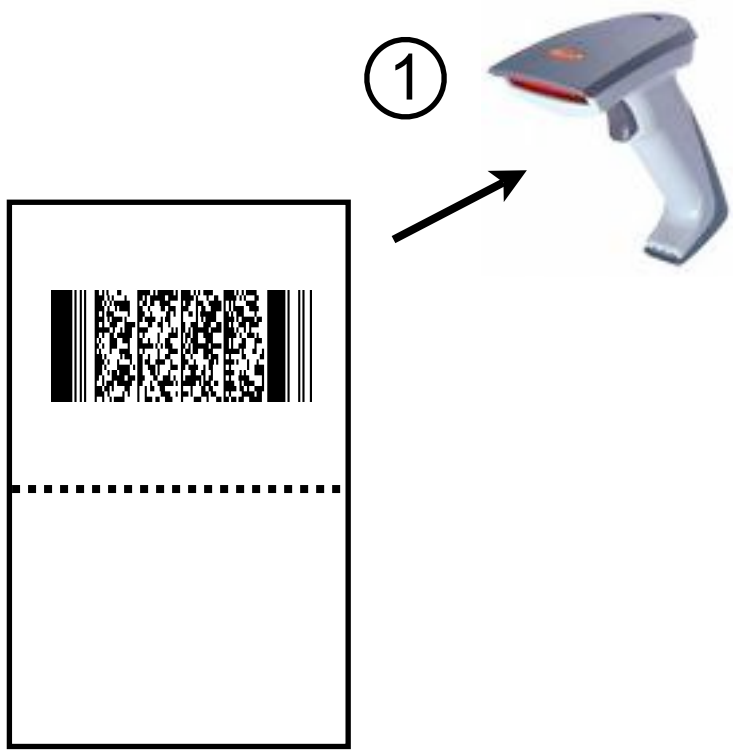


  
**Alice**

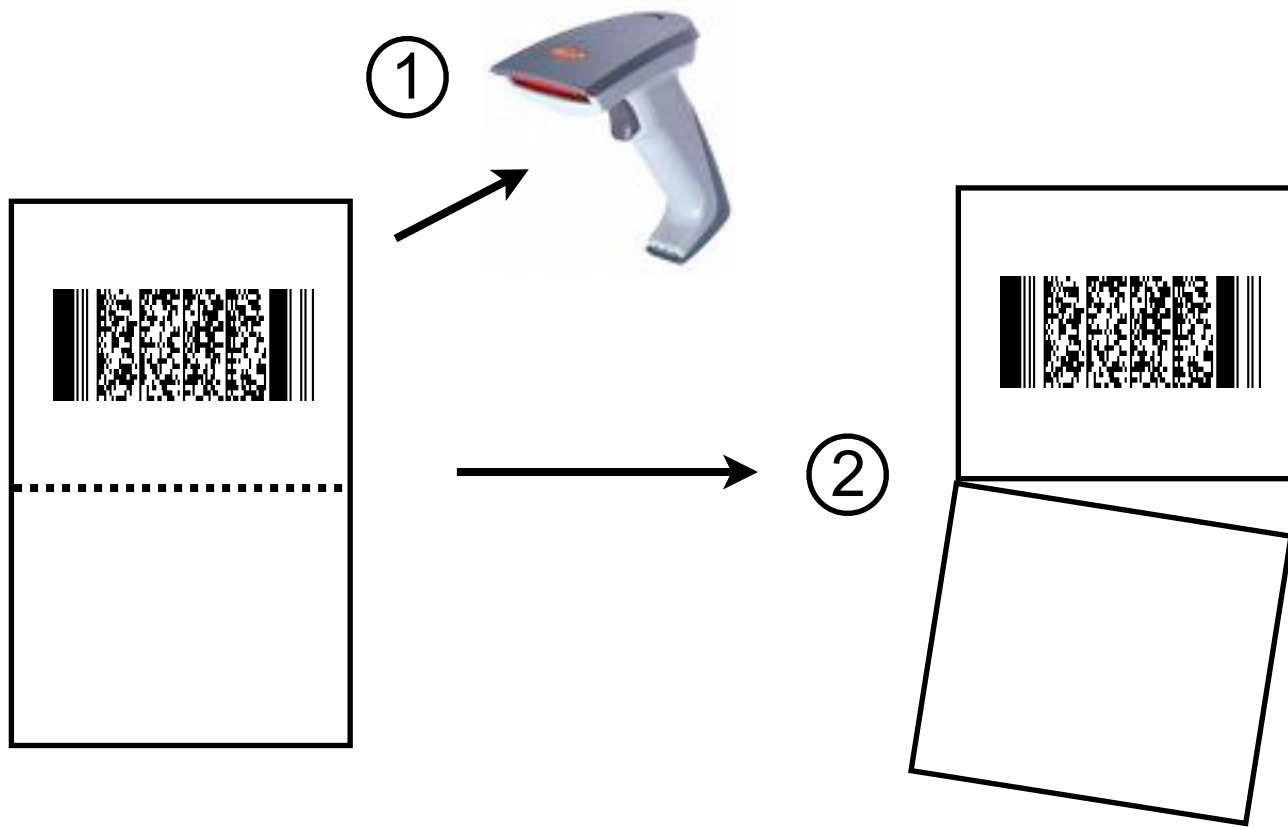
# Encrypted Ballot



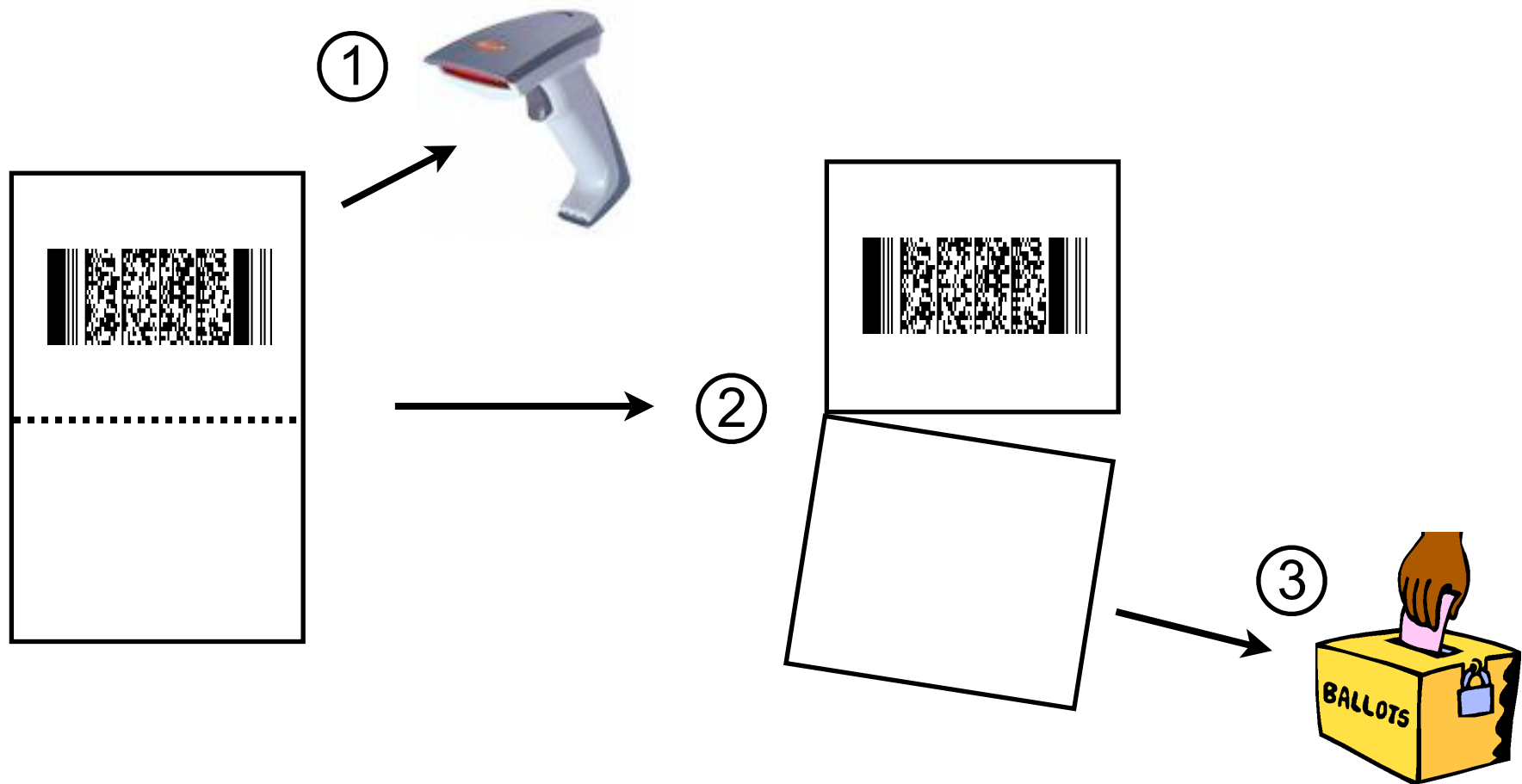
# Ballot Casting



# Ballot Casting

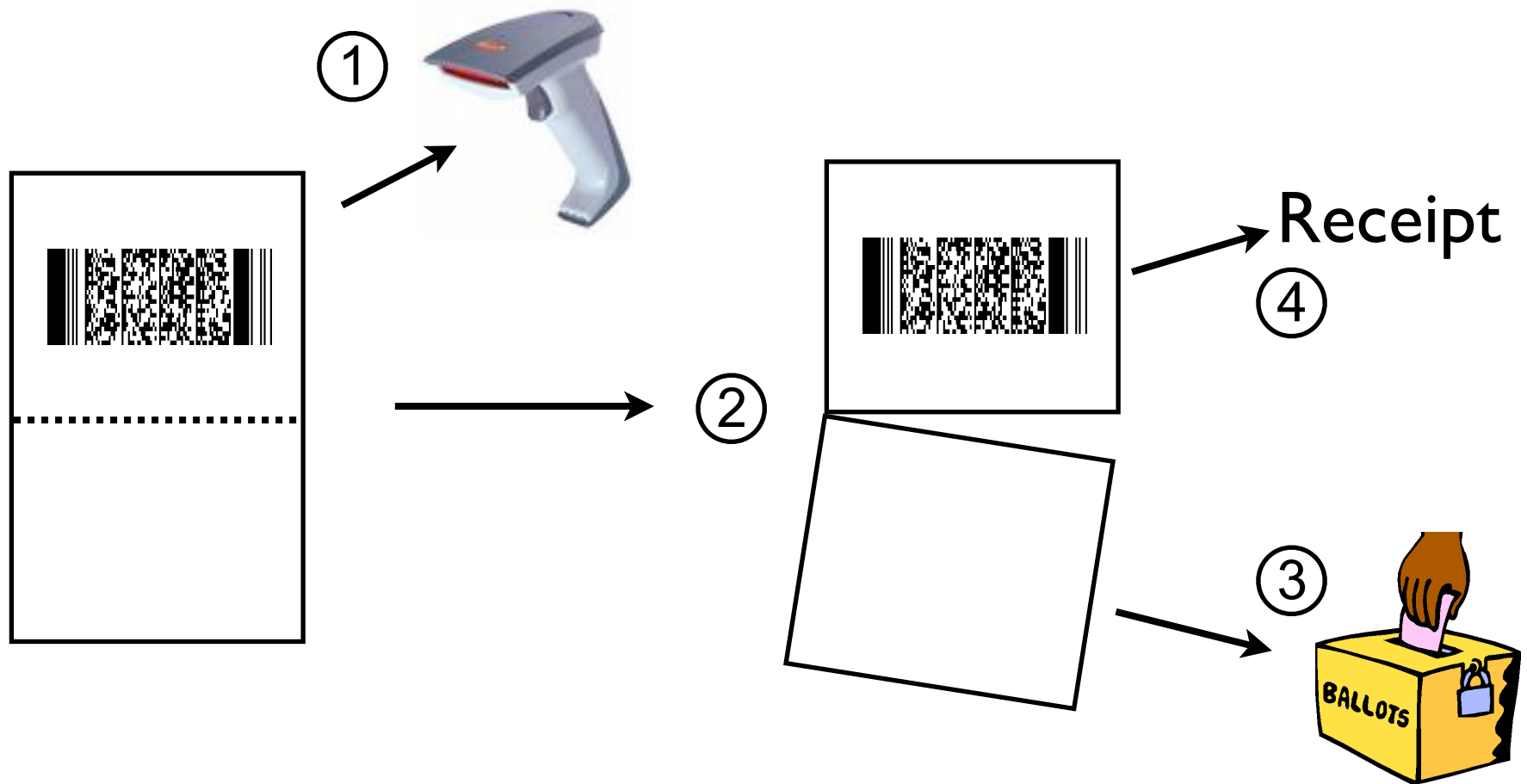


# Ballot Casting



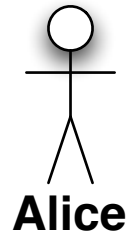


# Ballot Casting

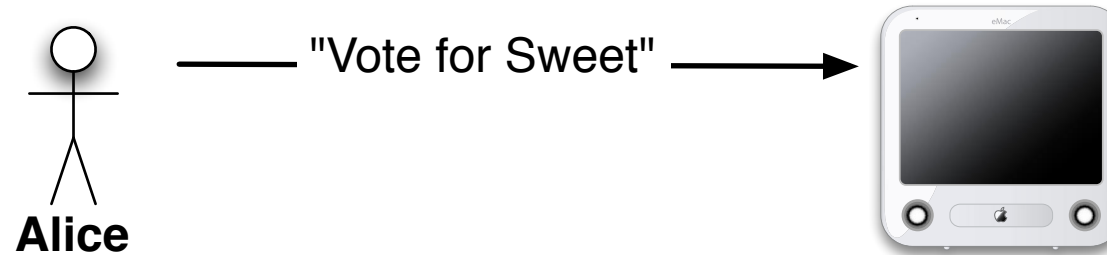


# Verifying Consistency [Benaloh]

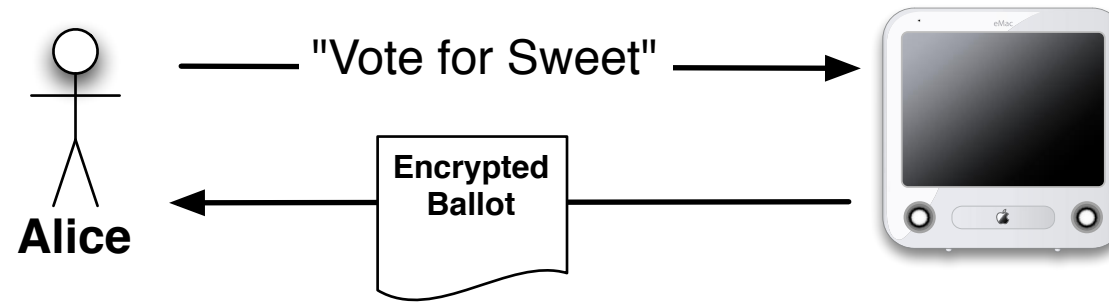
# Verifying Consistency [Benaloh]



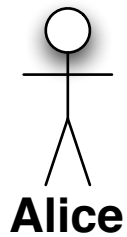
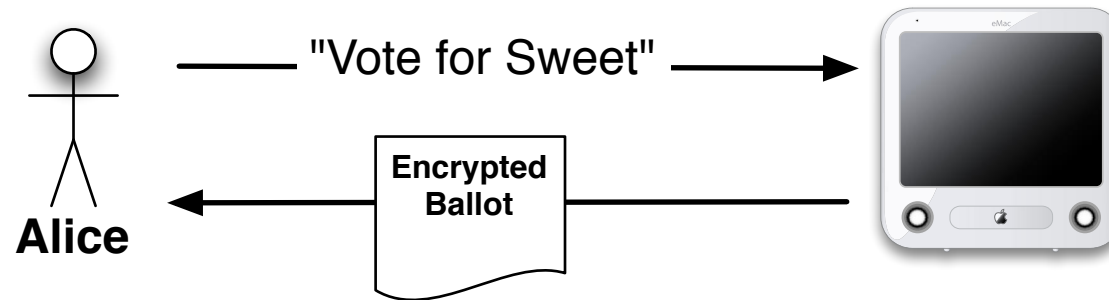
# Verifying Consistency [Benaloh]



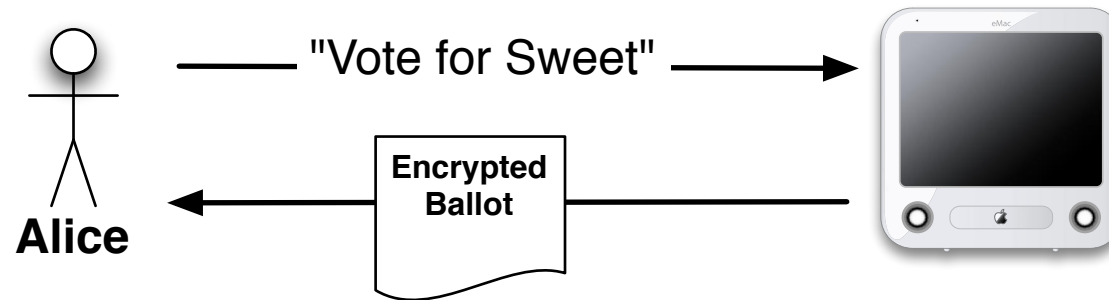
# Verifying Consistency [Benaloh]



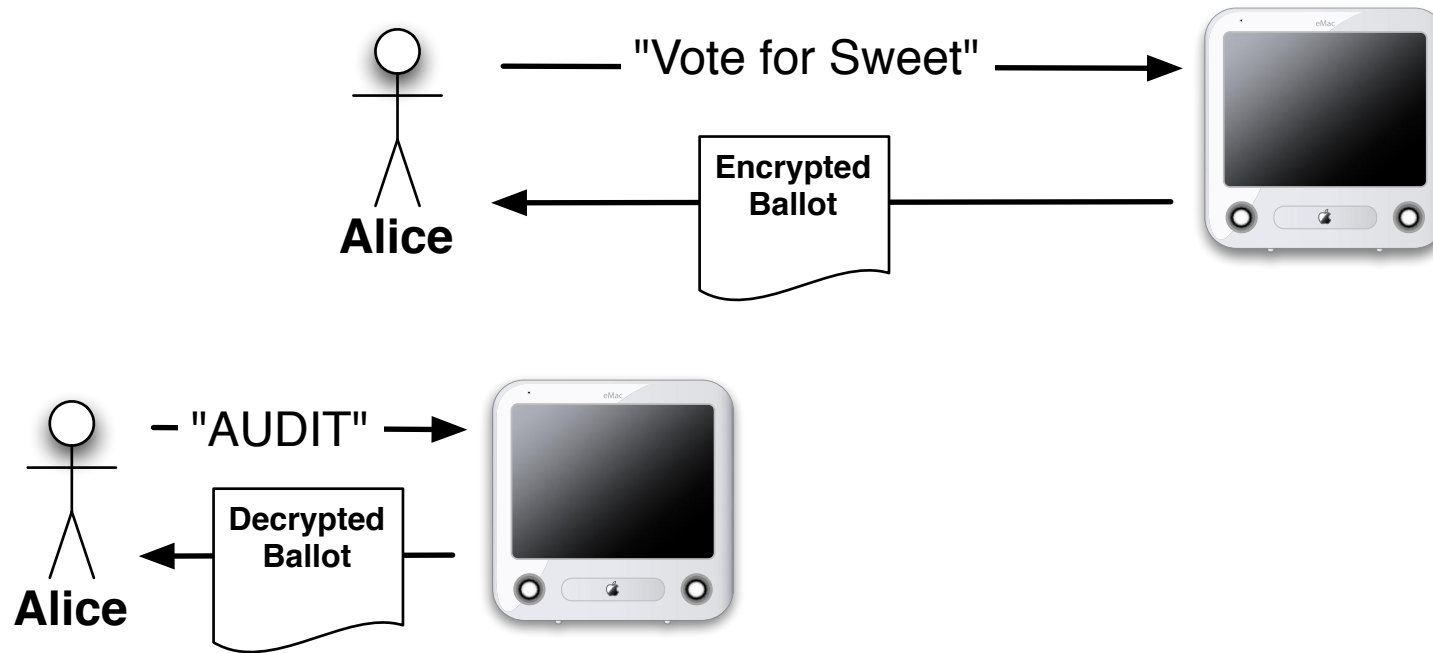
# Verifying Consistency [Benaloh]



# Verifying Consistency [Benaloh]

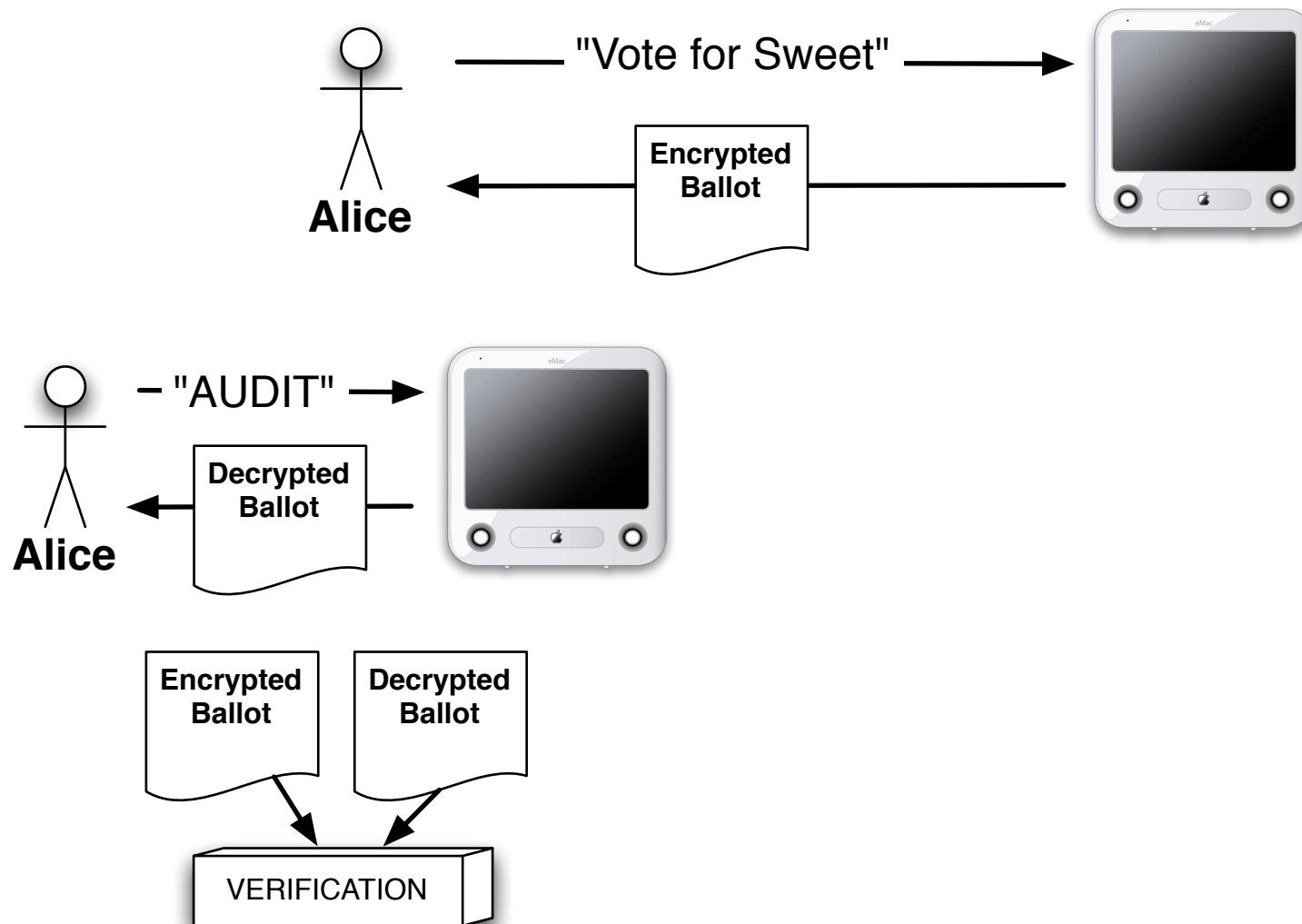


# Verifying Consistency [Benaloh]

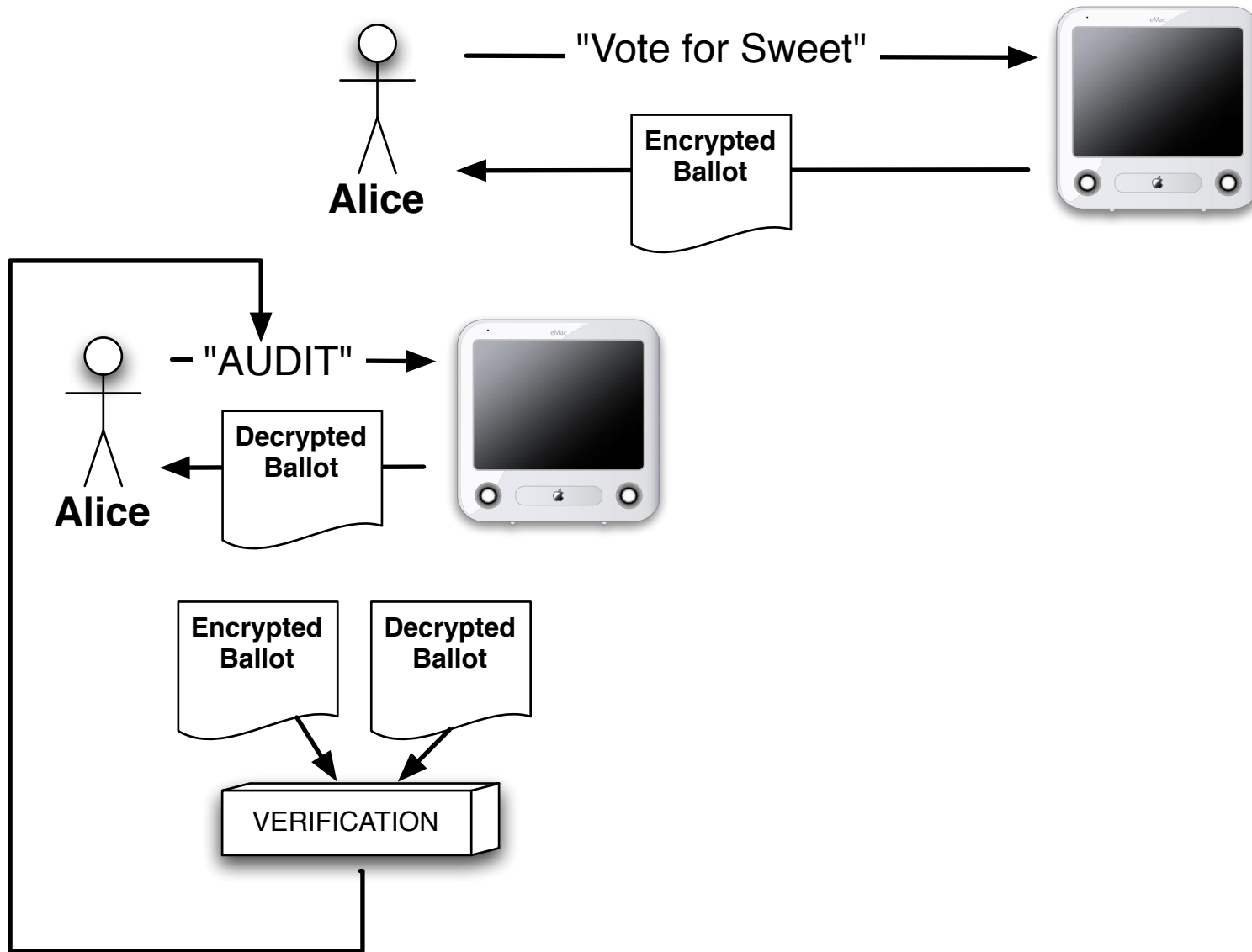




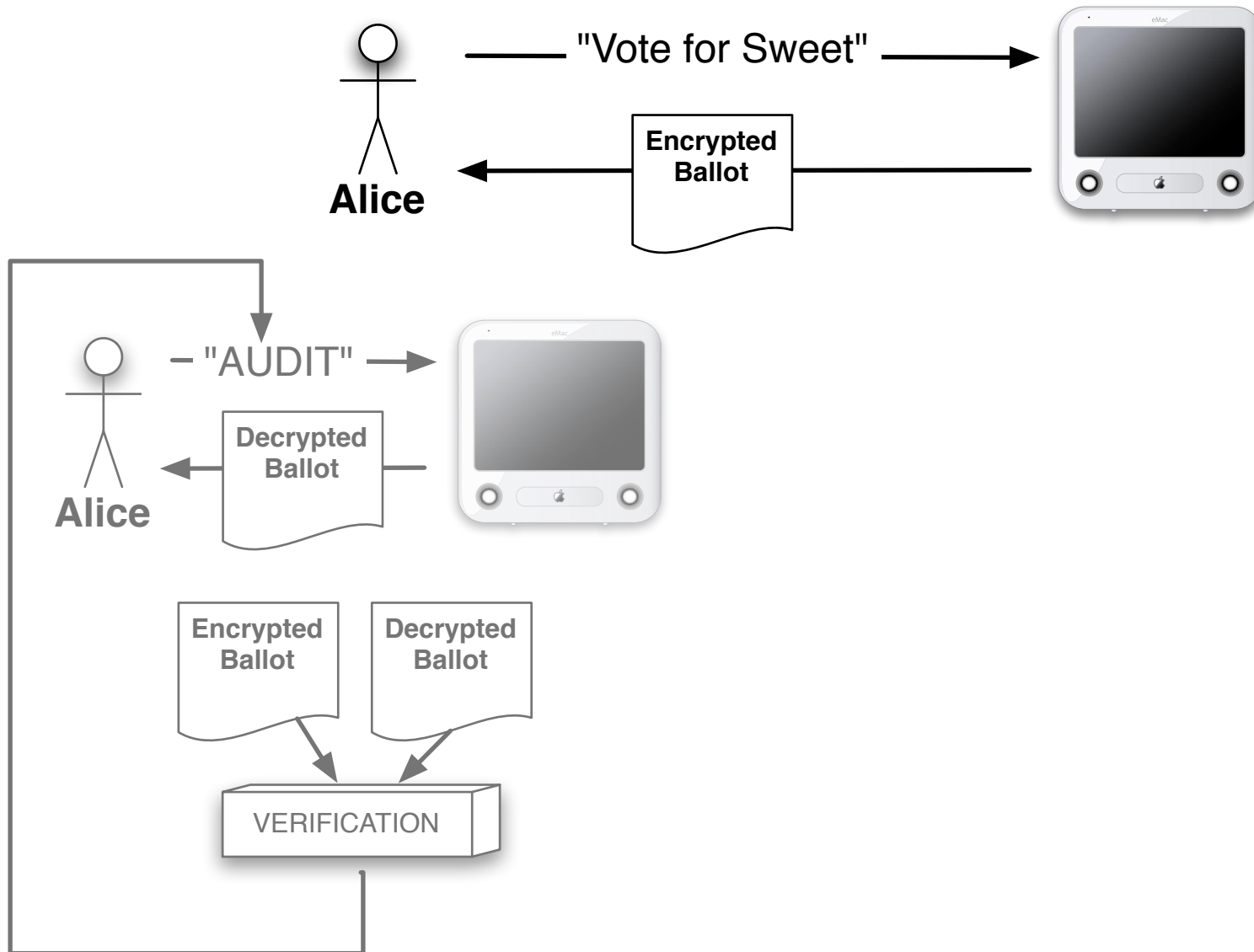
# Verifying Consistency [Benaloh]



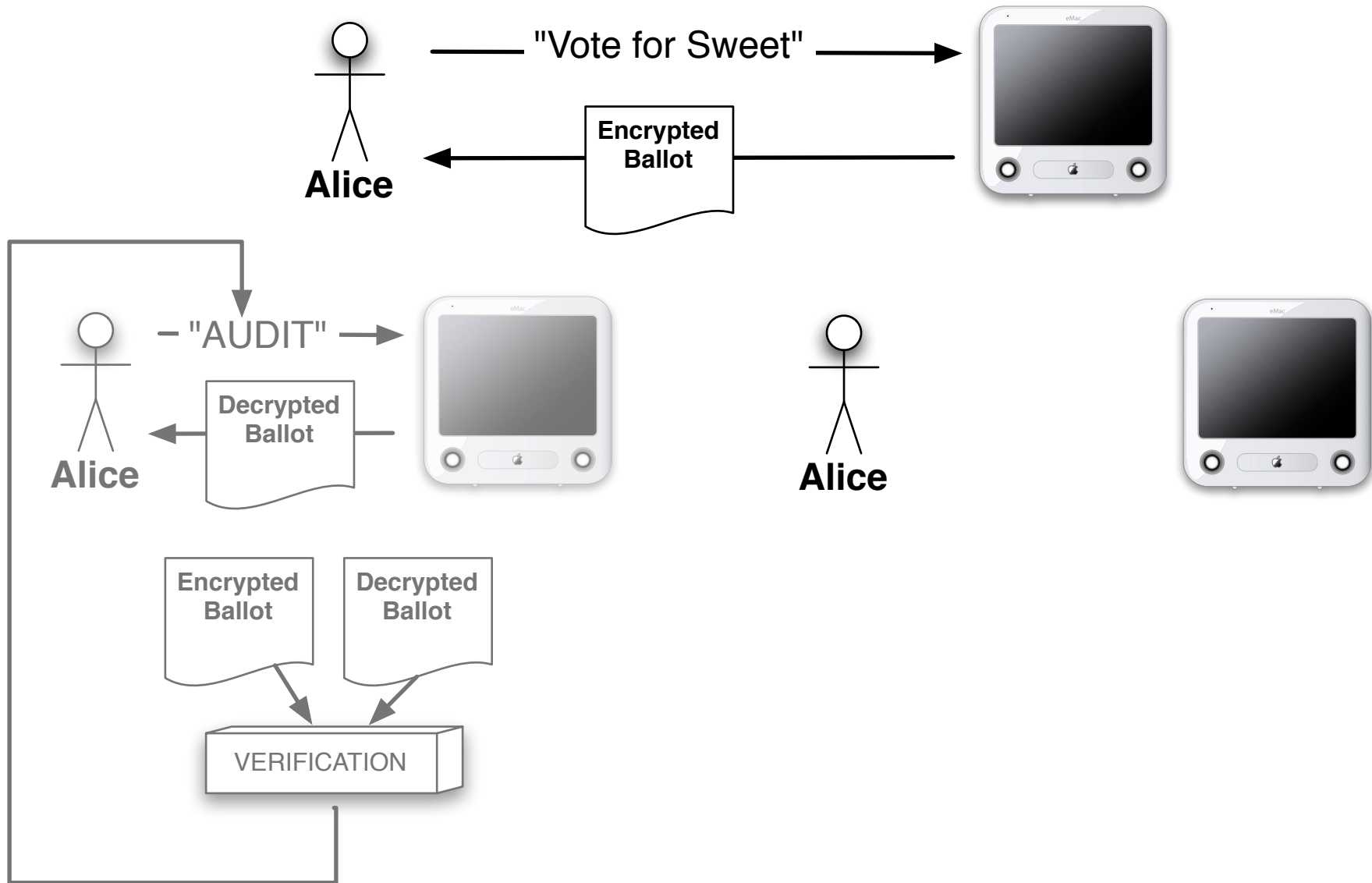
# Verifying Consistency [Benaloh]



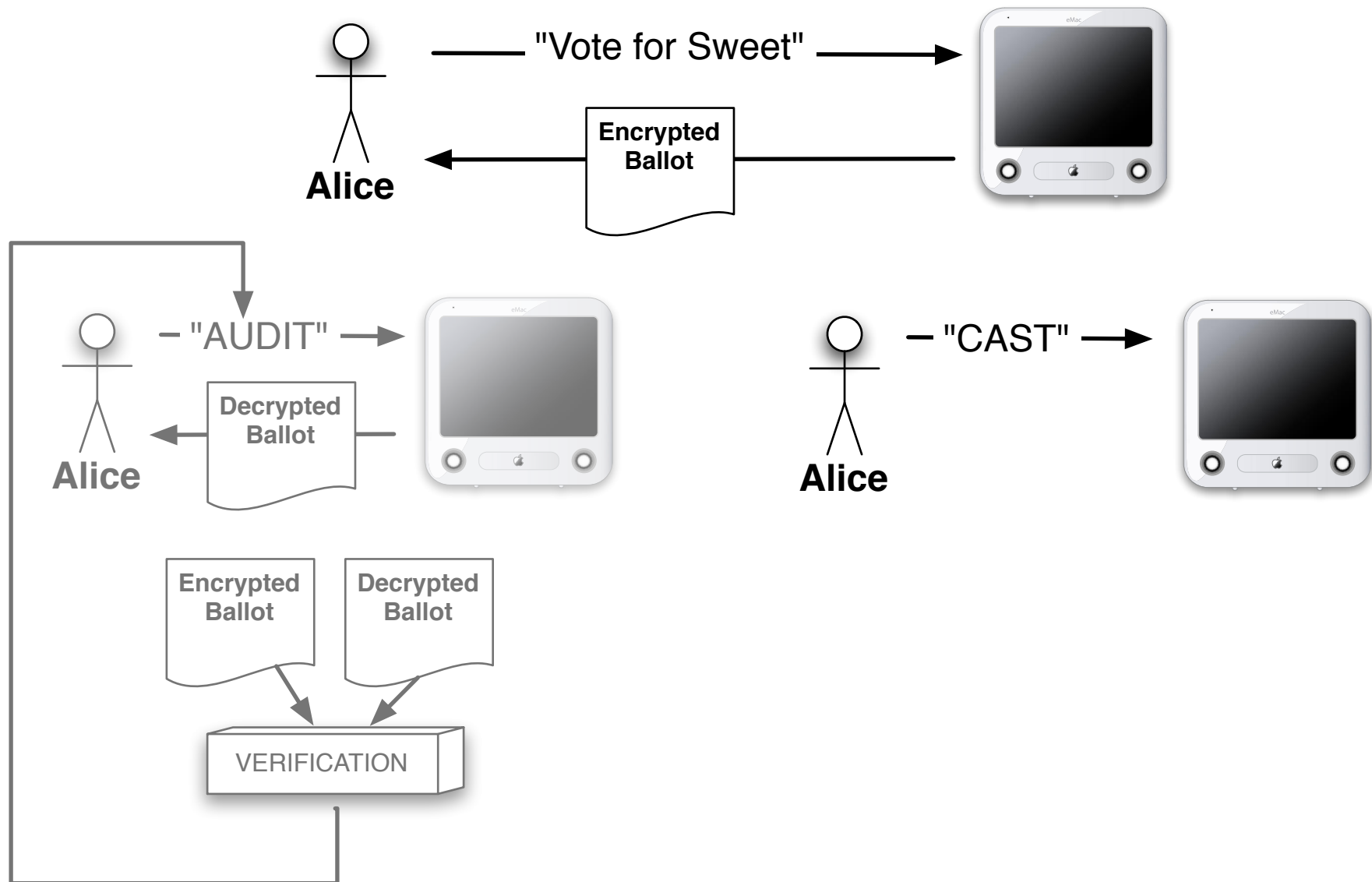
# Verifying Consistency [Benaloh]



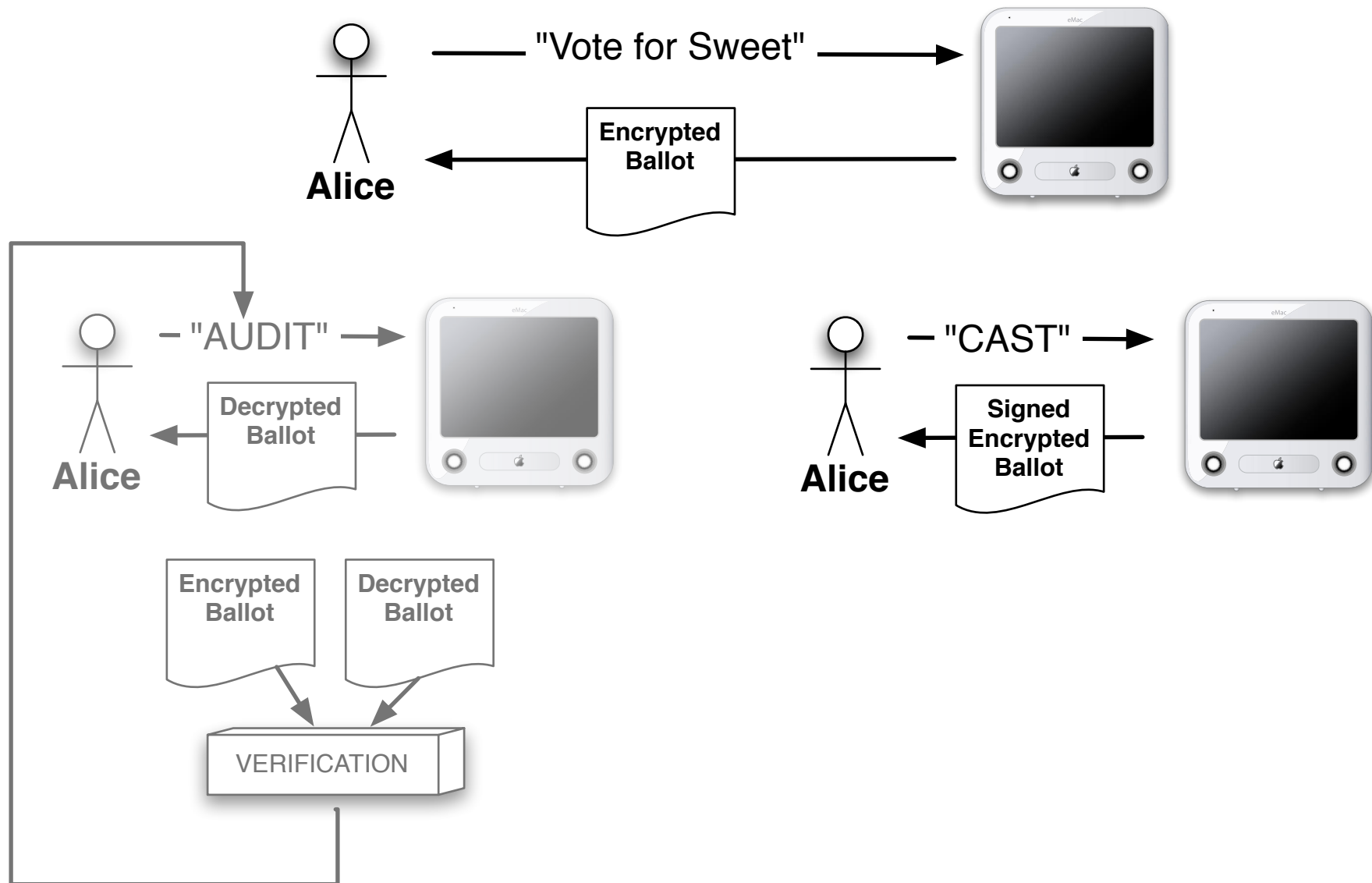
# Verifying Consistency [Benaloh]



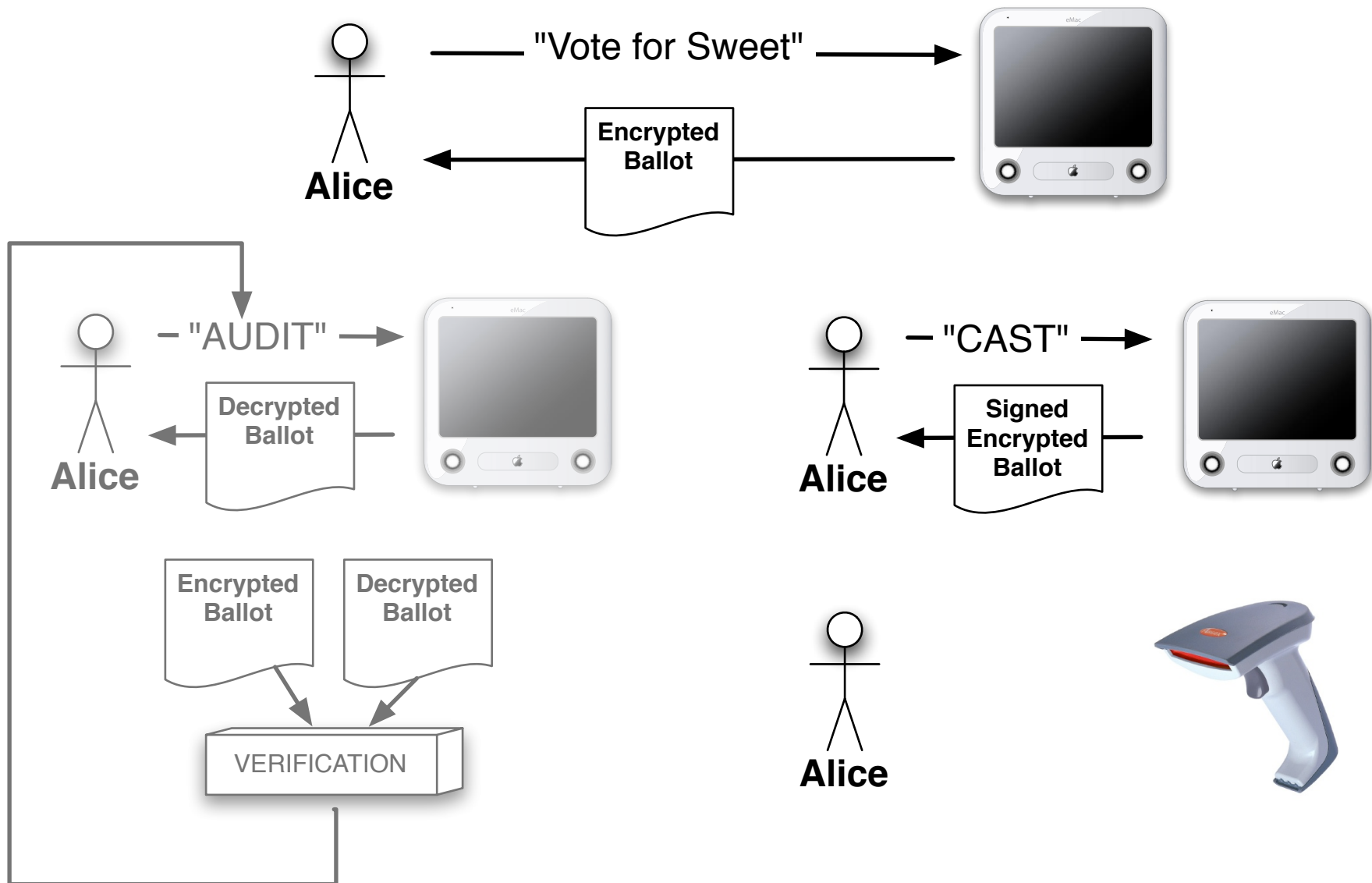
# Verifying Consistency [Benaloh]



# Verifying Consistency [Benaloh]

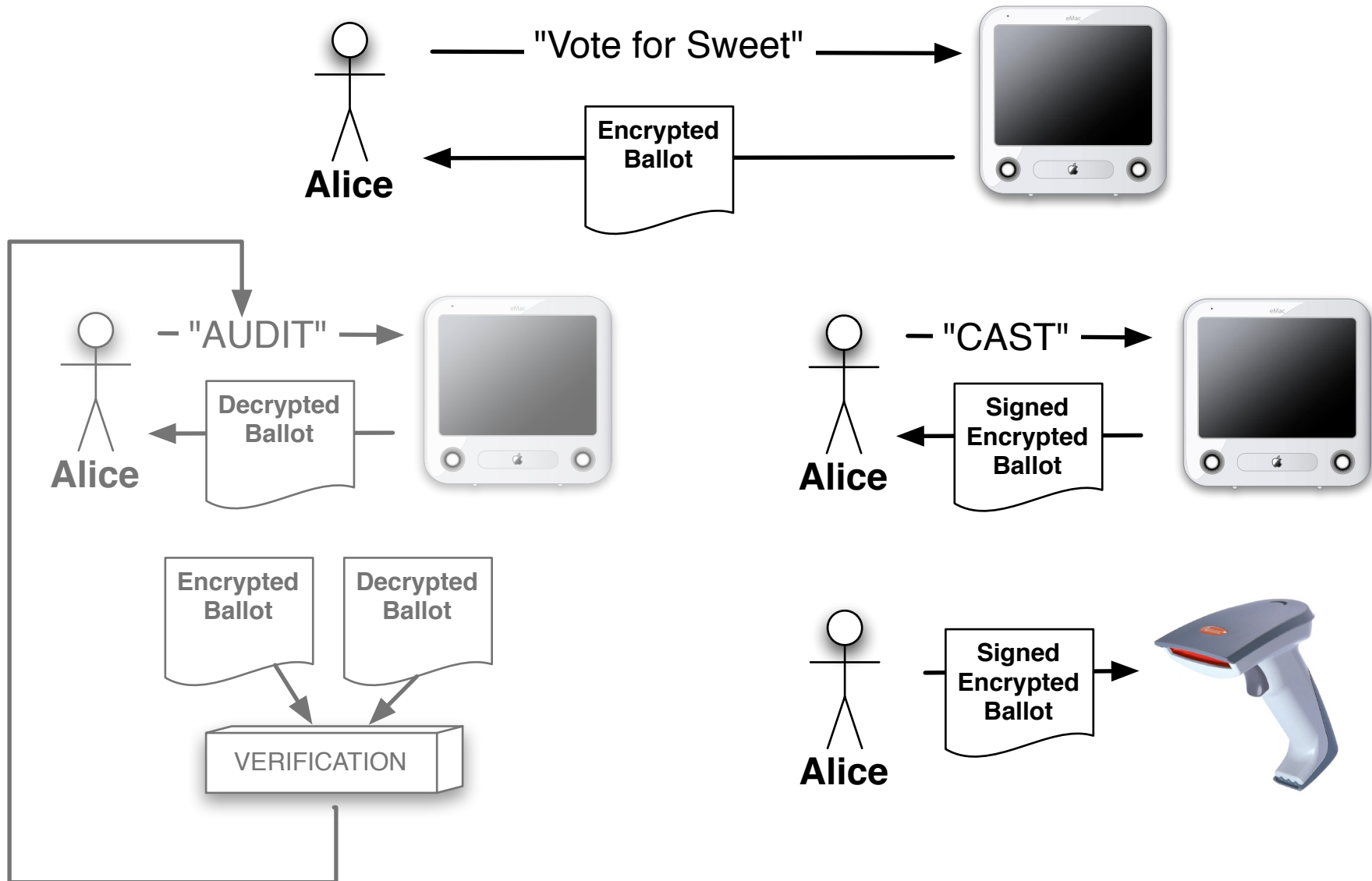


# Verifying Consistency [Benaloh]



<http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg>

# Verifying Consistency [Benaloh]



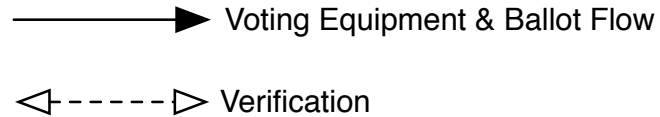
<http://en.wikipedia.org/wiki/Image:Barcode-scanner.jpg>



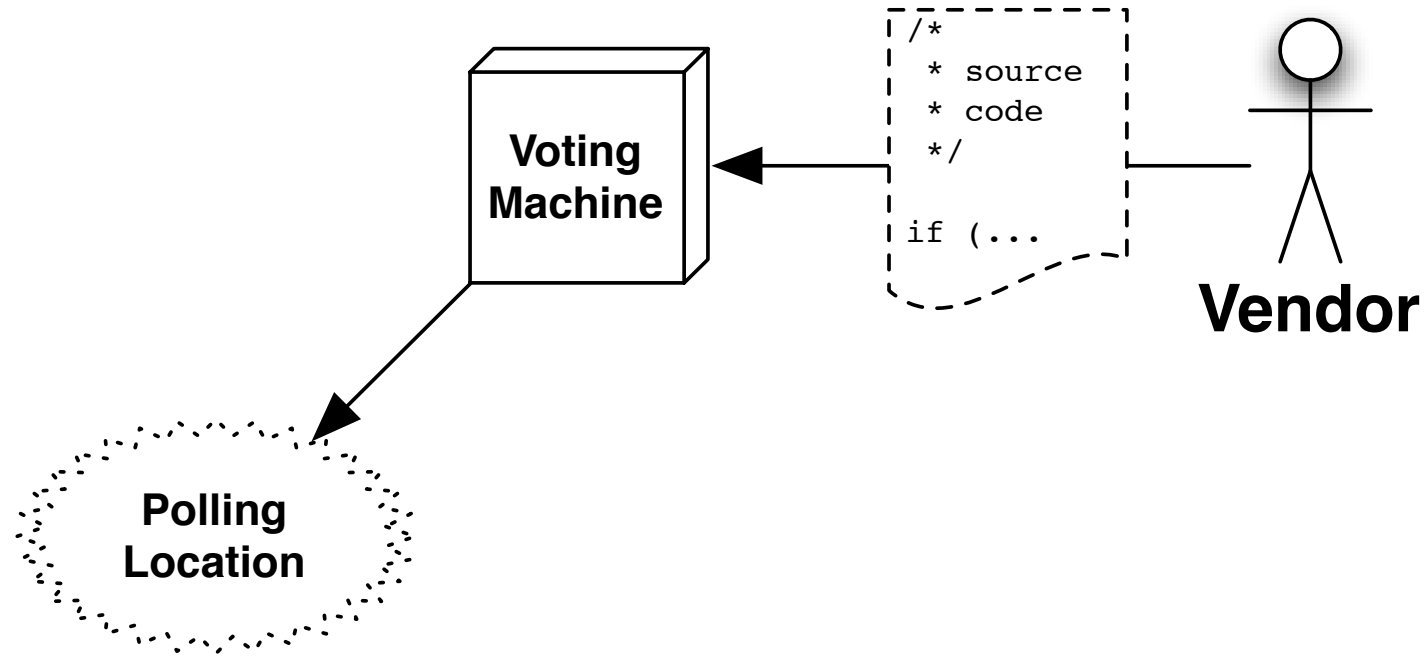
# The Tallying Process

- **Paper tally**
- **Electronic tally**
  1. Homomorphic public-key encryption or mixnets
  2. Zero-knowledge proofs

# Putting It Together



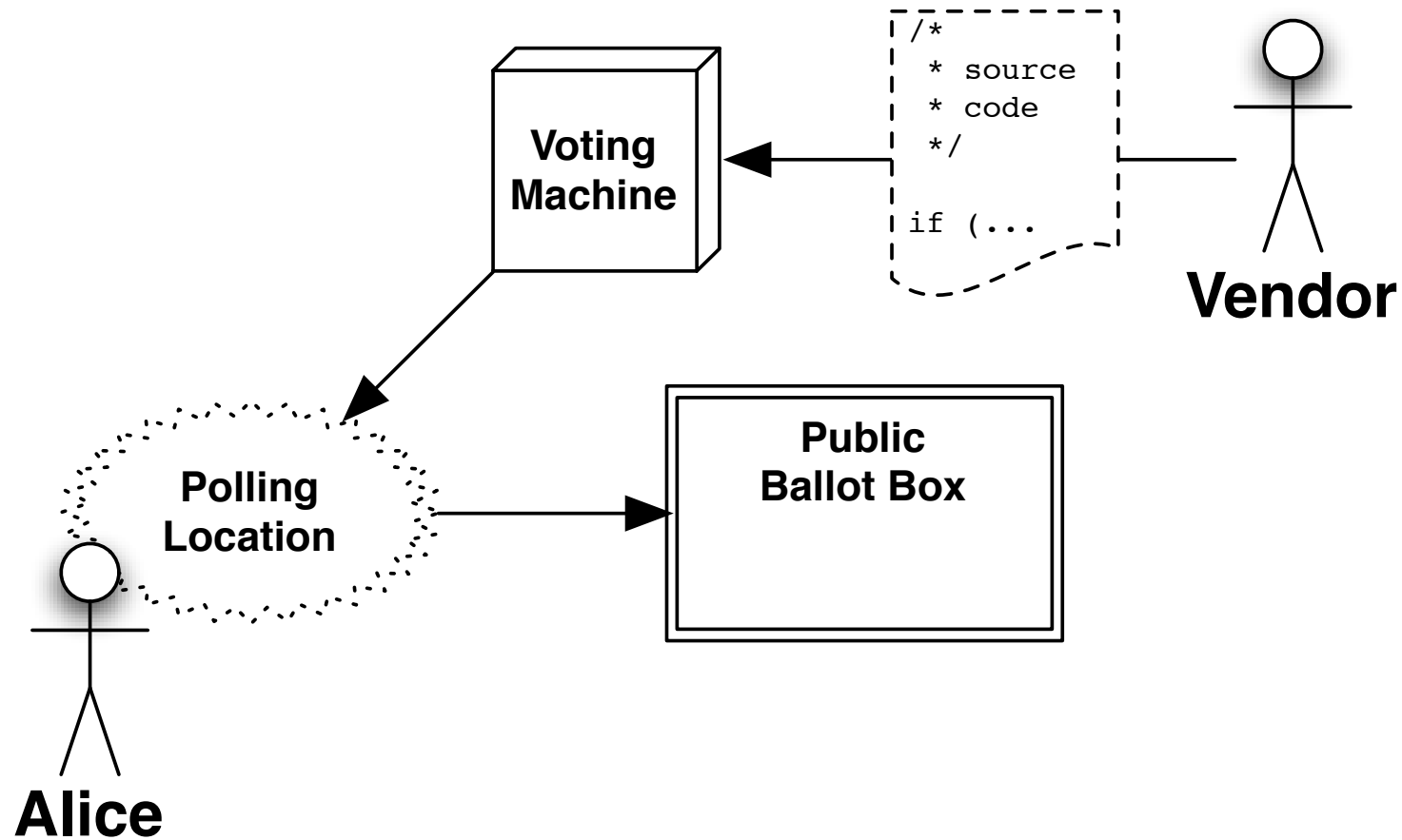
# Putting It Together



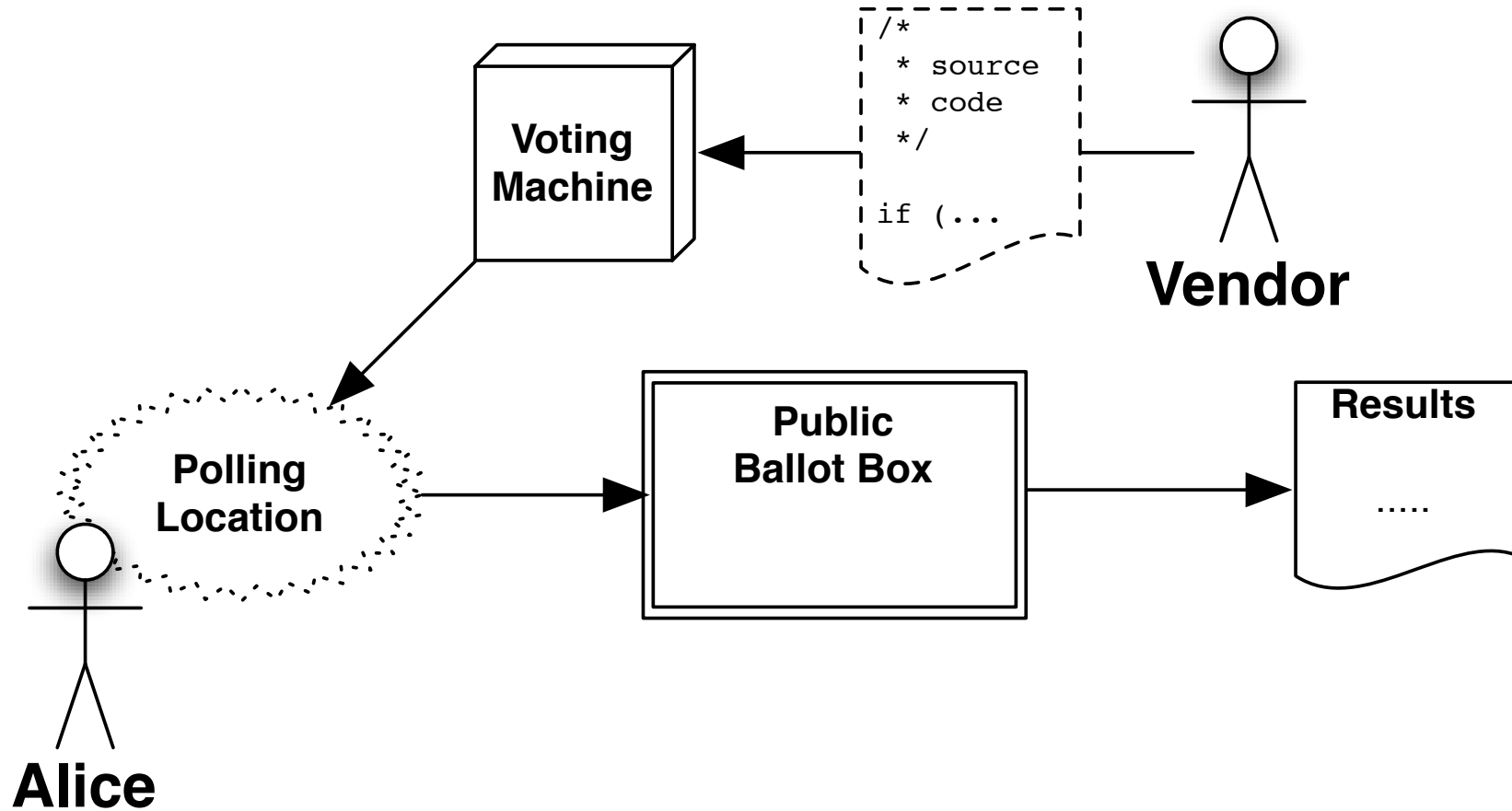
————▶ Voting Equipment & Ballot Flow

◀-----▶ Verification

# Putting It Together



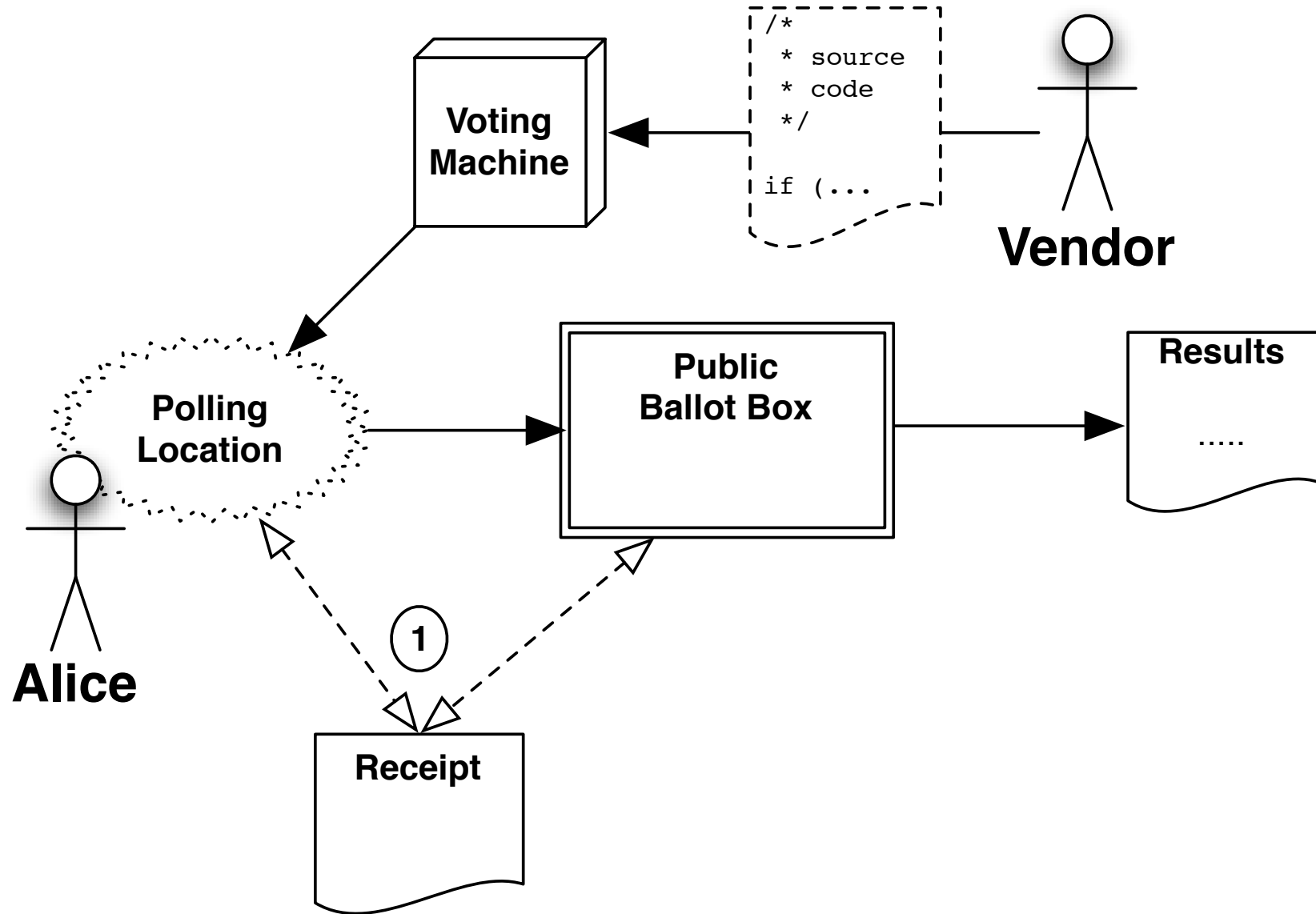
# Putting It Together



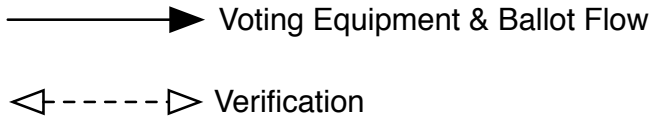
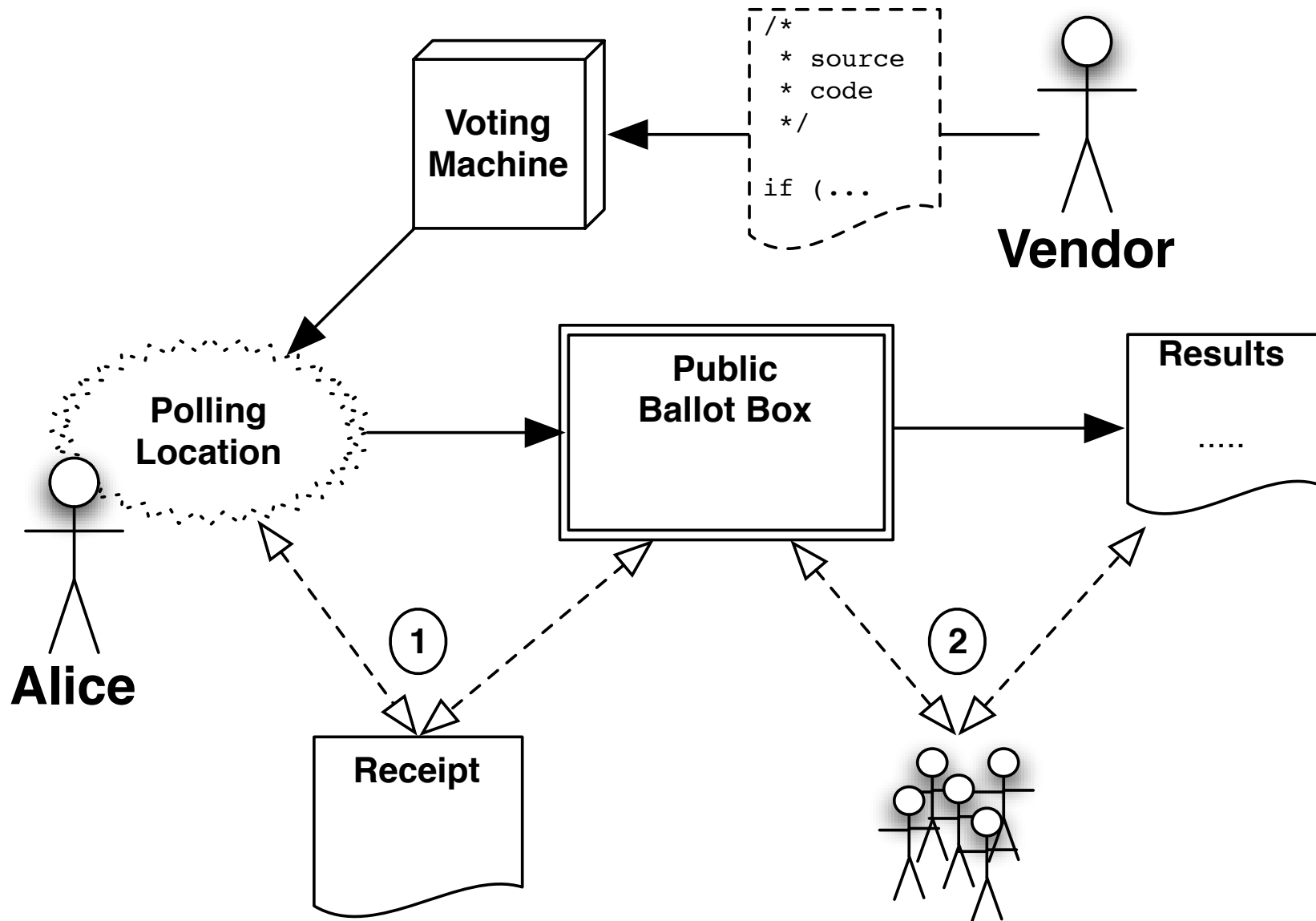
————▶ Voting Equipment & Ballot Flow

◀-----▶ Verification

# Putting It Together



# Putting It Together



# Open-Audit Elections

- **Alice** verifies **her vote**.
- **Everyone** verifies **the tally**.
- **Incoercibility** is enforced.



# Open-Audit Elections

- **Alice** verifies **her vote**.
- **Everyone** verifies **the tally**.
- **Incoercibility** is enforced.

Anyone can Audit.

# Open Audit Voting: Helios (Ben Adida, 2009)

**Helios Voting Booth**

## Princeton Fall 2009 Test Election

Election Fingerprint:  
**qncOeX00k7snXPBTjX9k258J981AY163KP2m8Nyj3+o**

Election to evaluate Helios for Princeton Student Elections

|                   |             |            |
|-------------------|-------------|------------|
| <b>(1) Select</b> | (2) Encrypt | (3) Submit |
|-------------------|-------------|------------|

---

**Question #1 of 3**

*Who should be the Class of 2013 President?*

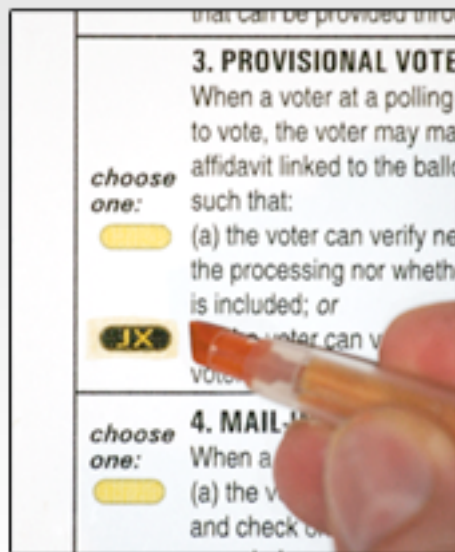
(select up to 1 answer)

- Miss Piggy
- Jerry Seinfeld
- Bugs Bunny
- Chuck Norris

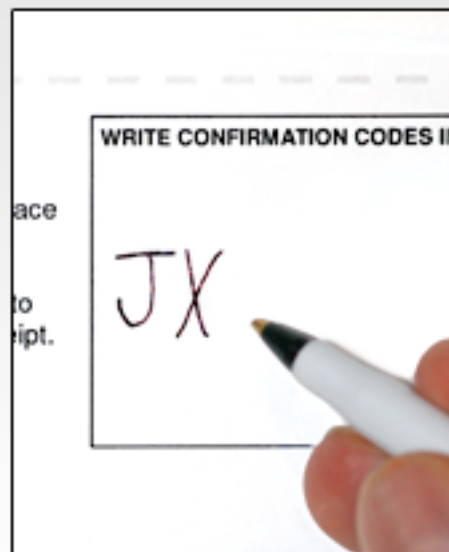
Next

# Open Audit Voting: Scantegrity II (Chaum et al., 2009)

## Mark



## Record



## Check



# Questions?

