

Cryptography and Voting

Ben Adida
Harvard University

EVT & WOTE
August 11th, 2009
Montreal, Canada

“If you think
cryptography
is the solution
to your problem....

... then you
don't understand
cryptography...

... then you
don't understand
cryptography...

... and you don't
understand your
problem.”

-Peter, Butler, Bruce

Yet, cryptography solves
problems that initially
appear to be impossible.

There is a
potential paradigm shift.

A means of
election verification
far more powerful
than other methods.

Three Points

1. Voting is a unique trust problem.
2. Cryptography is not just about secrets, it creates trust between competitors, it democratizes the auditing process.
3. Open-Audit Voting is closing in on practicality.

1.

Voting is a unique
trust problem.

“Swing Vote”

terrible movie.

hilarious ending.

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."





Bad Analogies

- Dan Wallach's great rump session talk.
- More than that
ATMs and planes are vulnerable
(they are, but that's not the point)
- It's that voting is **much** harder.

Bad Analogies

■ Adversaries

- ➔ pilots vs. passengers (airline is on your side, I think.)
- ➔ banking privacy is only voluntary:
you are not the enemy.

■ Failure Detection & Recover

- ➔ plane crashes & statements vs. 2% election fraud
- ➔ Full banking receipts vs. destroying election evidence

■ Imagine

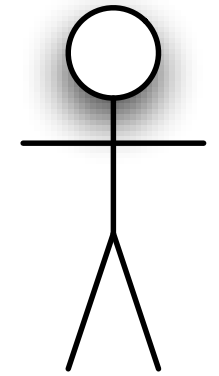
- ➔ a bank where you never get a receipt.
- ➔ an airline where the pilot is working against you.

Ballot secrecy
conflicts with auditing,
cryptography
can reconcile them.

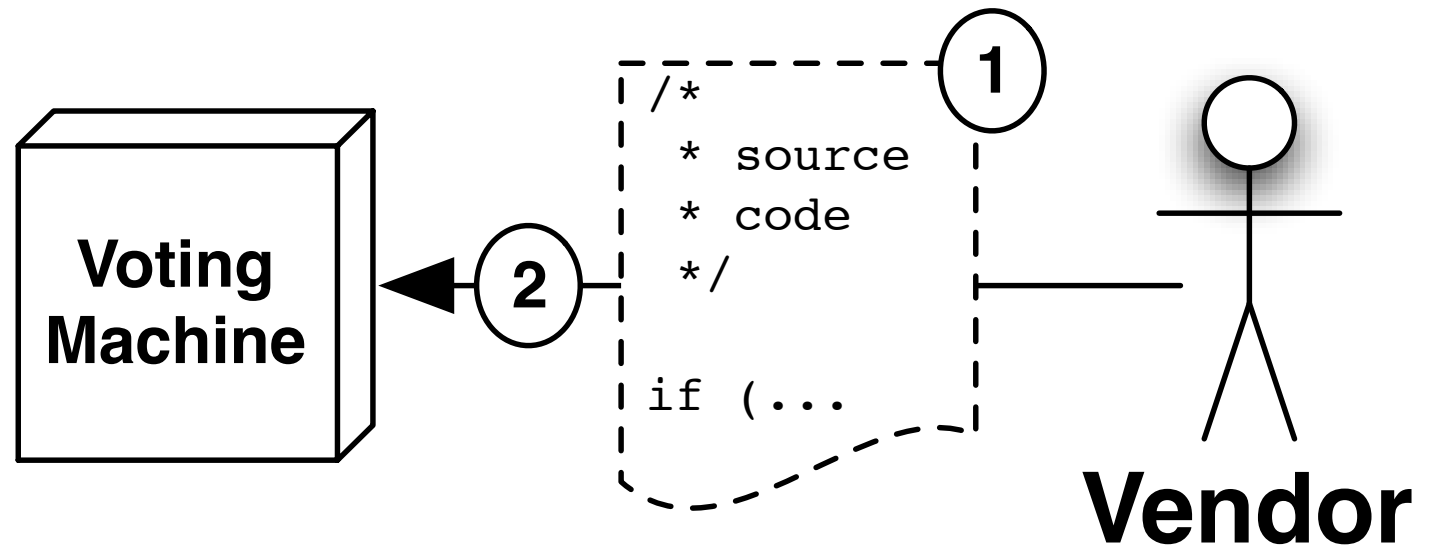


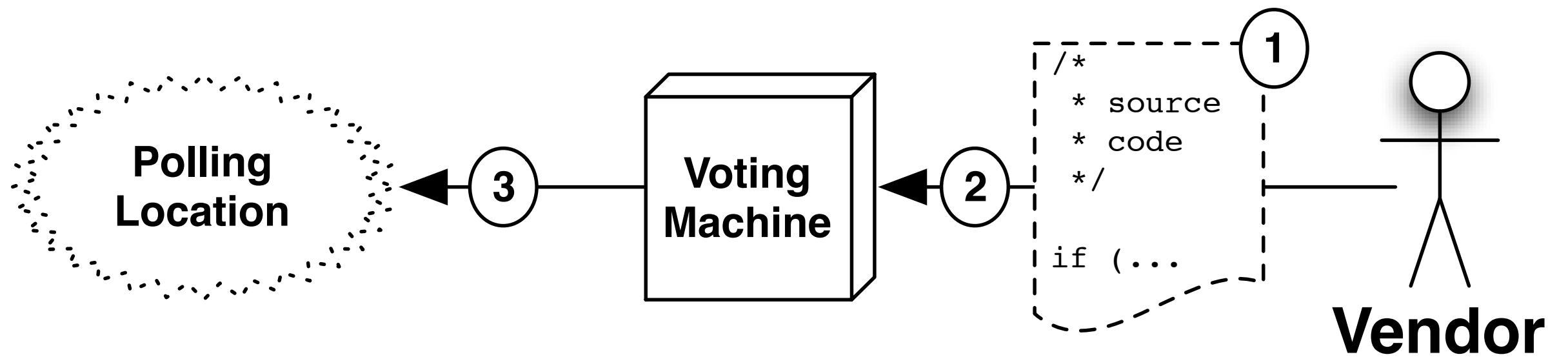

```
/*  
 * source  
 * code  
 */  
if (...
```

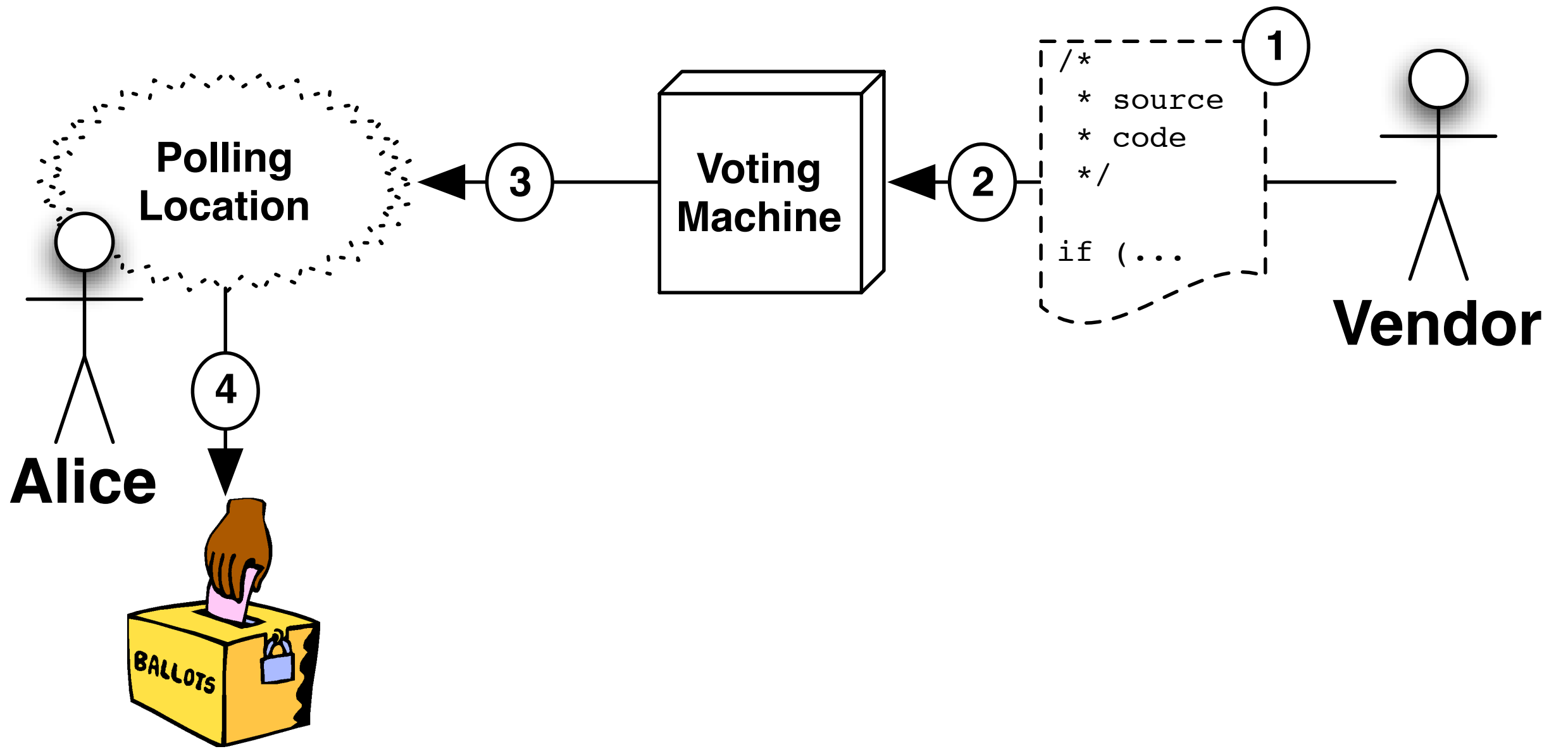
1

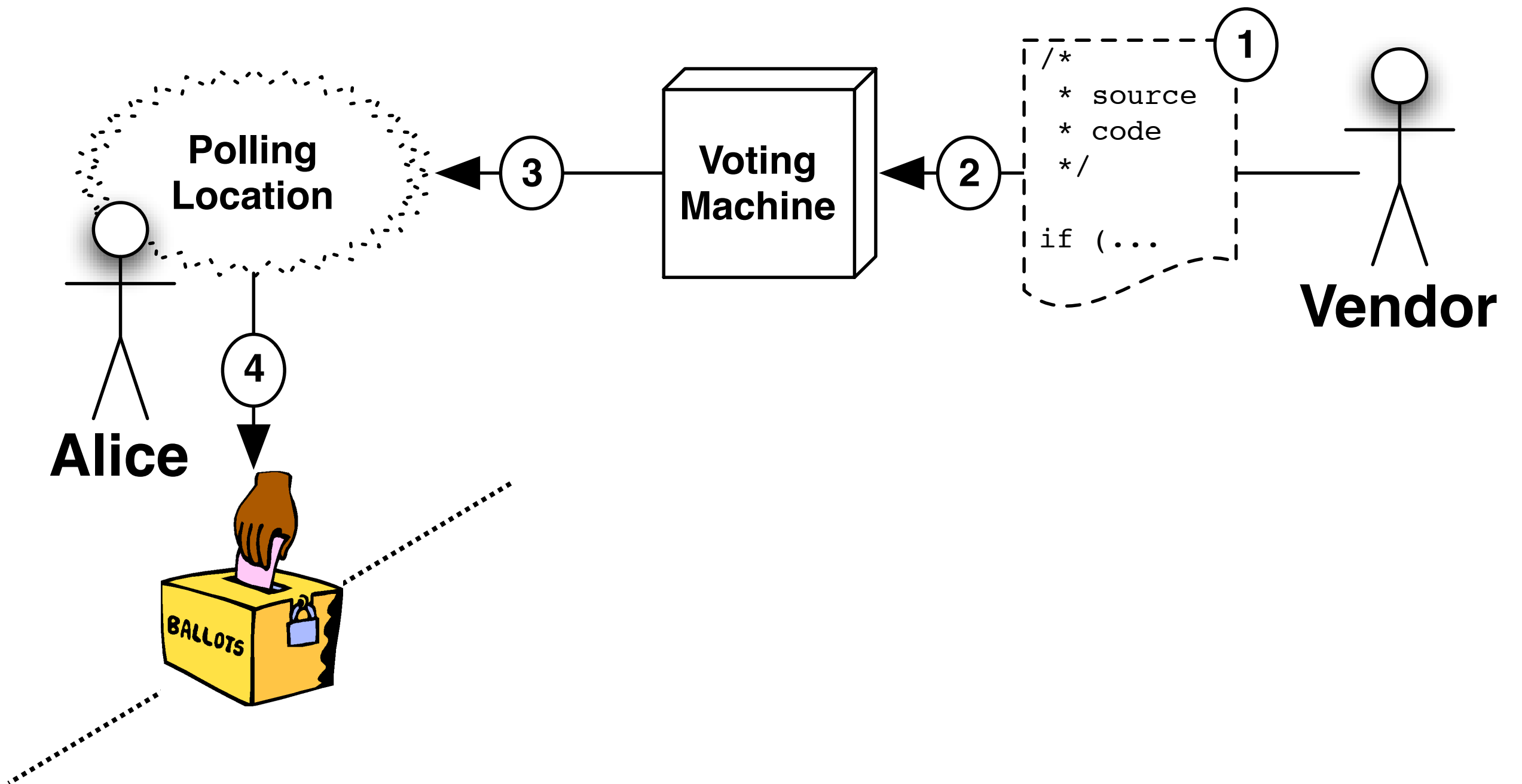


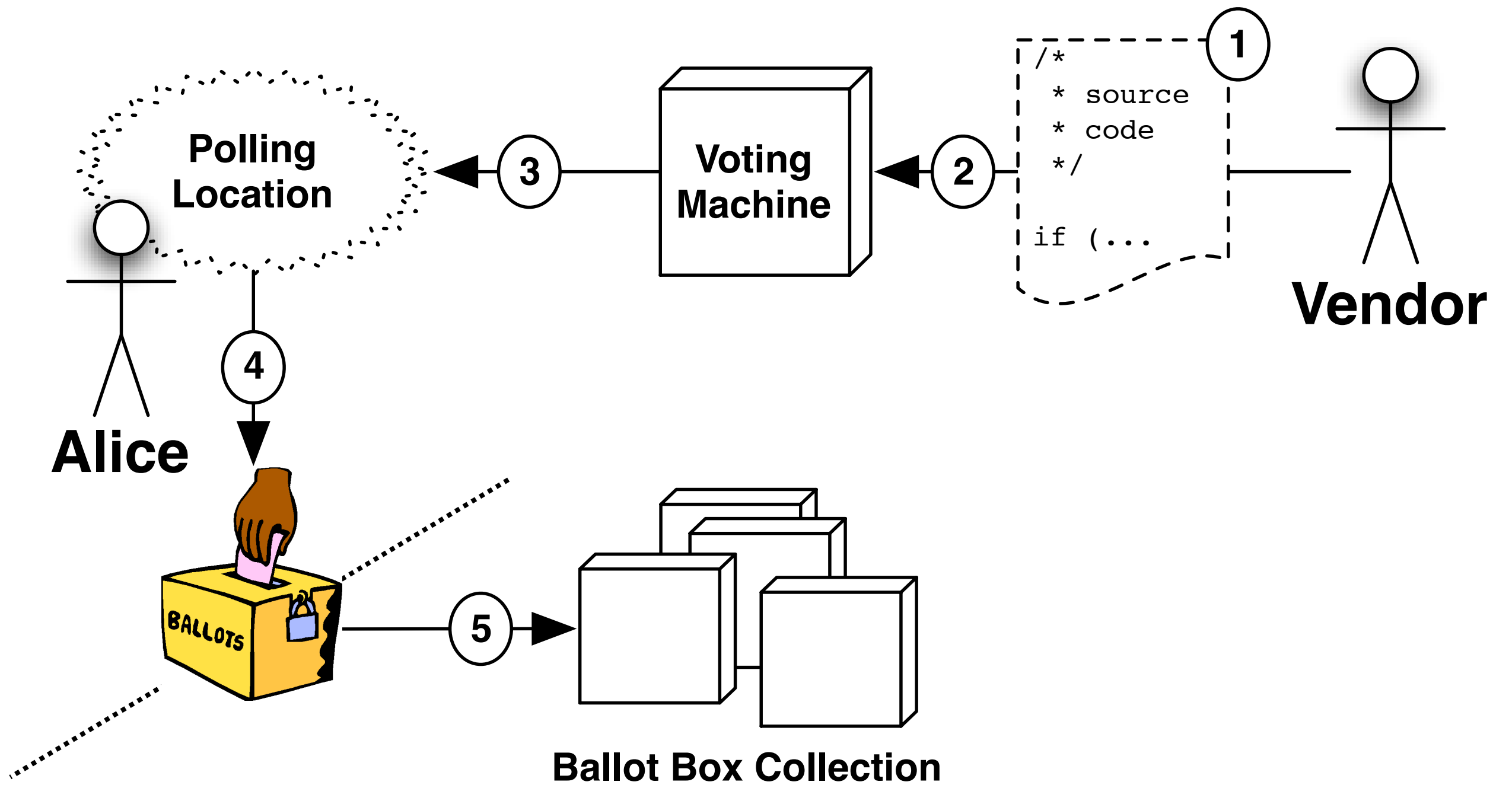
Vendor

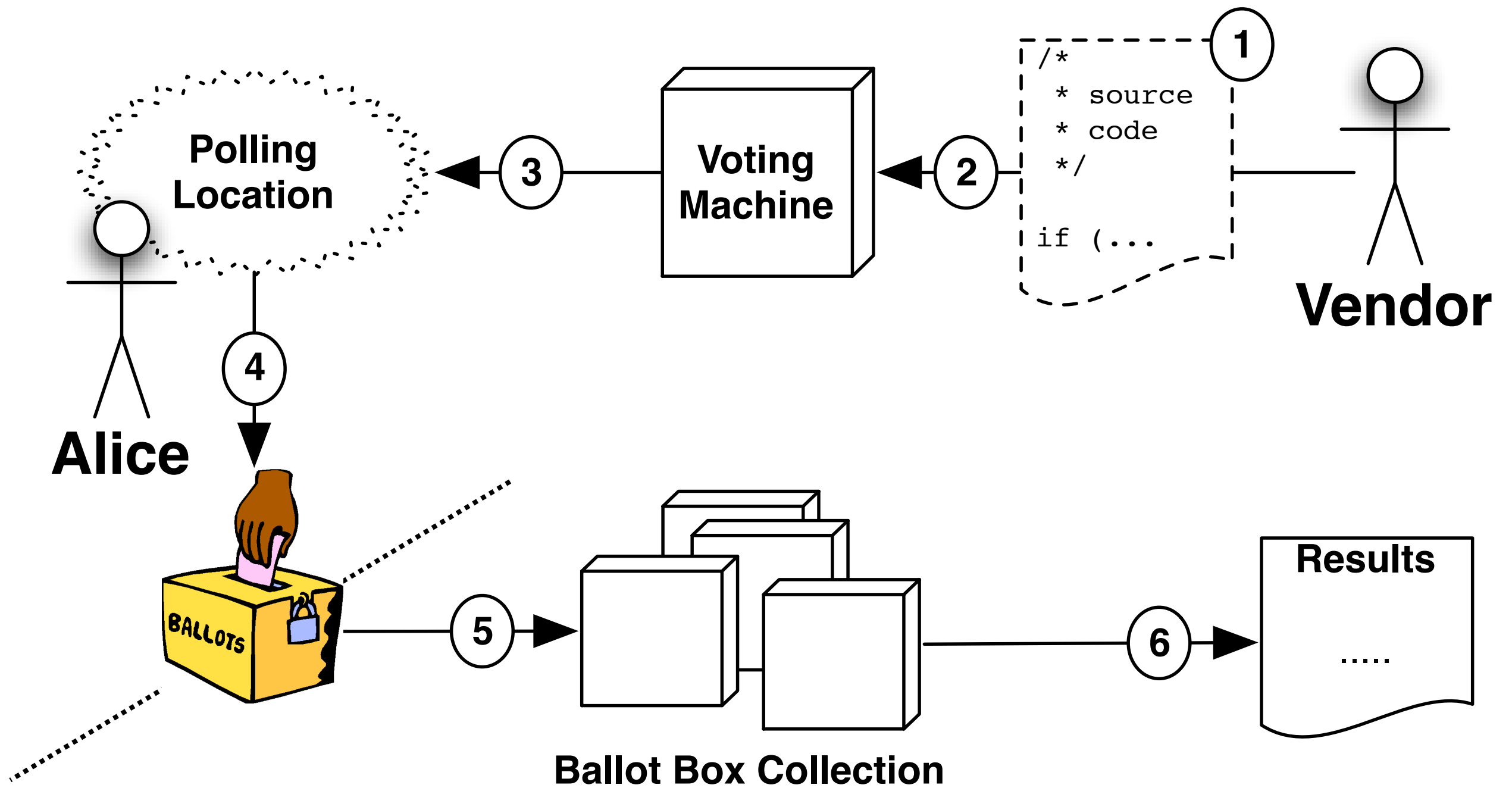


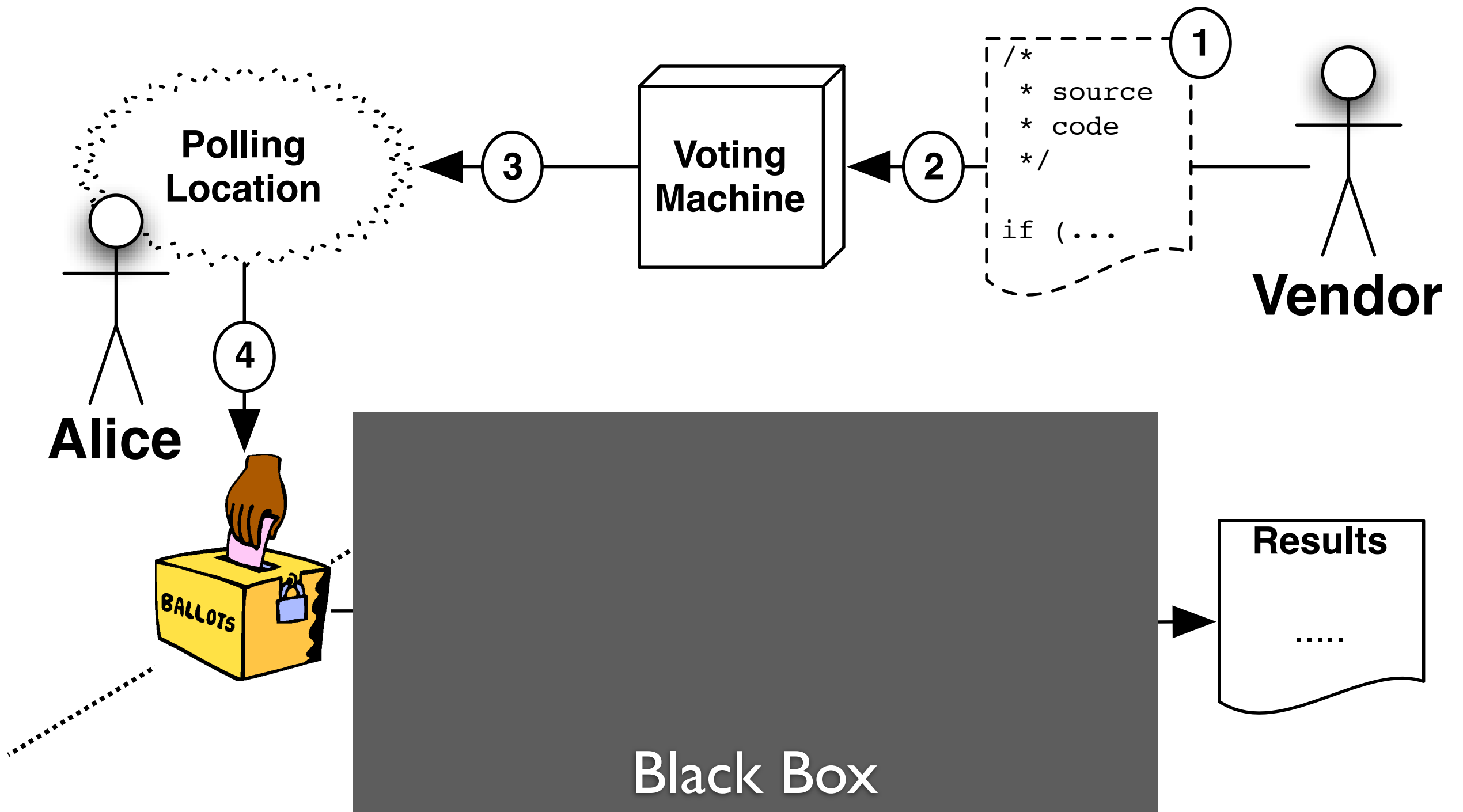












Chain of Custody

Chain of Custody

Scavenged ballot box lids haunt S.F. elections

[Erin McCormick, Chronicle Staff Writer](#)

Monday, January 7, 2002

Chain of Custody

Scavenged **ballot box** lids haunt S.F. elections

[Erin McC](#) Helicopter Crash Delays Afghan
Monday, J Vote Count

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

Chain of Custody

Scavenged **ballot box** lids haunt S.F. elections

[Erin McC](#) Helicopter Crash Delays Afghan
Monday, J 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.

Chain of Custody

Scavenged **ballot box** lids haunt S.F. elections

[Erin McC](#)

Helicopter Crash Delays Afghan

Monday, J

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 election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY

Published: Thursday July 6, 2006

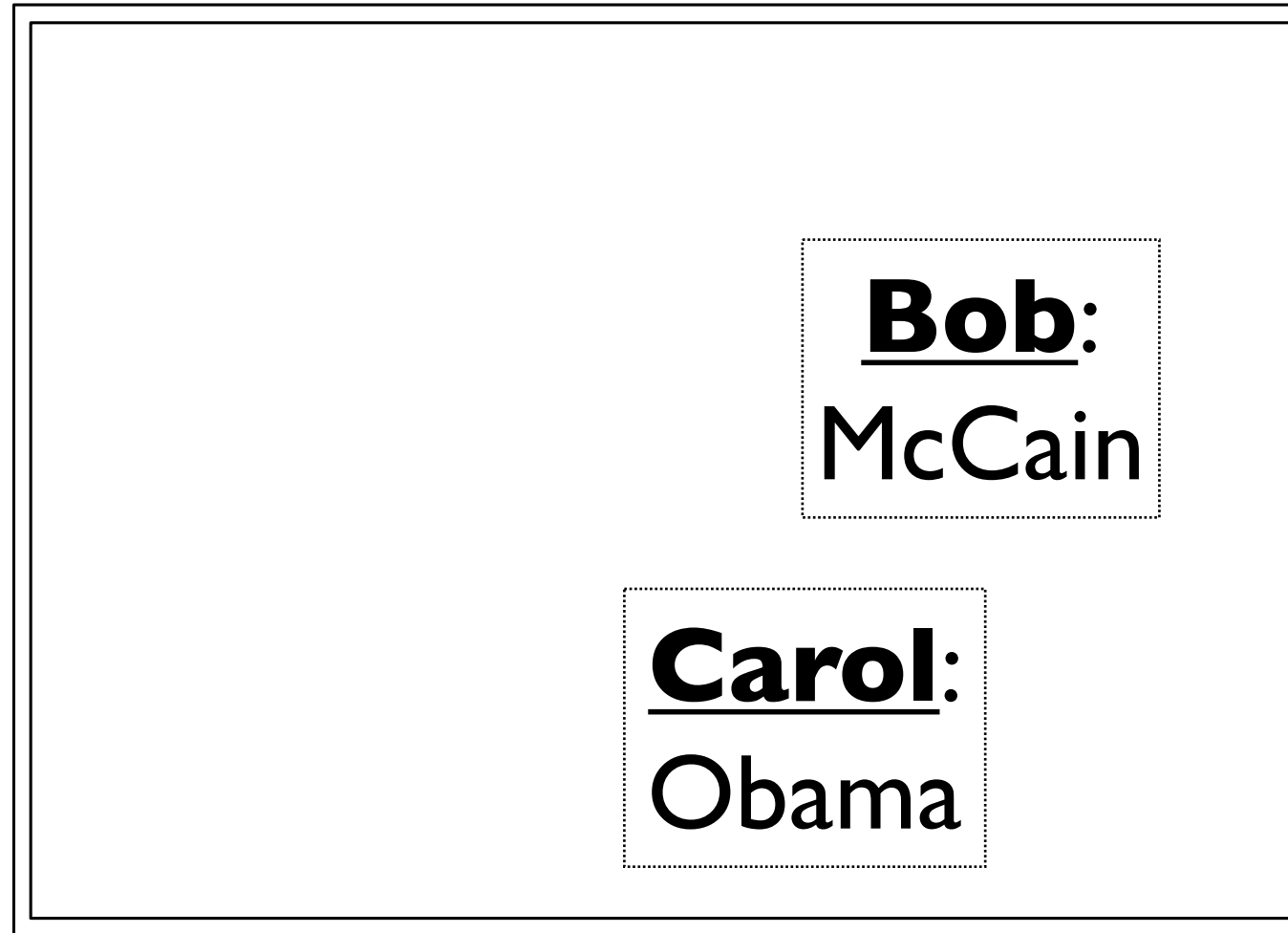
Initially,
cryptographers
re-created
physical processes
in the digital arena.

Then, a realization:
cryptography enables a
new voting paradigm

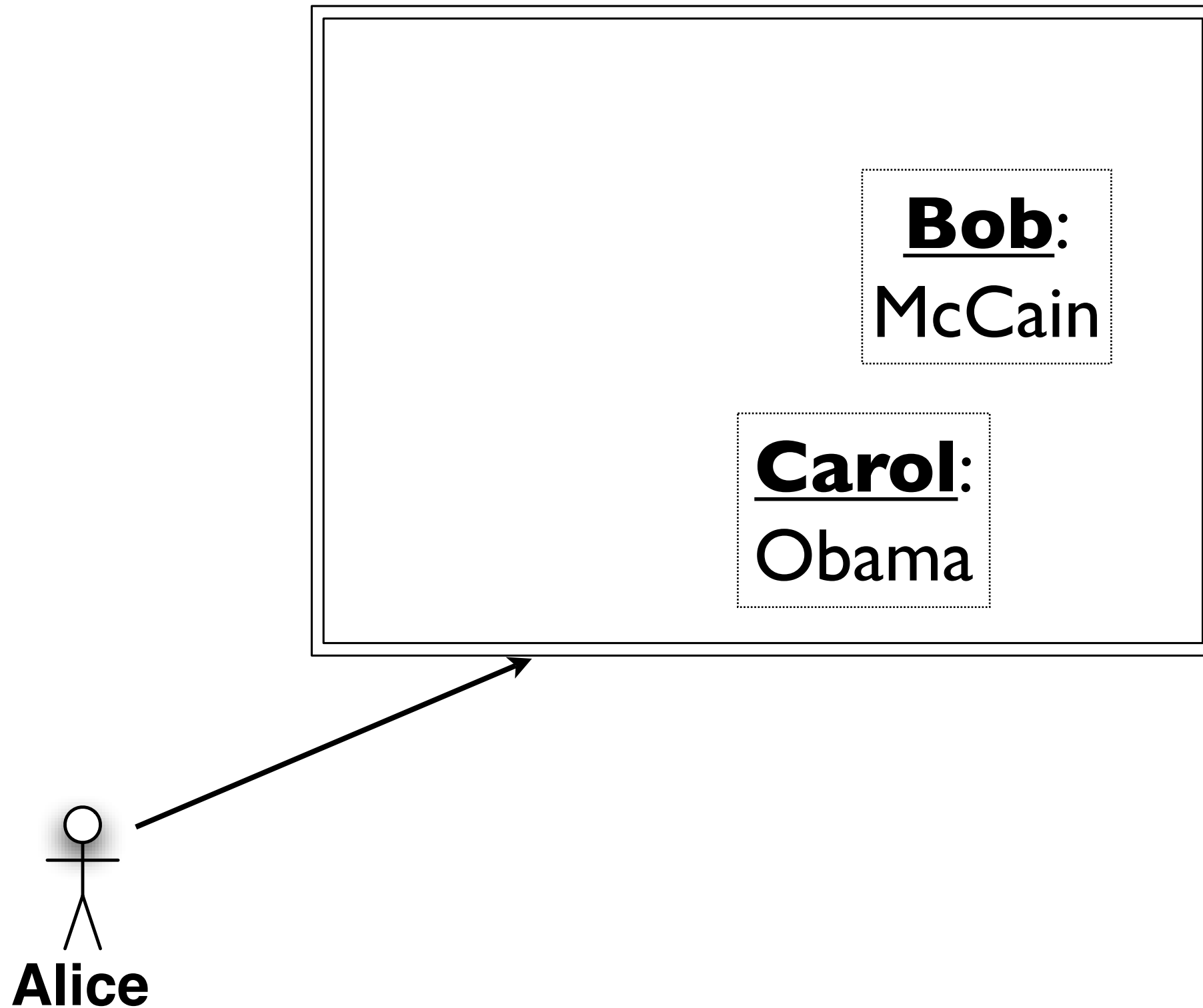
Secrecy + Auditability.



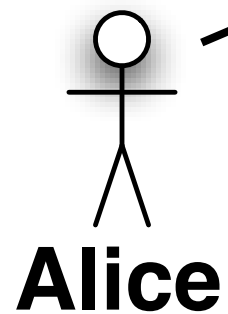
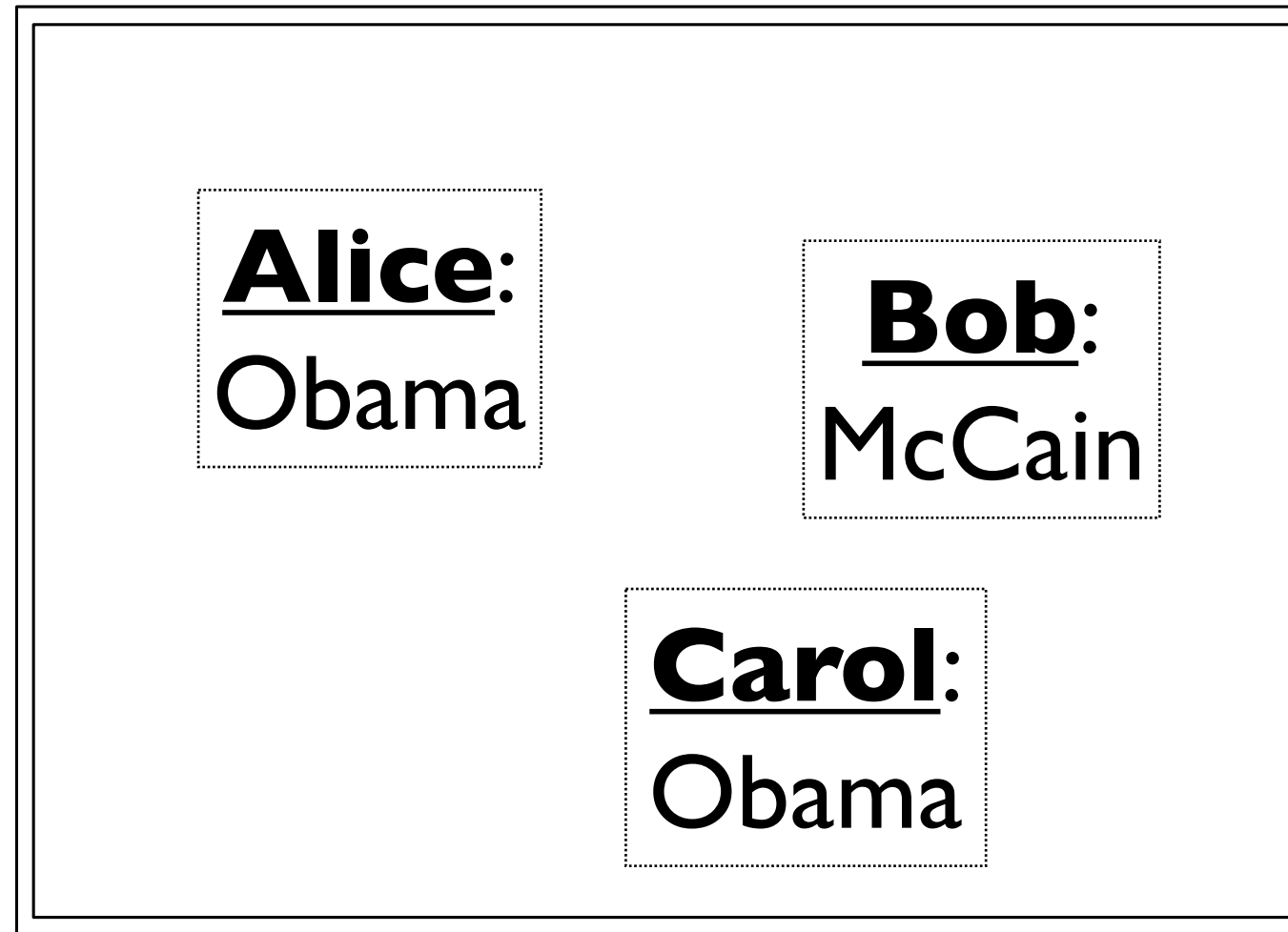
Public Ballots



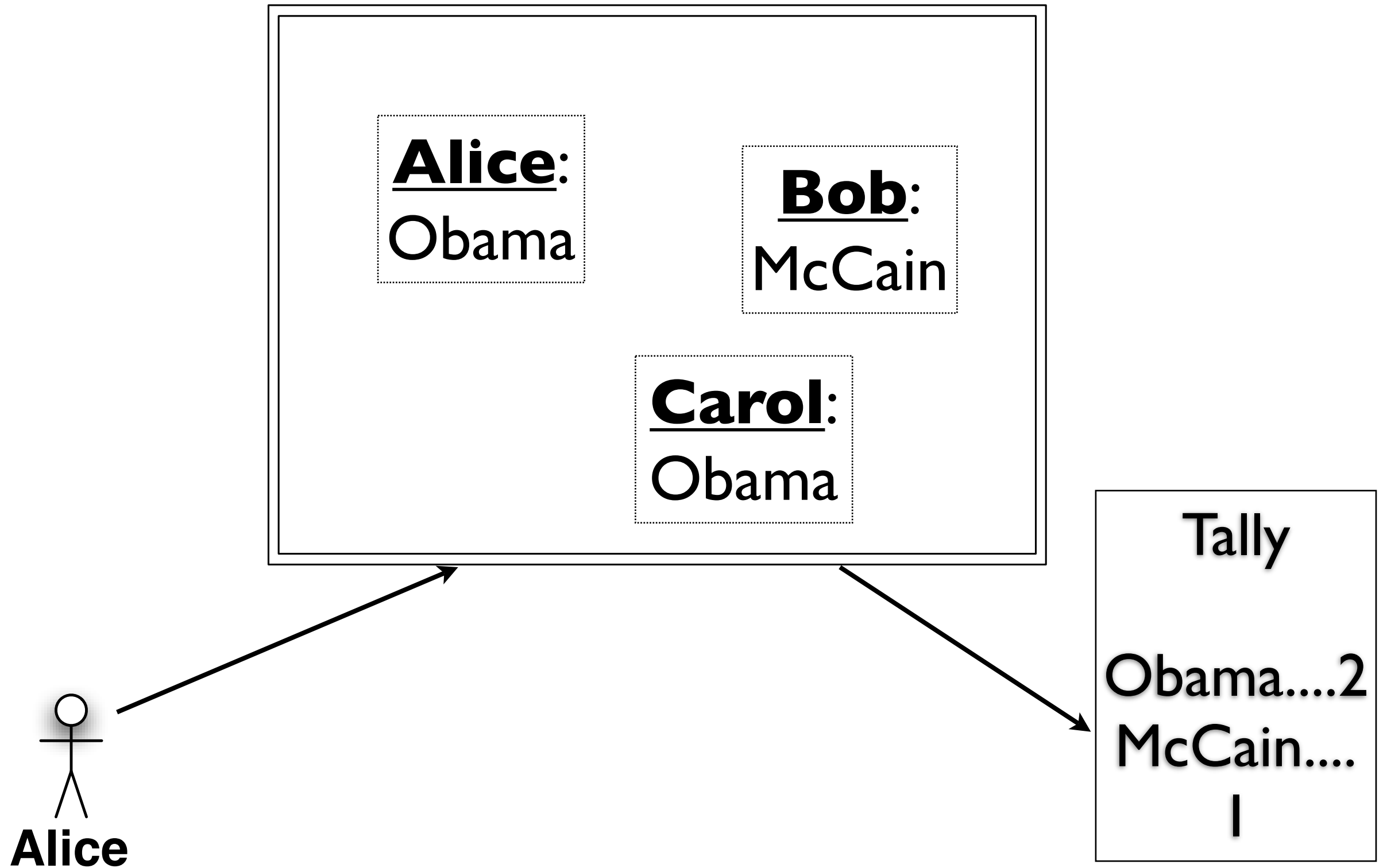
Public Ballots



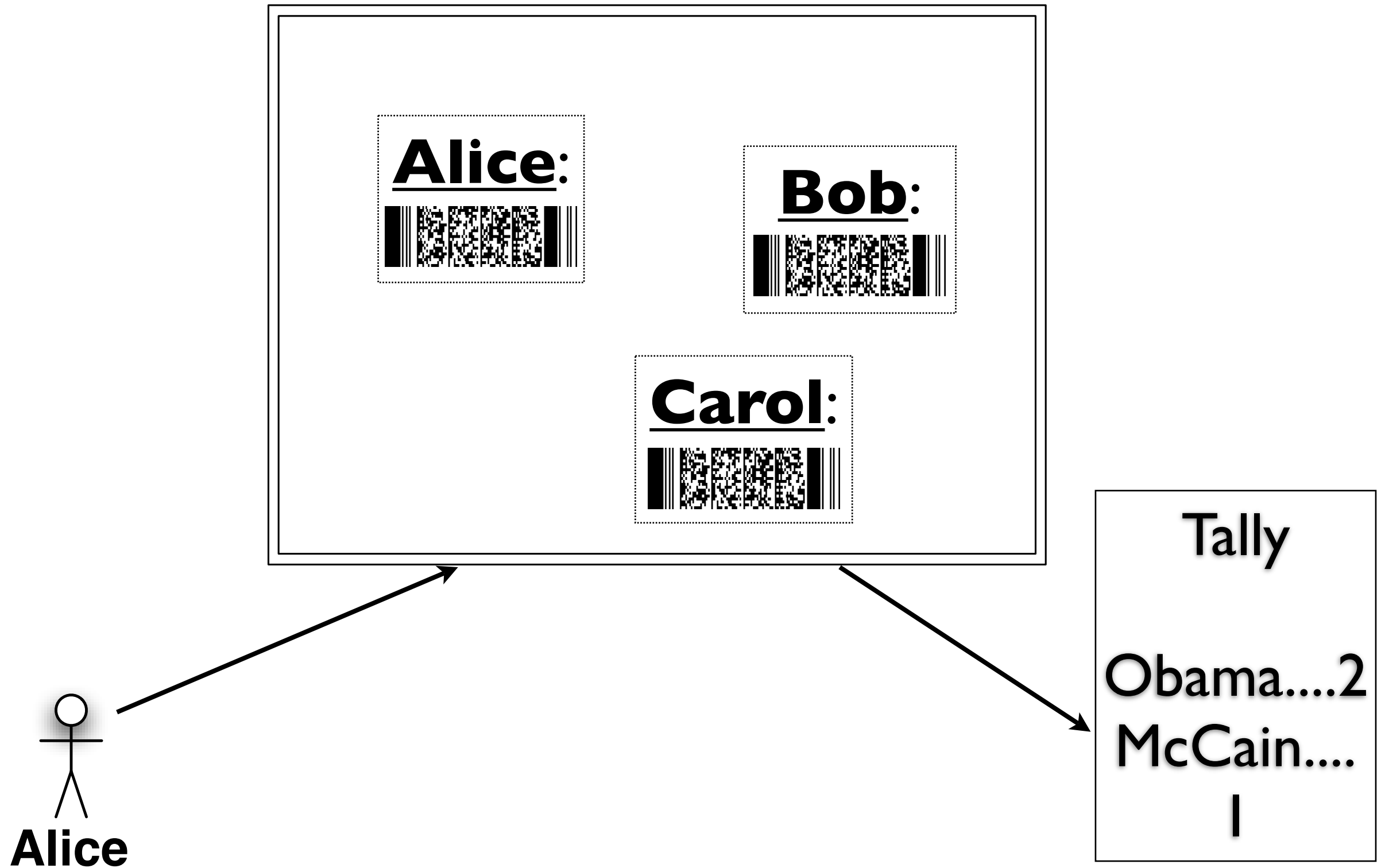
Public Ballots



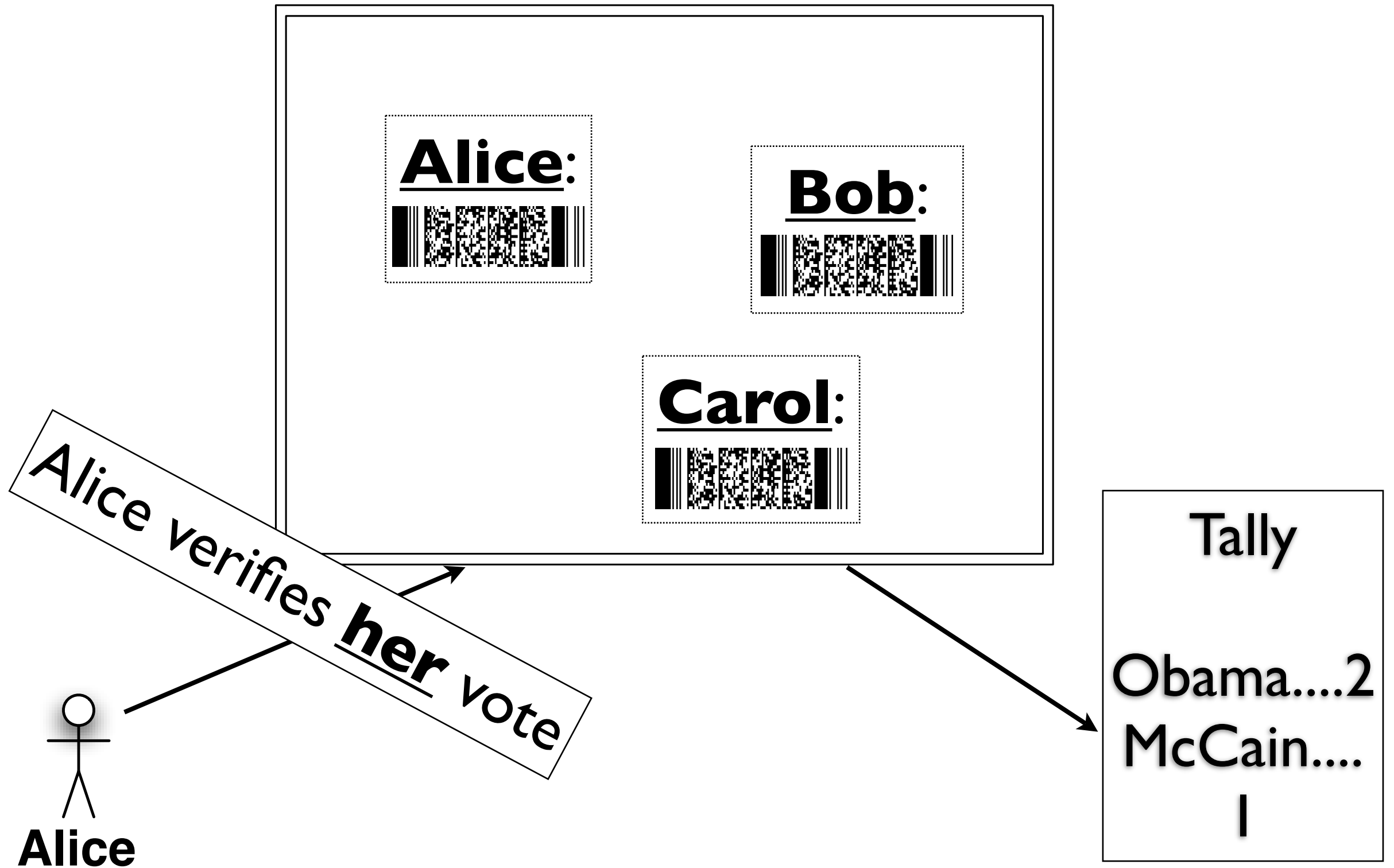
Public Ballots



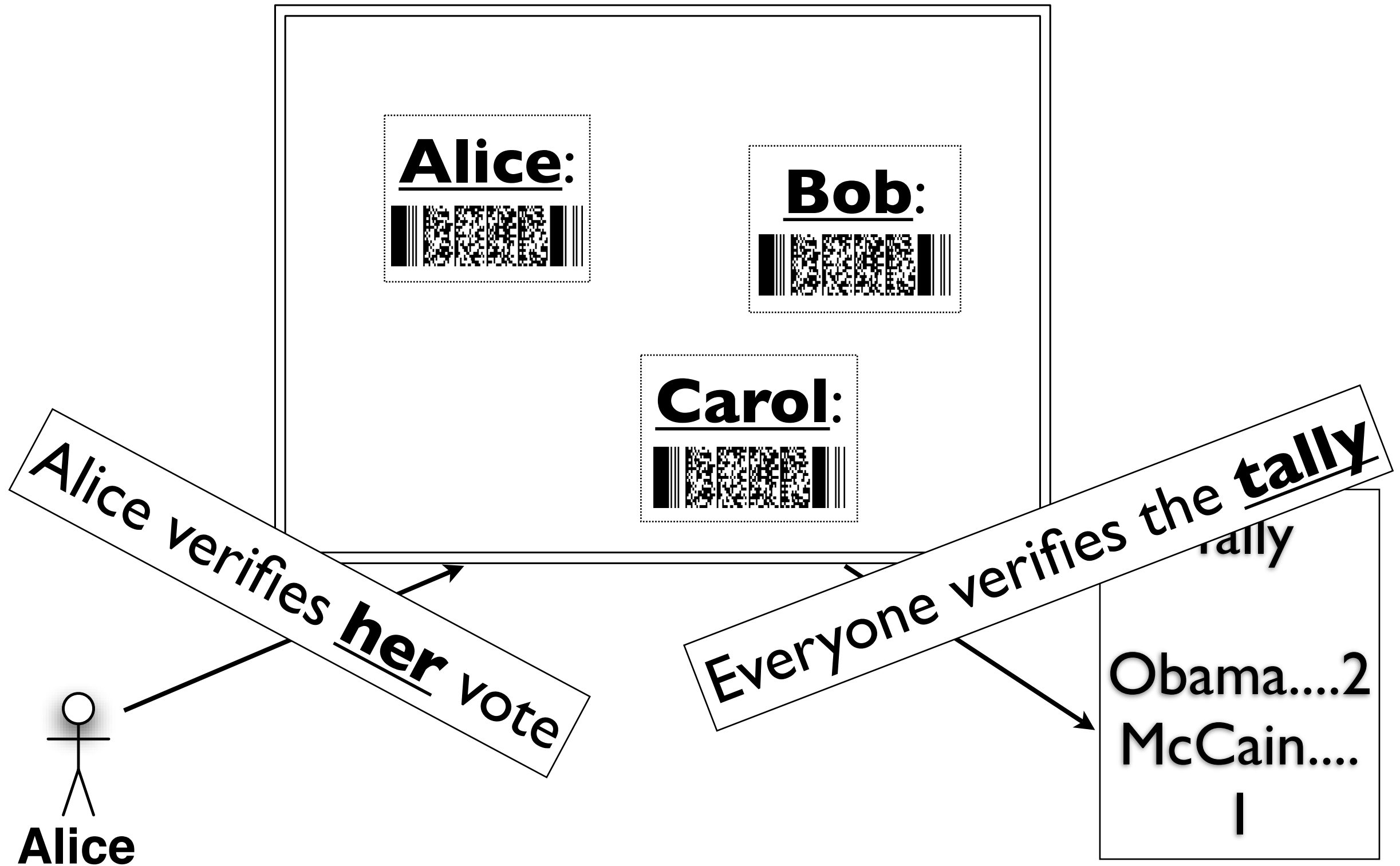
Encrypted Public Ballots



Encrypted Public Ballots

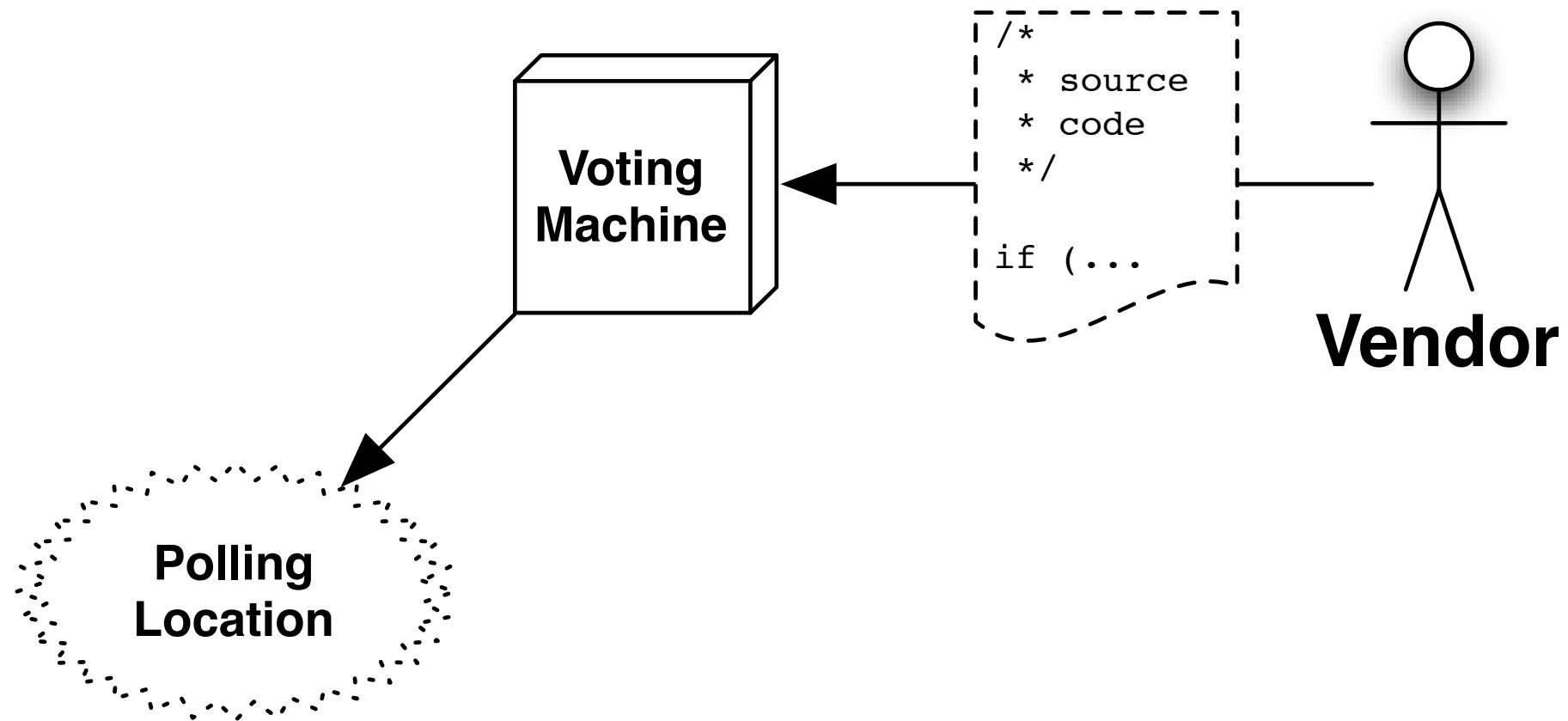


Encrypted Public Ballots

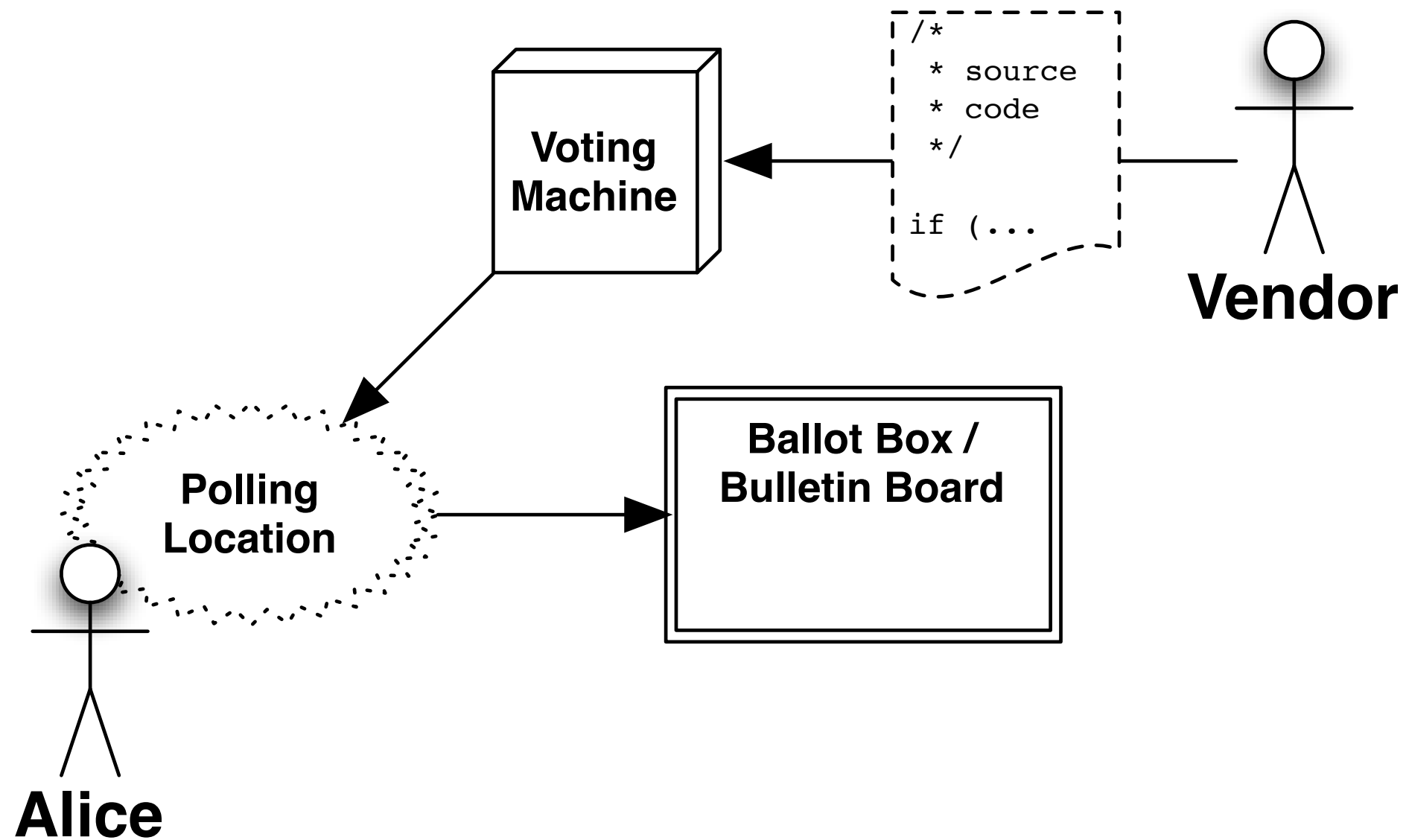


End-to-End Verification

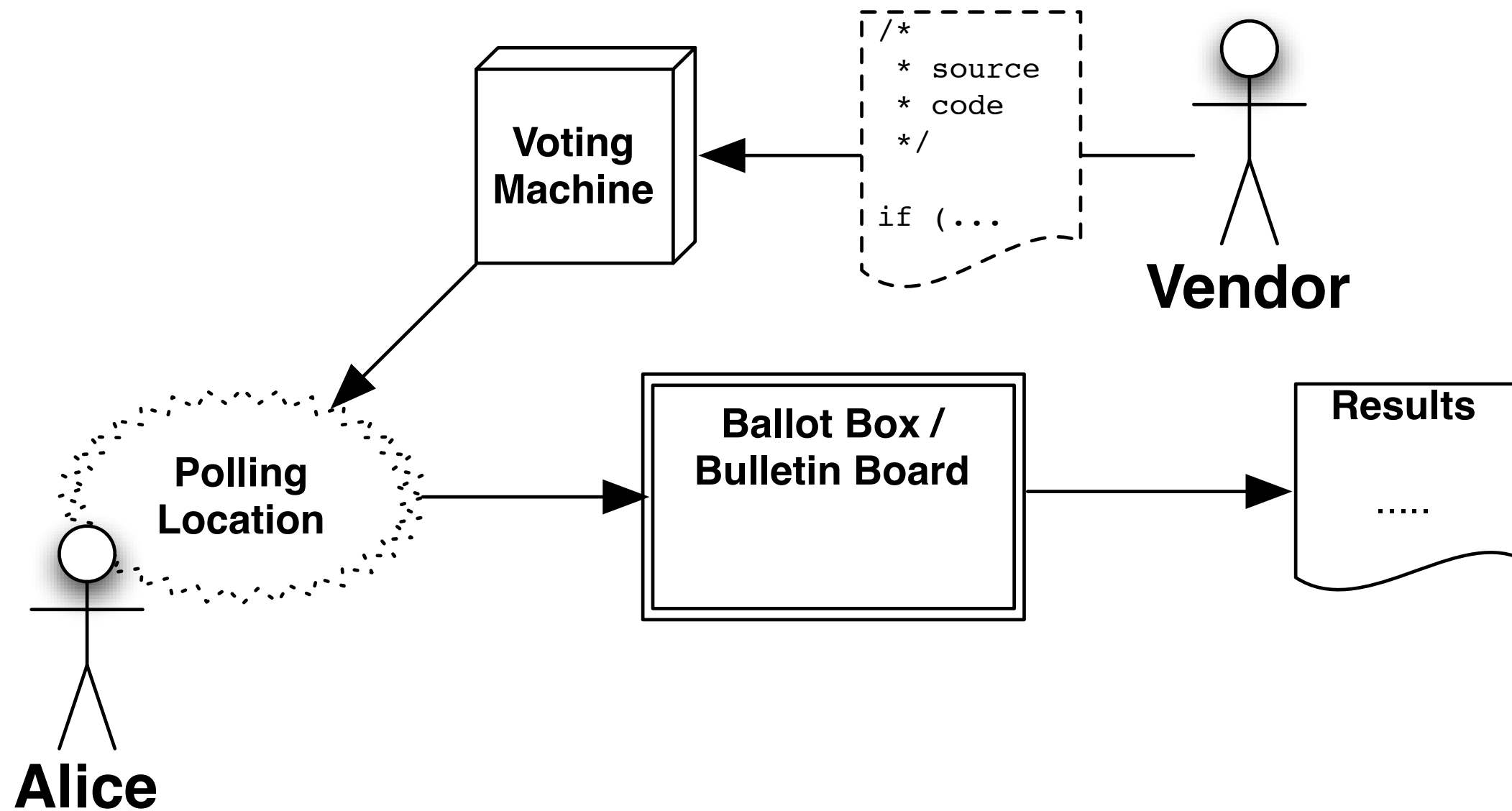
End-to-End Verification



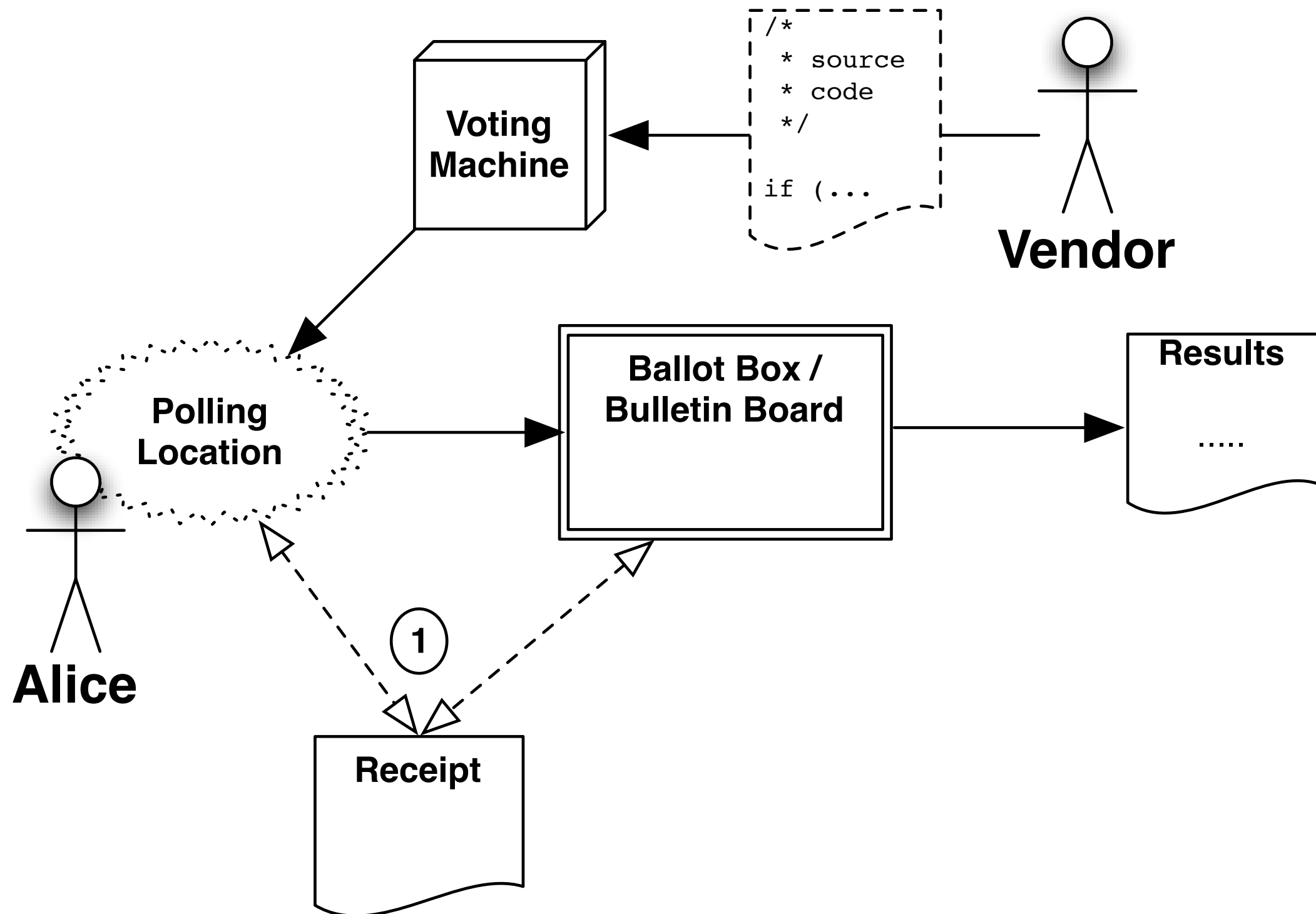
End-to-End Verification



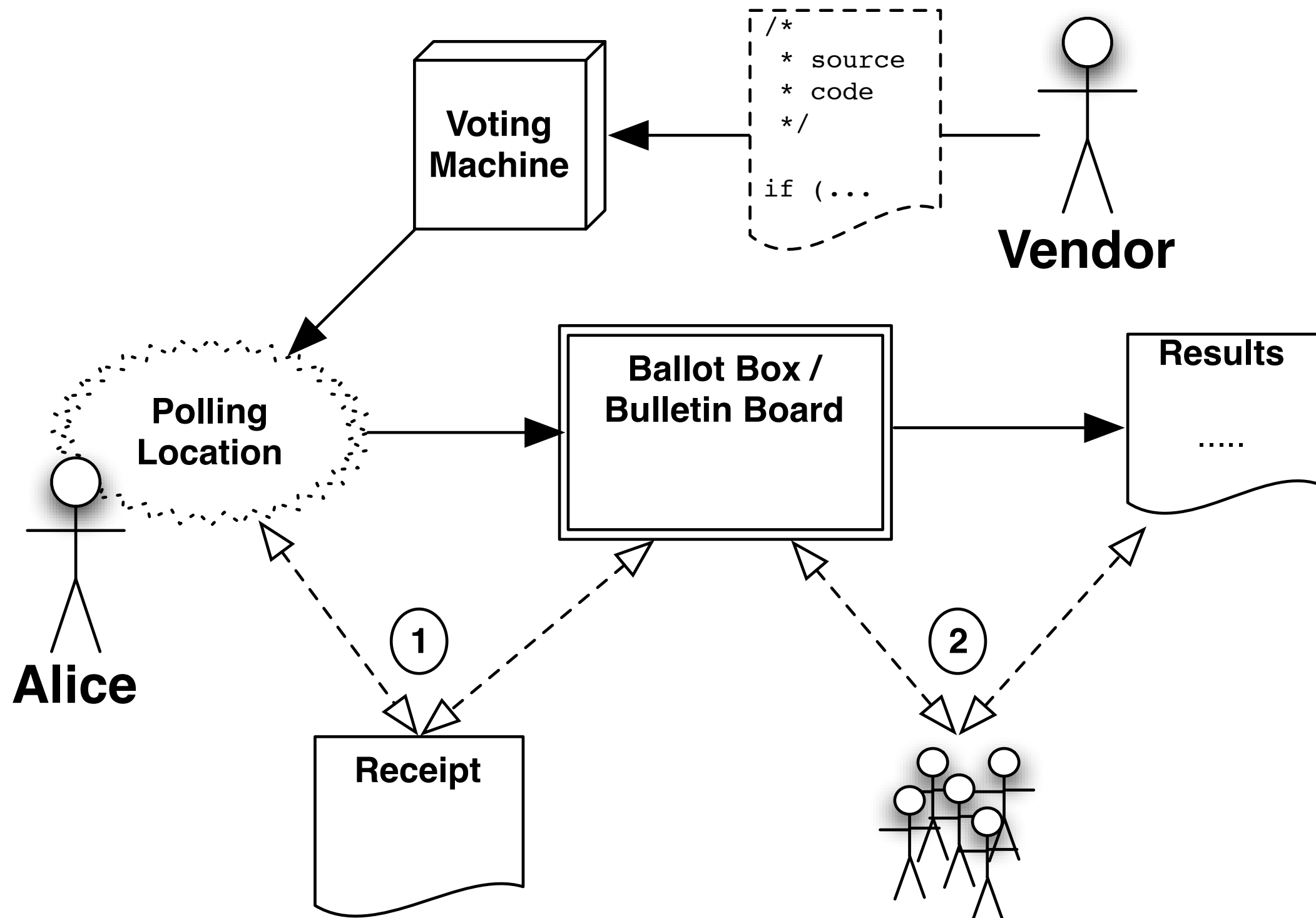
End-to-End Verification



End-to-End Verification



End-to-End Verification



Democratizing Audits

- Each voter is responsible for checking their receipt (no one else can.)
- Anyone, a voter or a public org, can audit the tally and verify the list of cast ballots.
- Thus, OPEN-AUDIT Voting.

2.

Cryptography is not just about secrets, creates trust between competitors.

Voting and encryption

A really secret ballot

Oct 22nd 2008

From Economist.com

Encrypting ballot papers should make elections more secure

NO!

Increased transparency
when some data
must remain secret.

So, yes, we encrypt,
and then we operate on the
encrypted data in public, so
everyone can see.

In particular, because the vote
is encrypted, it can remain
labeled with voter's name.

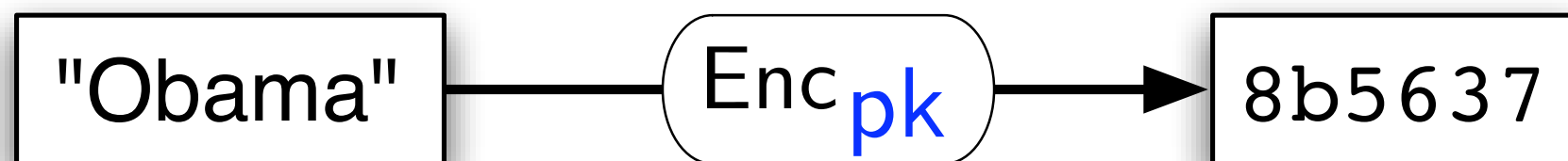
“Randomized” Encryption

“Randomized” Encryption

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

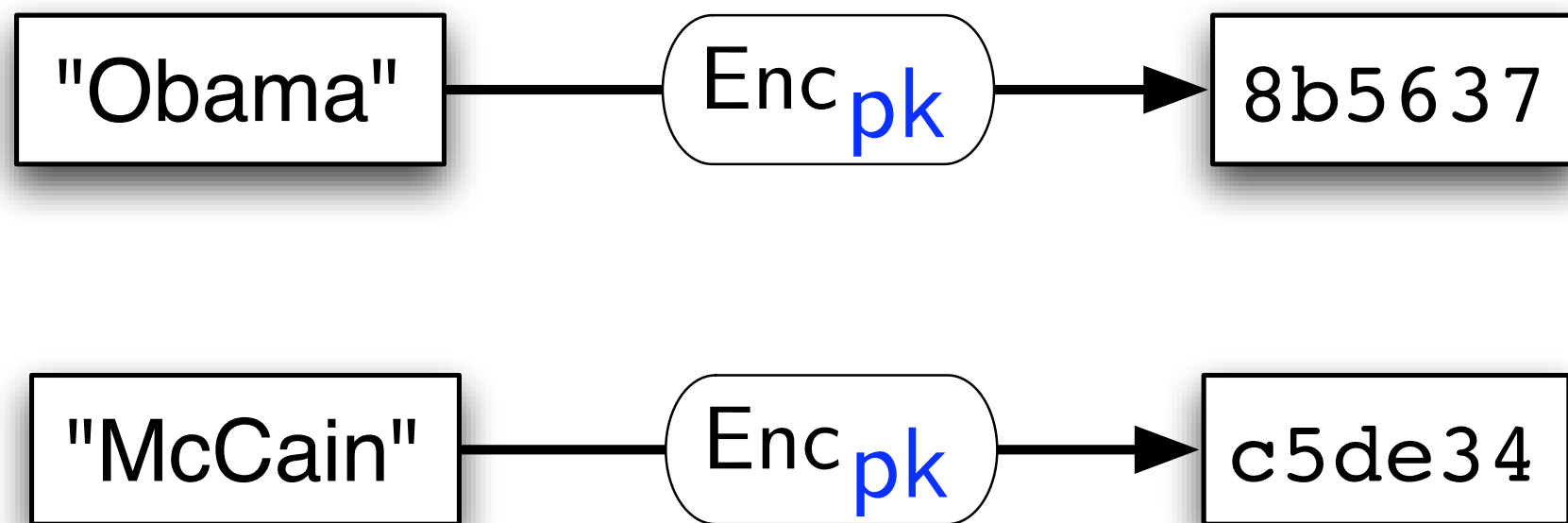
“Randomized” Encryption

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



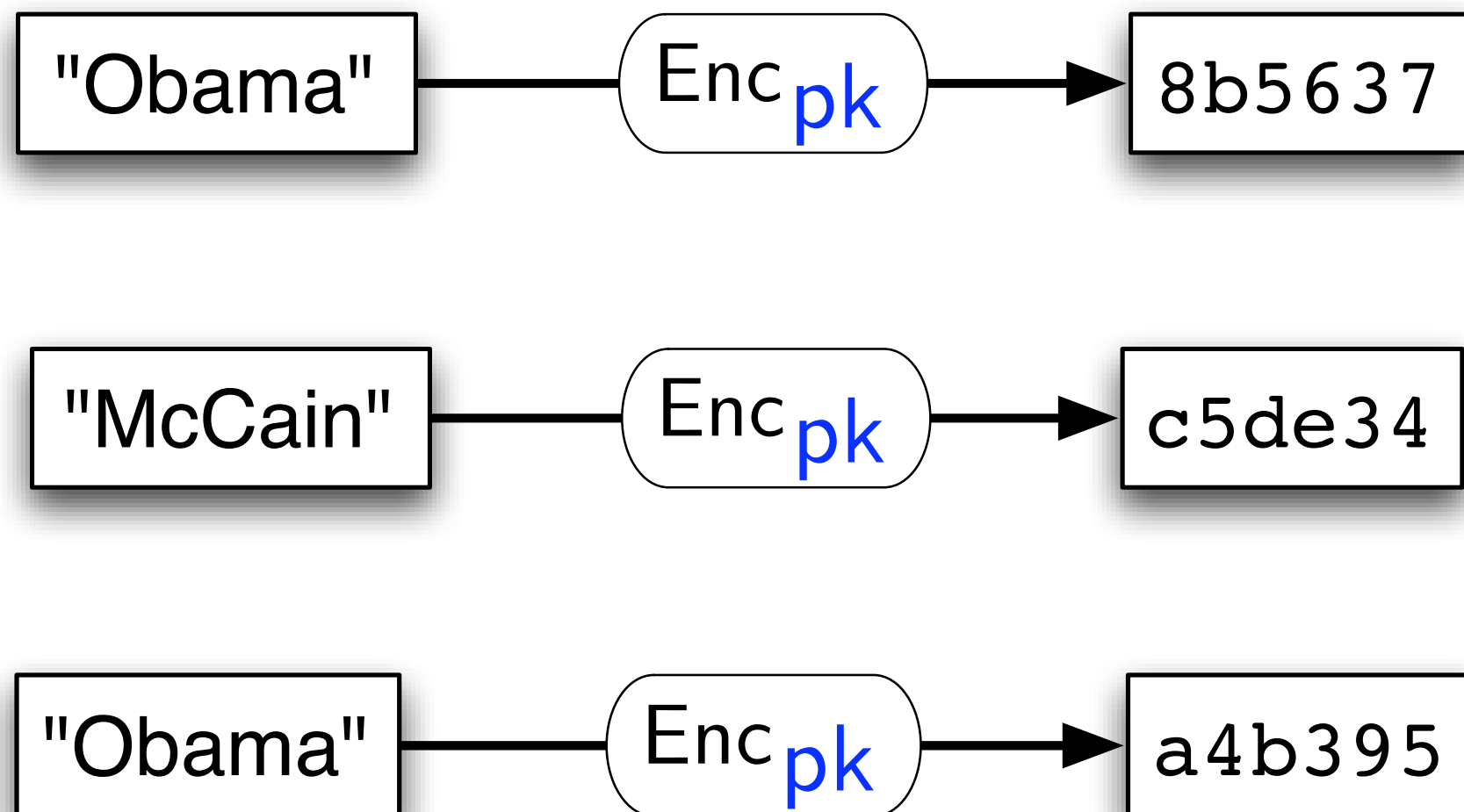
“Randomized” Encryption

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



“Randomized” Encryption

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



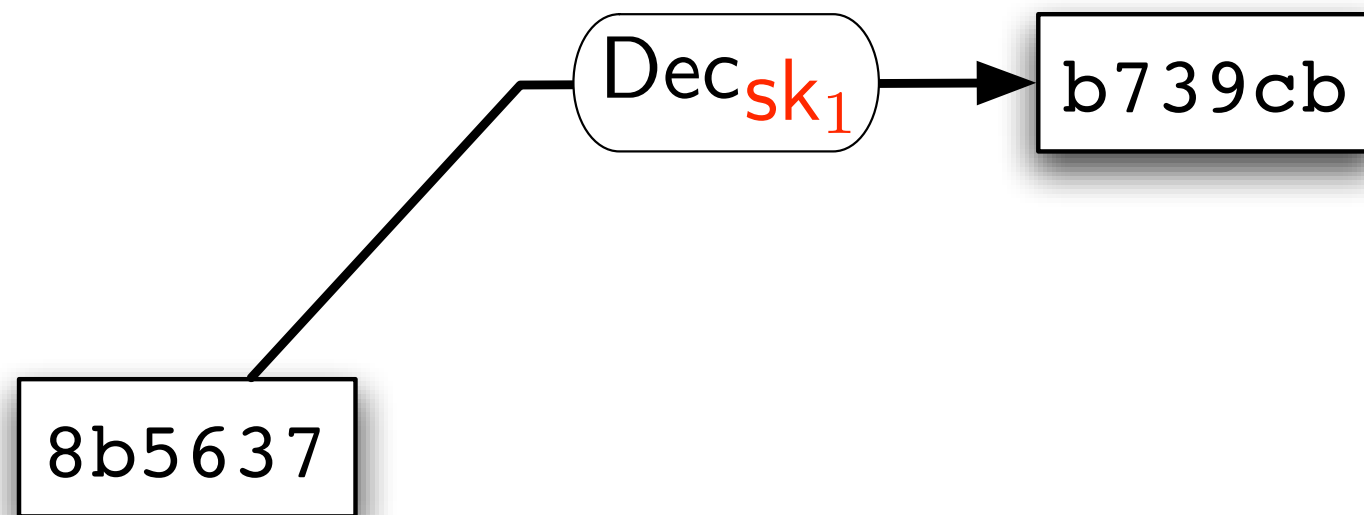
Threshold Decryption

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

8b5637

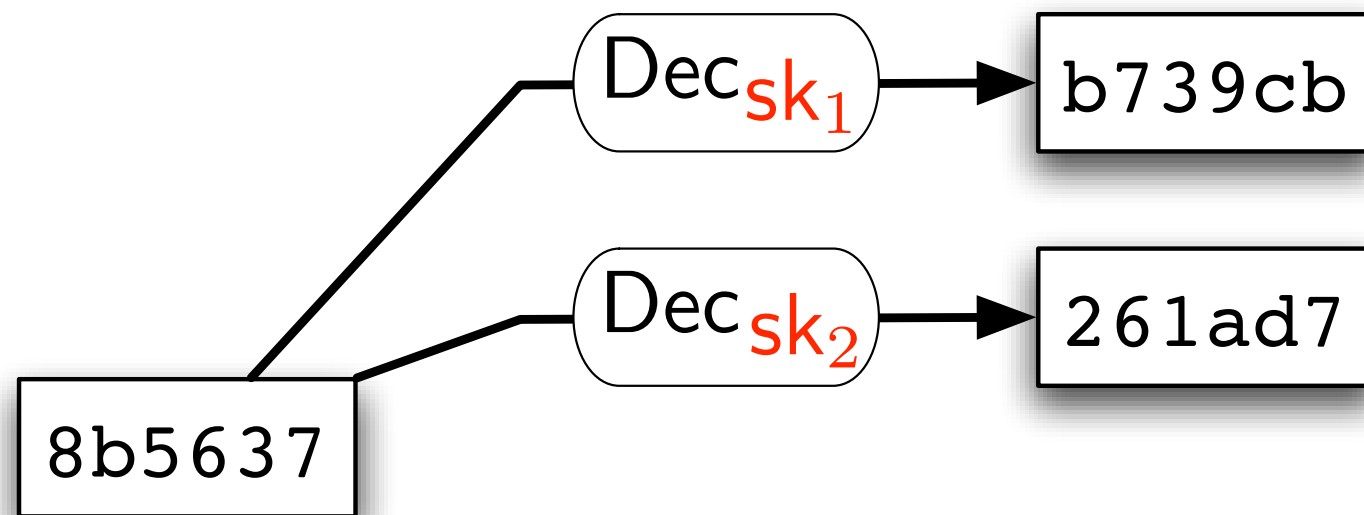
Threshold Decryption

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



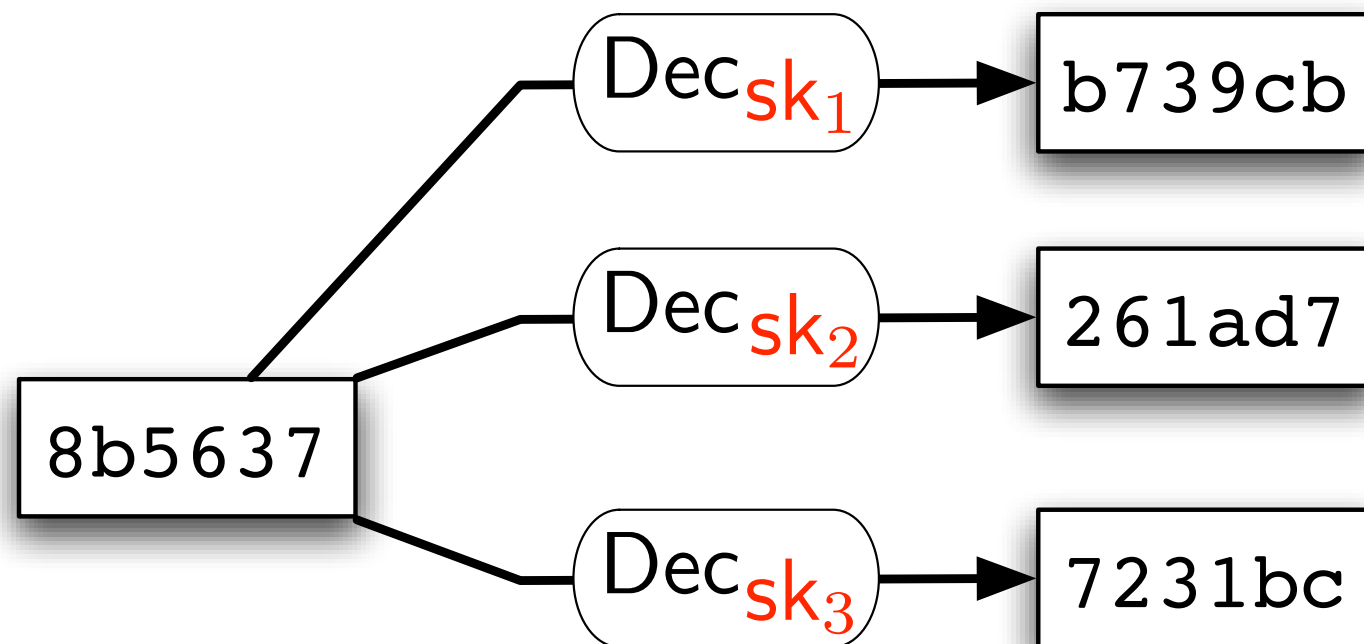
Threshold Decryption

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



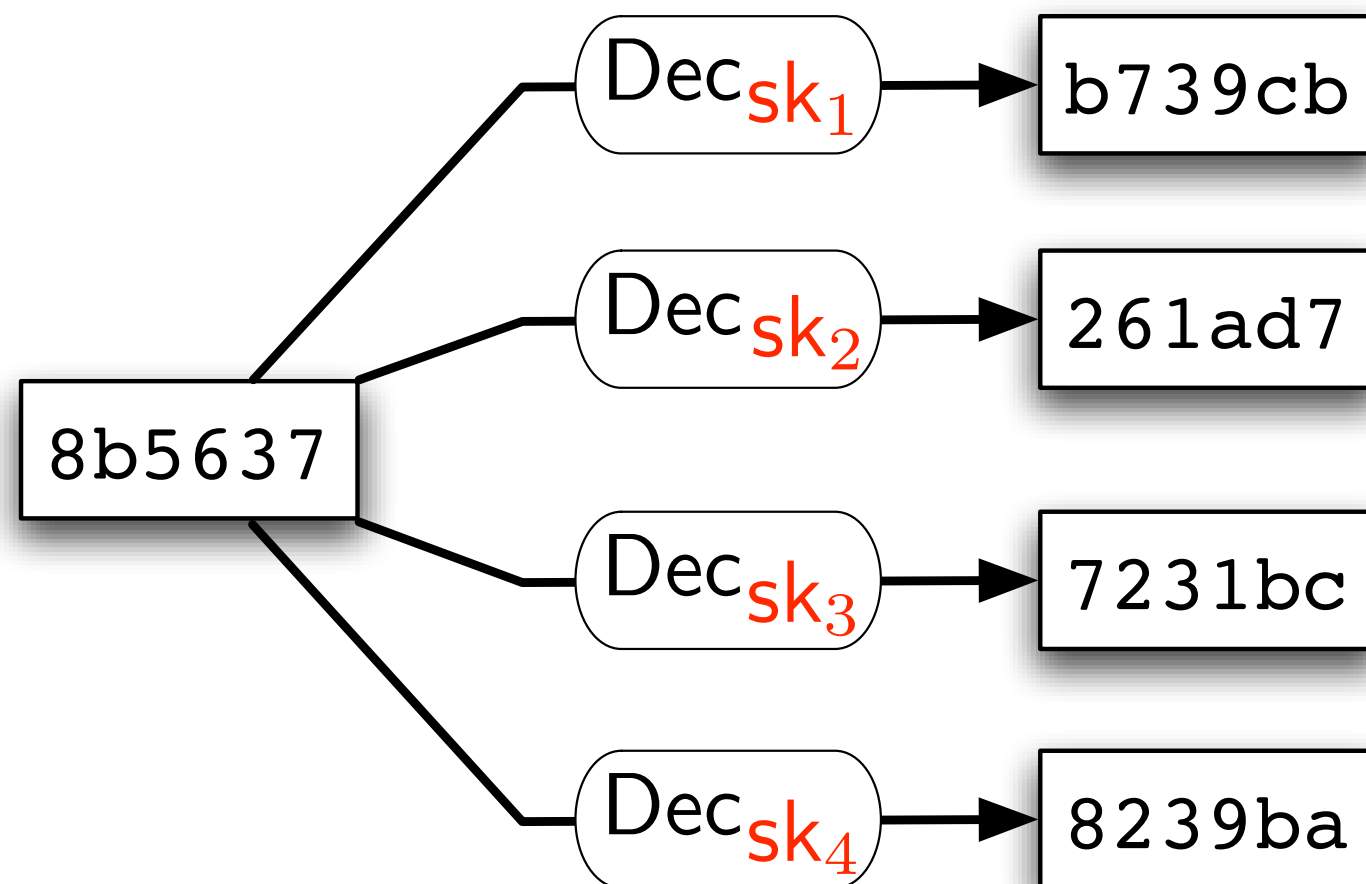
Threshold Decryption

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



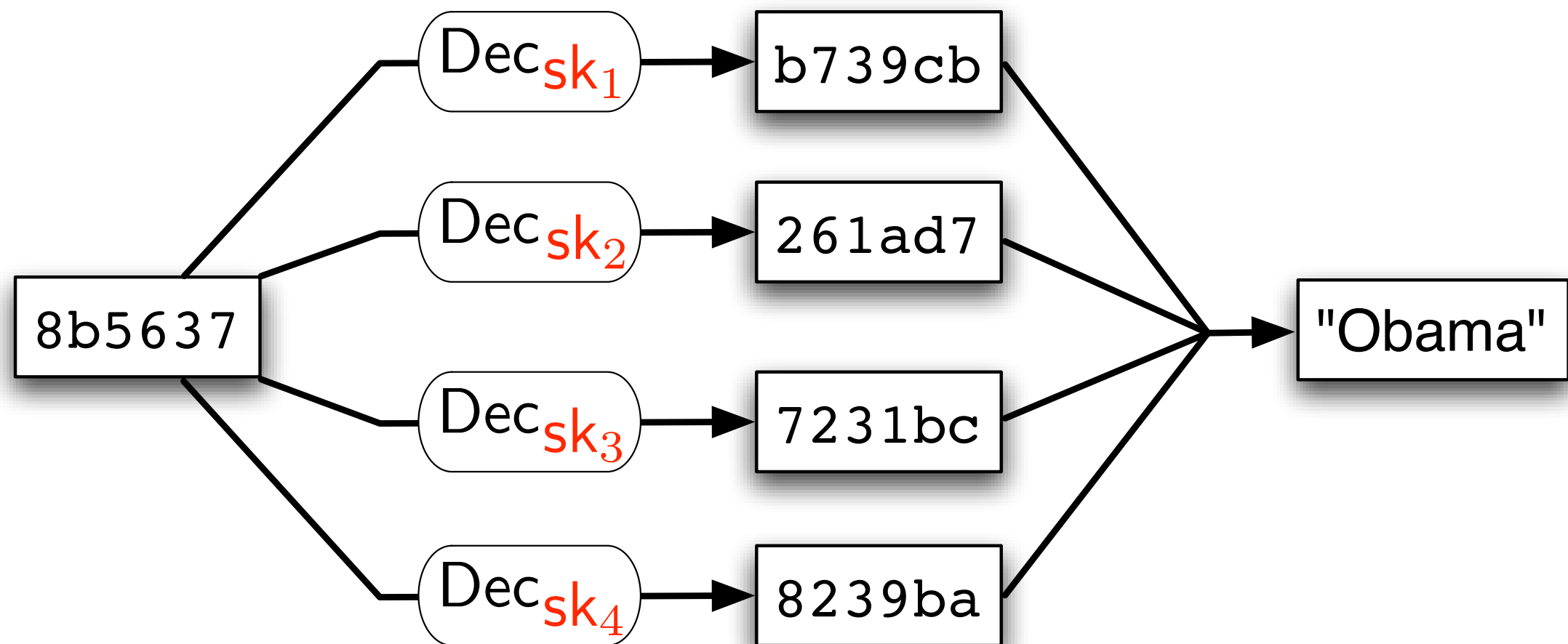
Threshold Decryption

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.

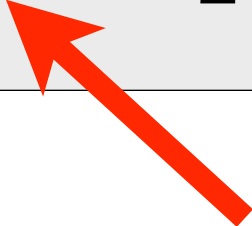


Homomorphic Encryption

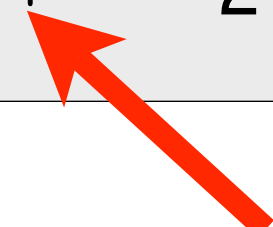
Homomorphic Encryption

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

Homomorphic Encryption

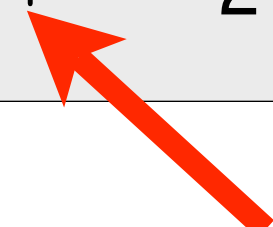
$$\text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 + m_2)$$


Homomorphic Encryption

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


$$g^{m_1} \times g^{m_2} = g^{m_1 + m_2}$$

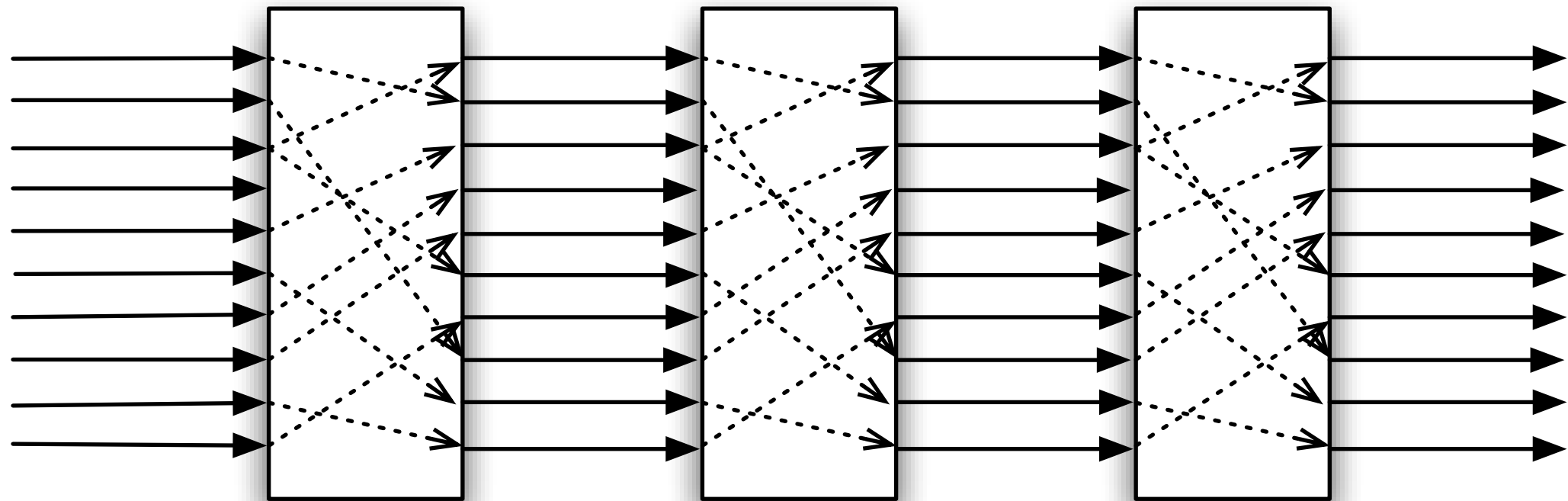
Homomorphic Encryption

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


$$g^{m_1} \times g^{m_2} = g^{m_1 + m_2}$$

then we can simply
add “under cover” of encryption!

Mixnets



$$c = \text{Enc}_{pk_1} (\text{Enc}_{pk_2} (\text{Enc}_{pk_3} (m)))$$

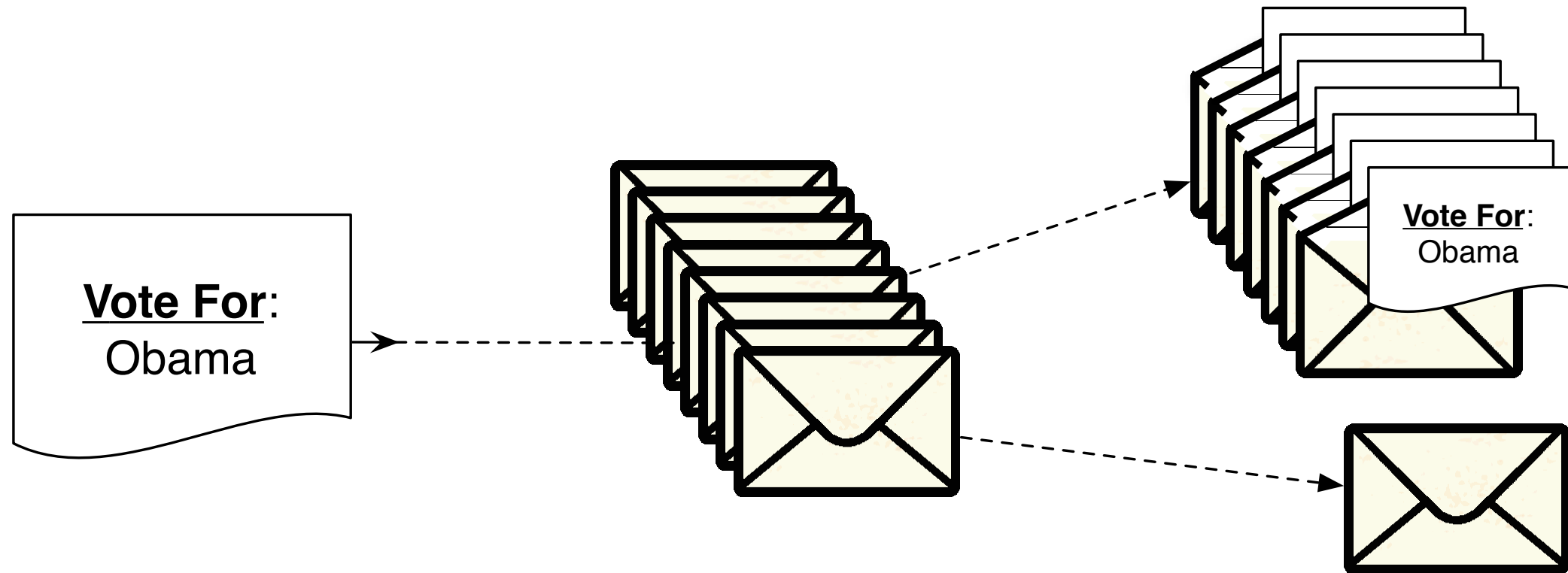
Each mix server “unwraps”
a layer of this encryption onion.

Proving certain details while
keeping others secret.

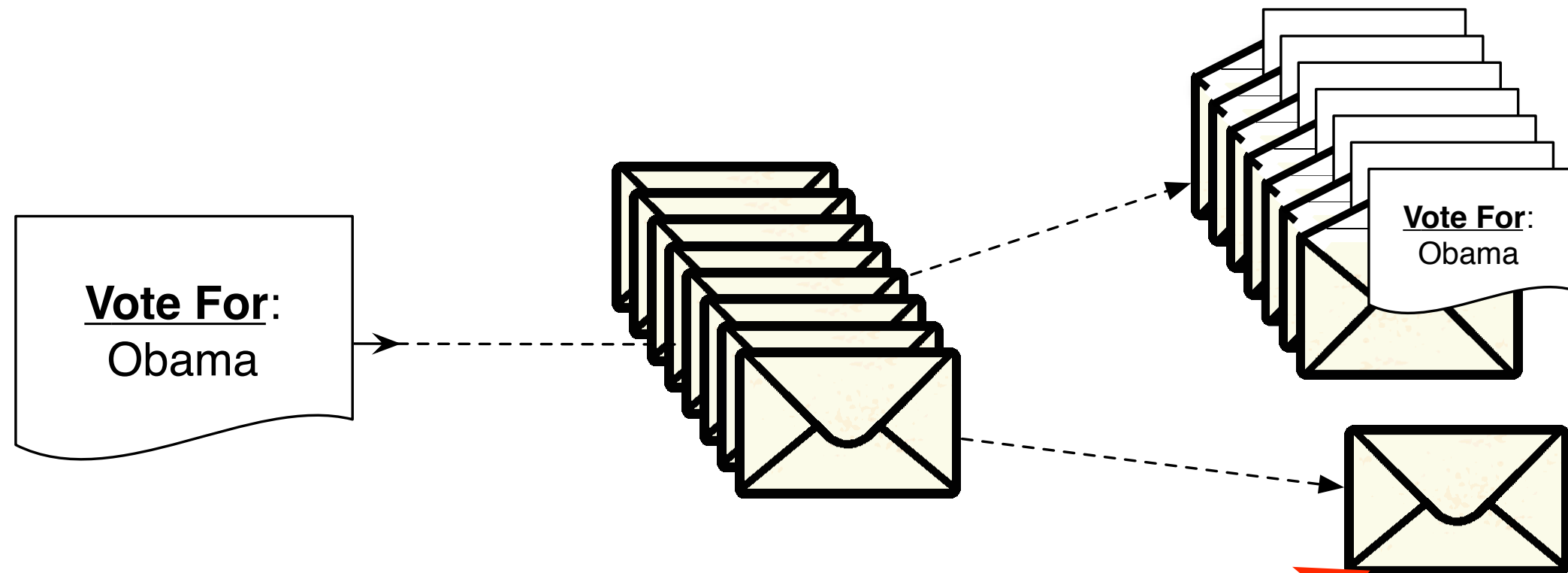
Proving a ciphertext
encodes a given message
without revealing
its random factor.

Zero-Knowledge Proof

Zero-Knowledge Proof

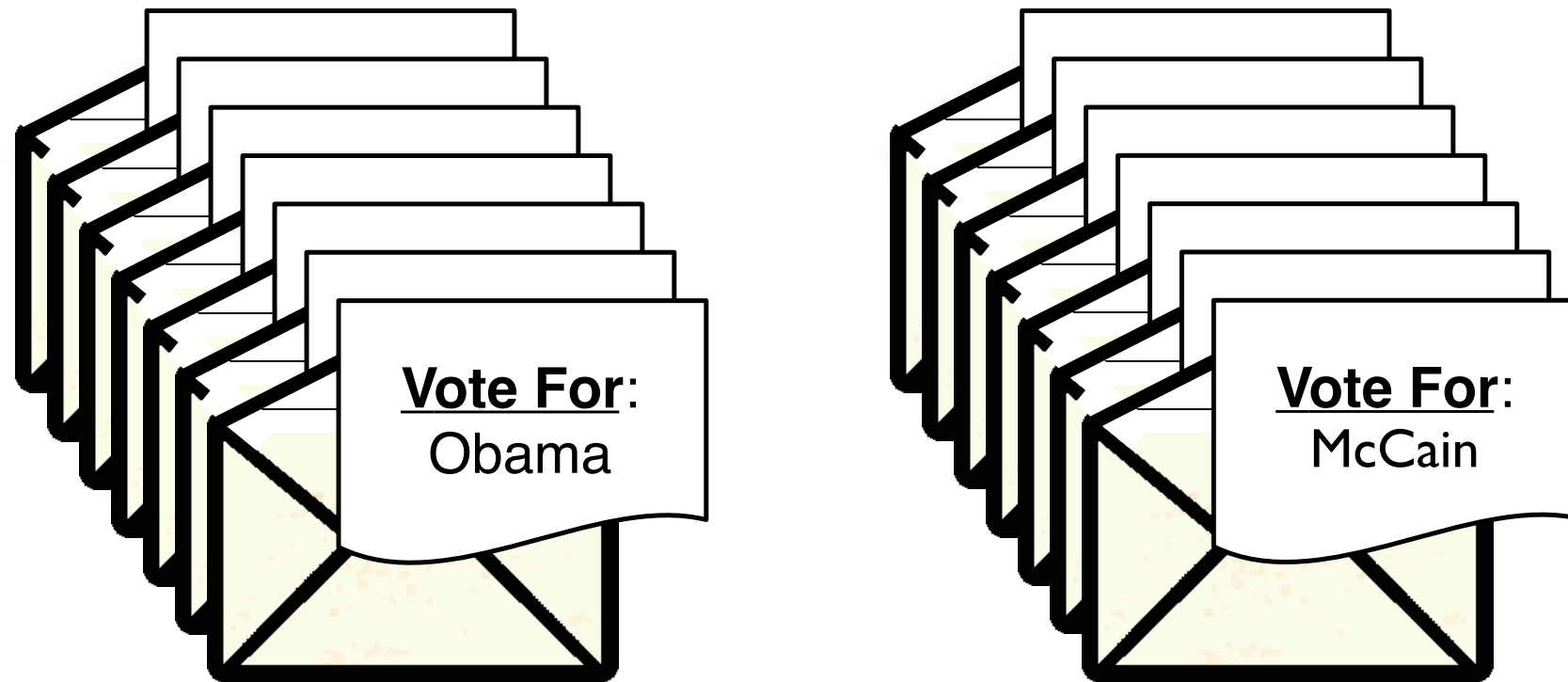


Zero-Knowledge Proof



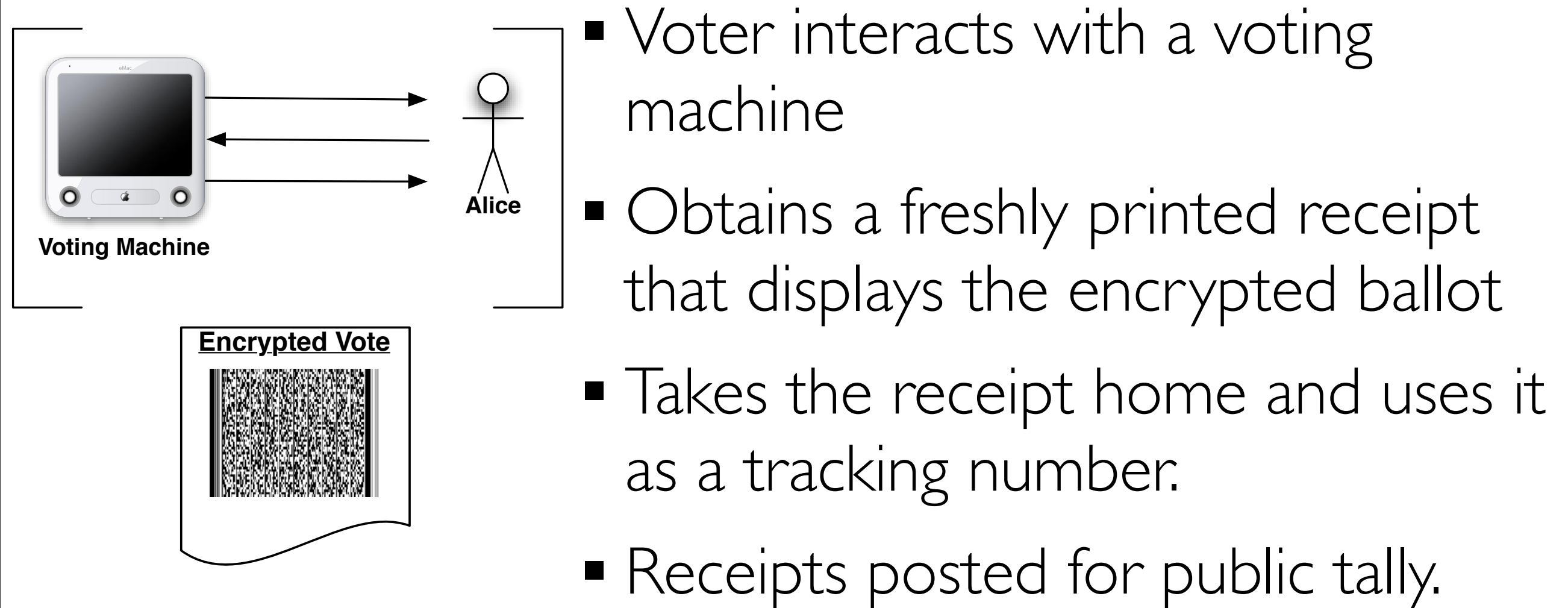
This last envelope likely contains "Obama"

Zero-Knowledge Proof

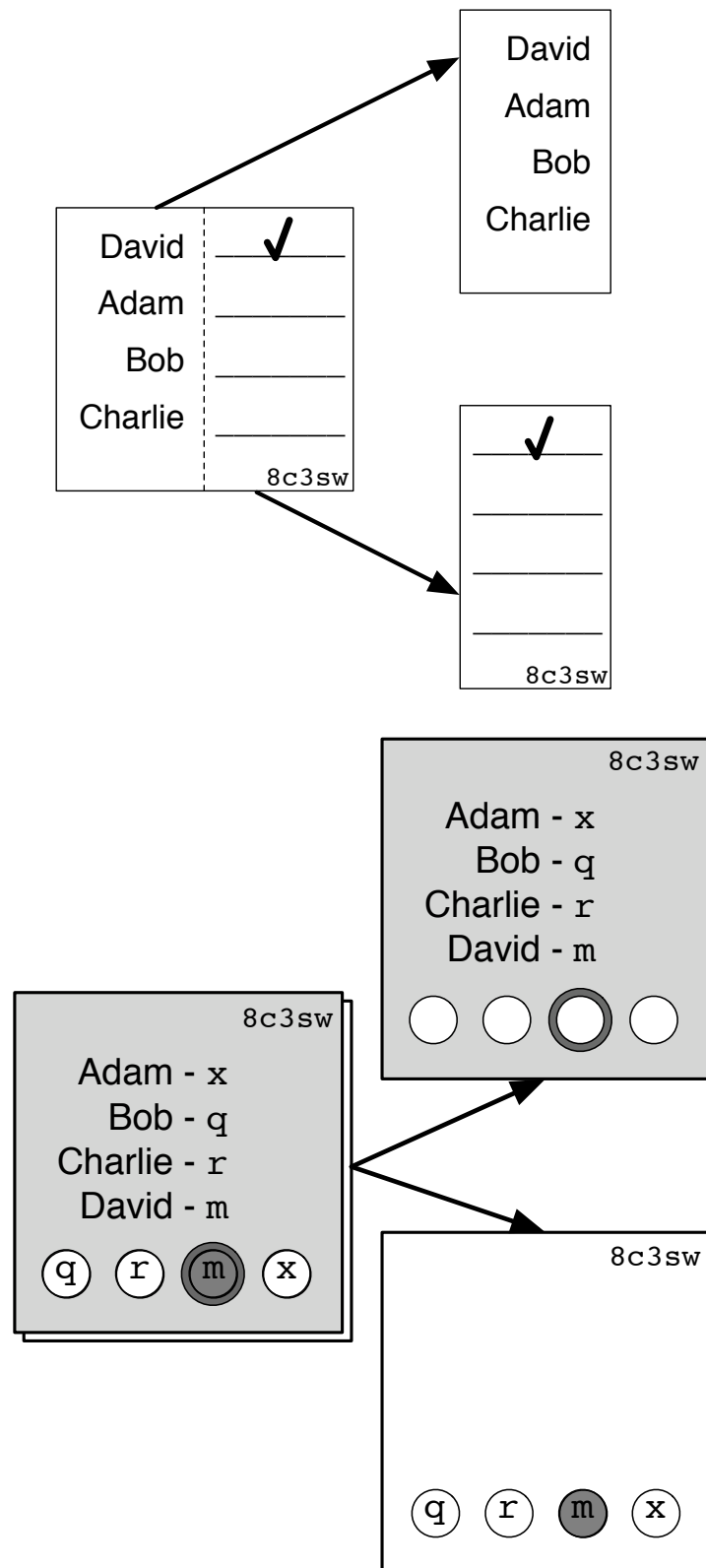


Open envelopes don't prove anything after the fact.

Electronic Experience



Paper Experience



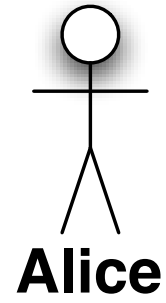
- Pre-print paper ballots with some indirection betw candidate and choice
- Break the indirection (tear, detach) for effective encryption
- Take receipt home and use it as tracking number.
- Receipts posted for public tally.

3.

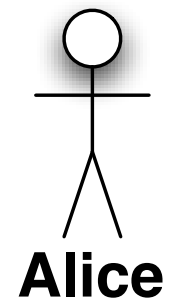
Cryptography-based Voting
(Open-Audit Voting)
is closing in on practicality.

Benaloh Casting

Benaloh Casting



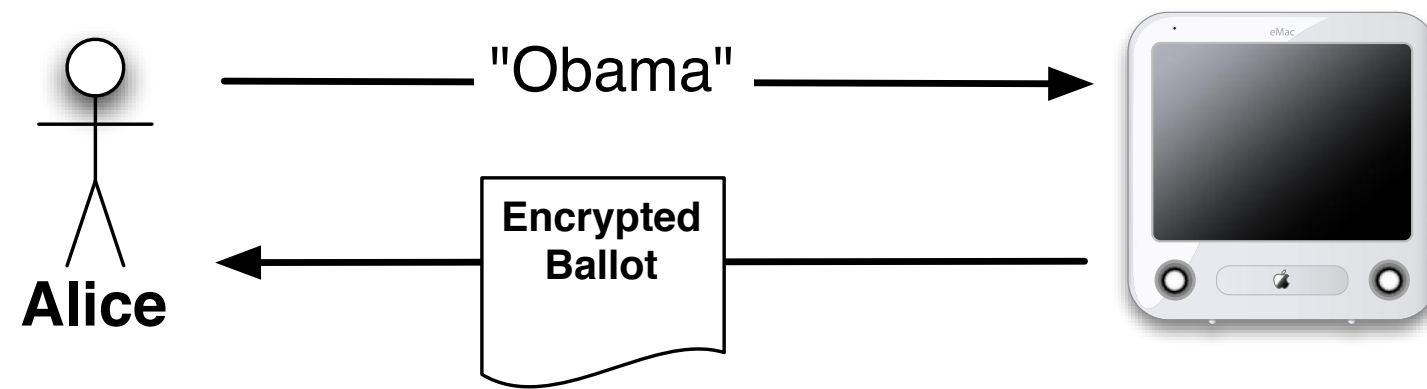
Benaloh Casting



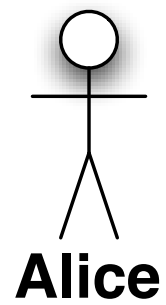
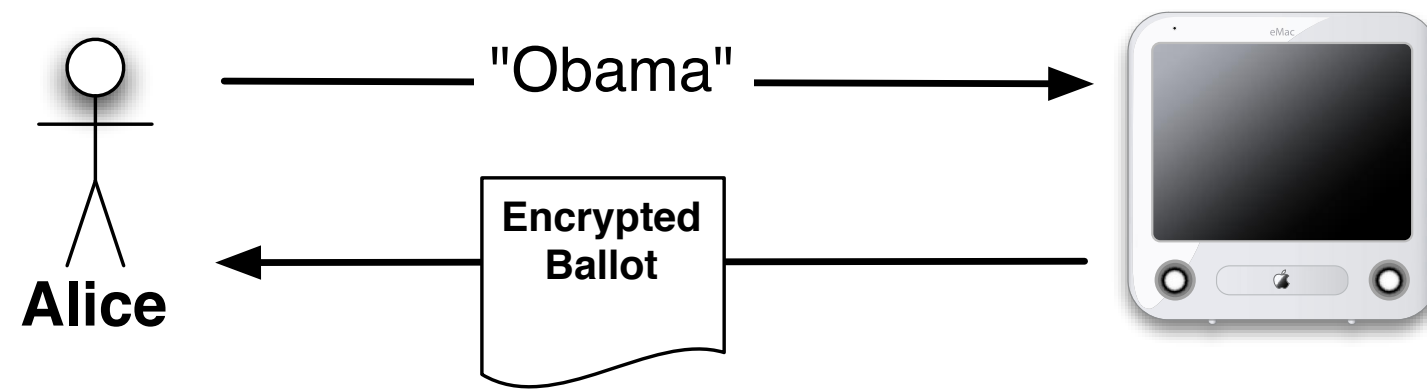
—————"Obama"————→



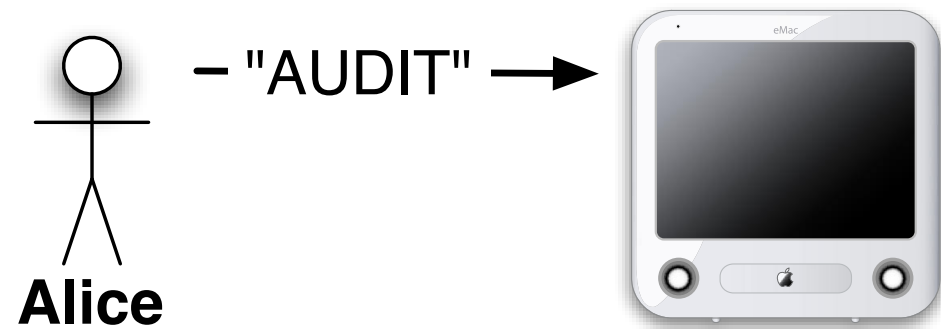
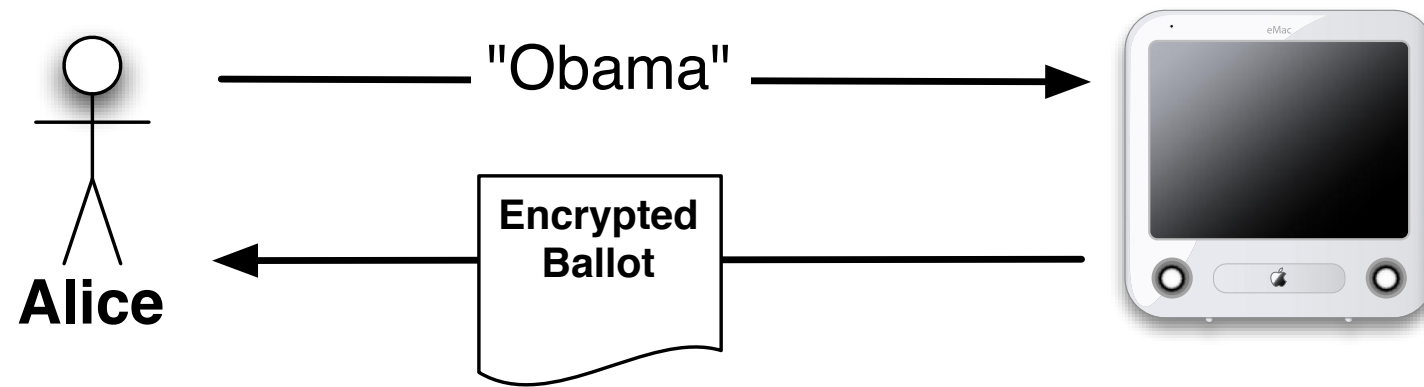
Benaloh Casting



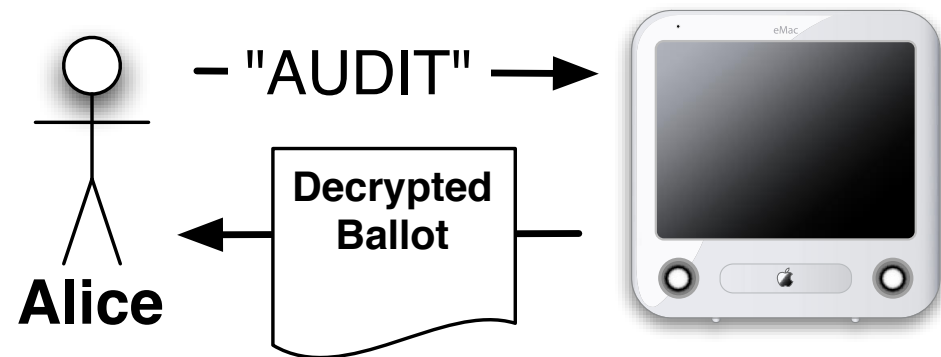
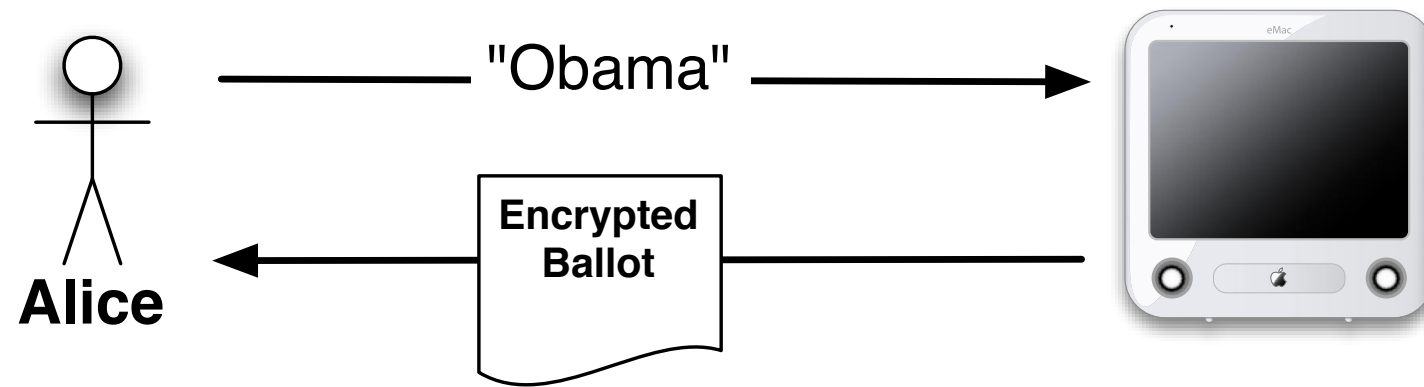
Benaloh Casting



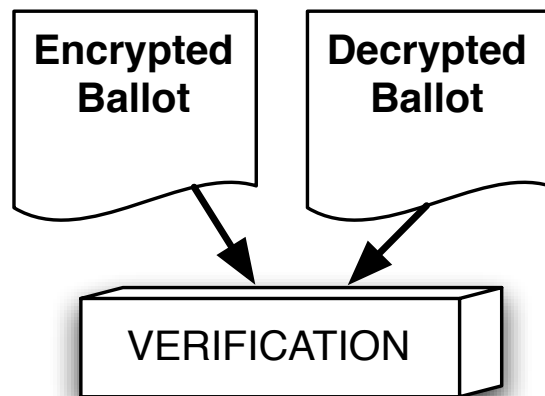
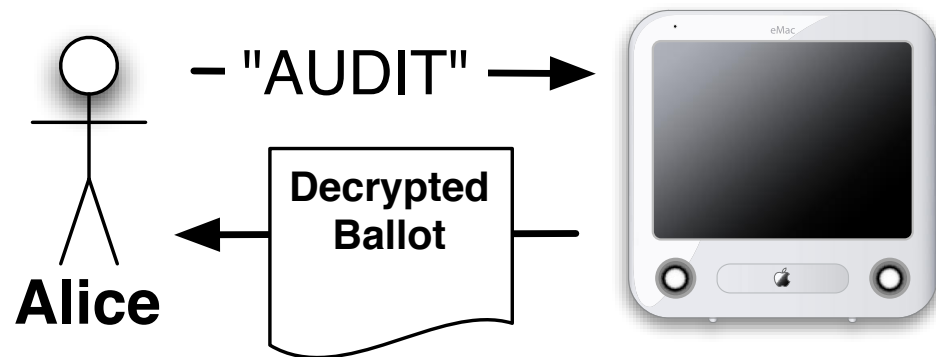
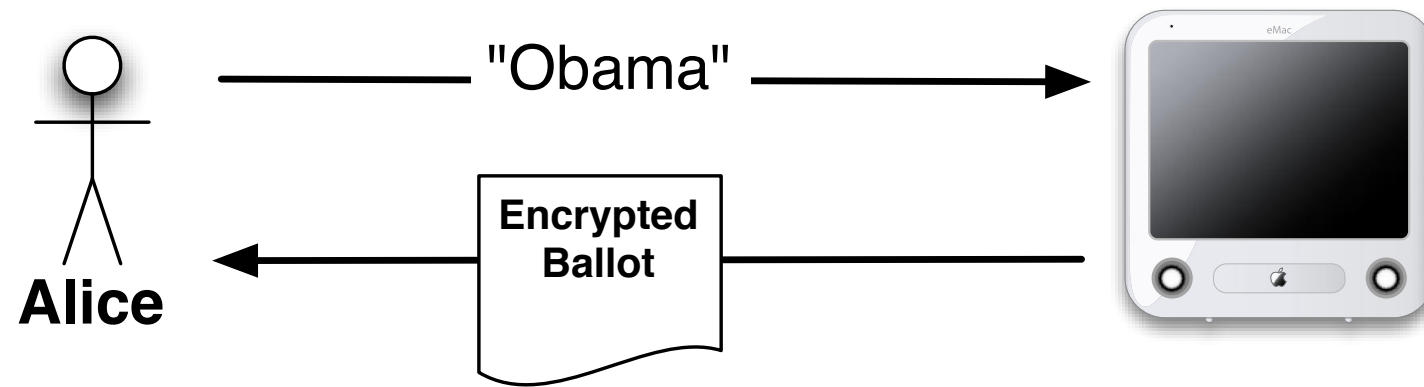
Benaloh Casting



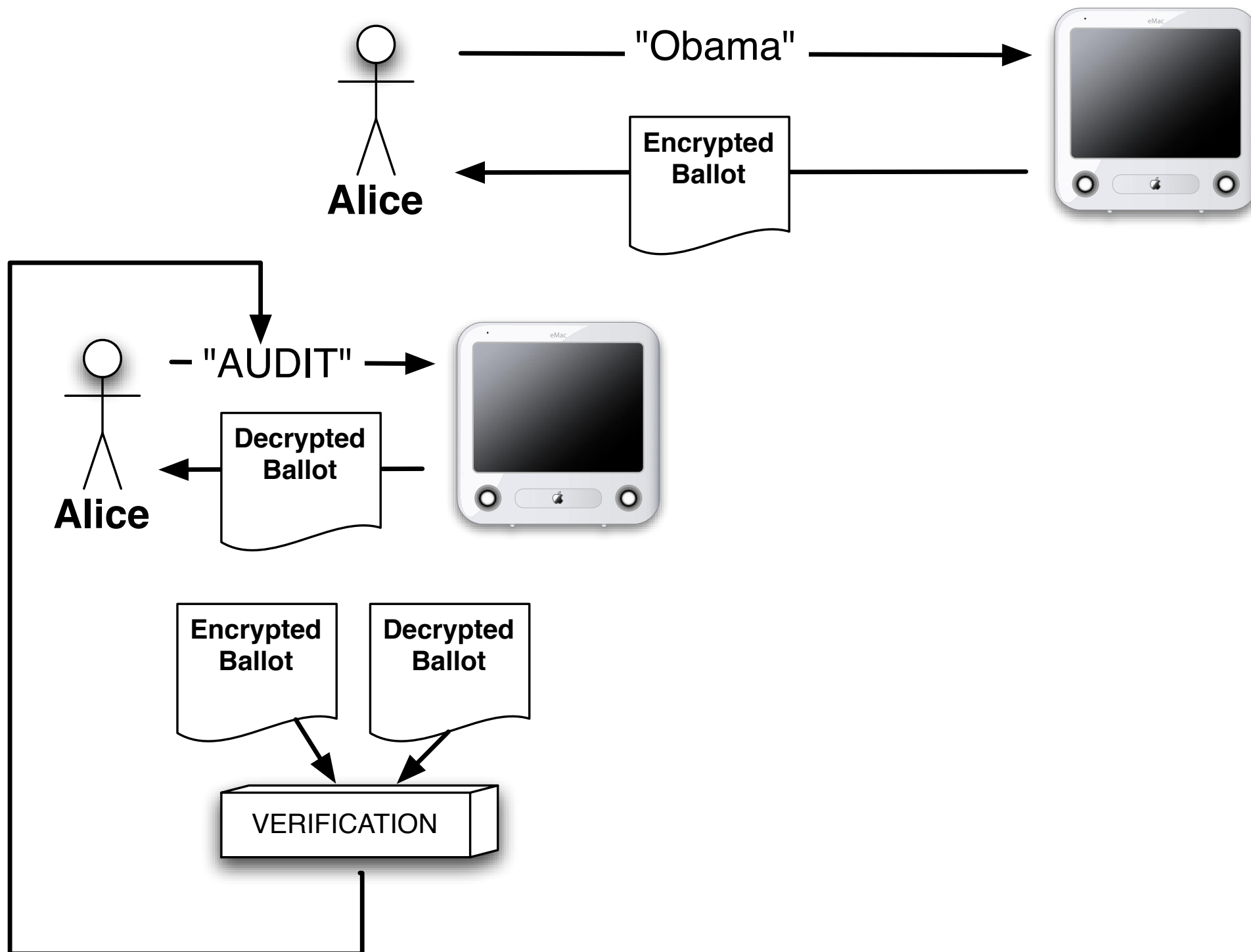
Benaloh Casting



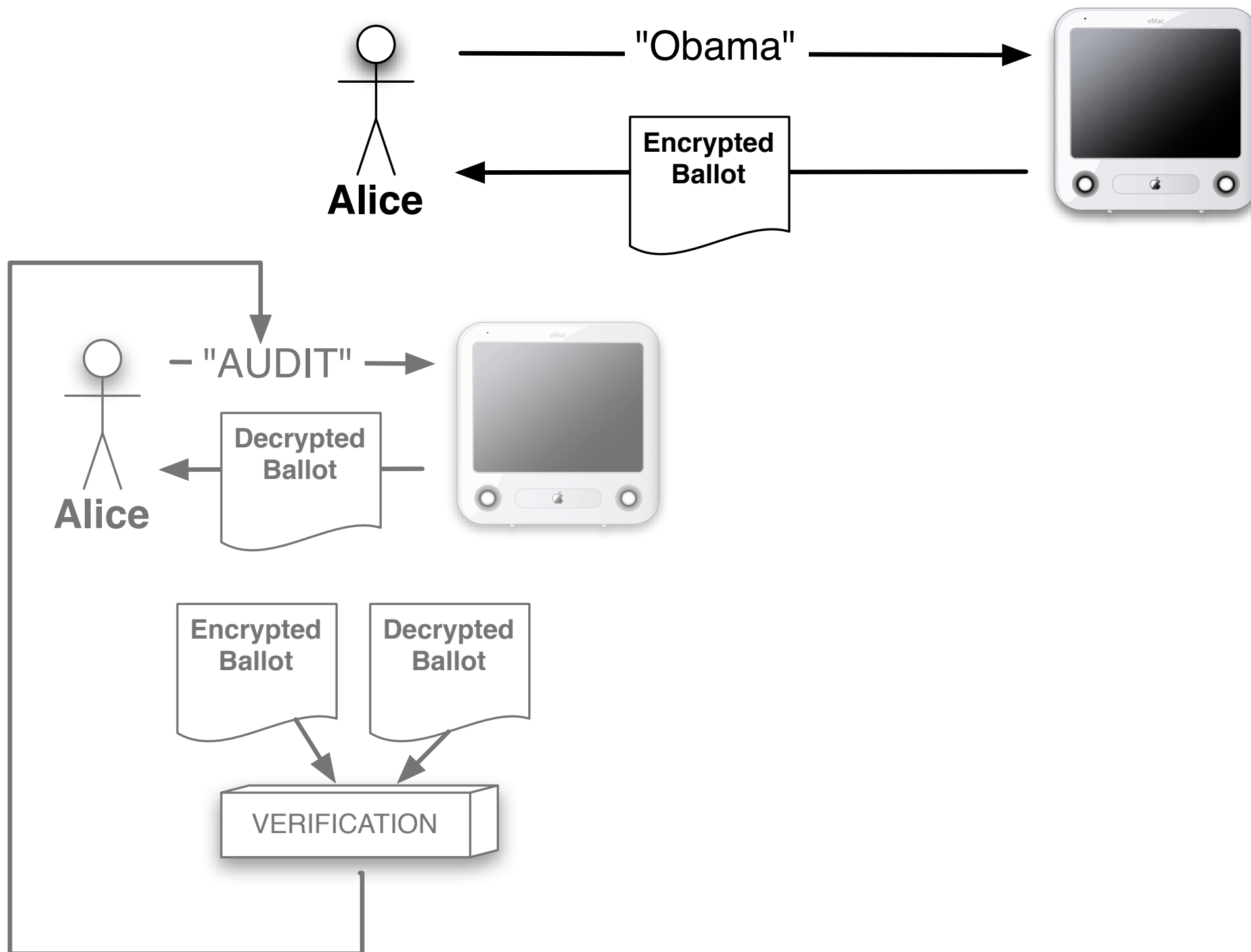
Benaloh Casting



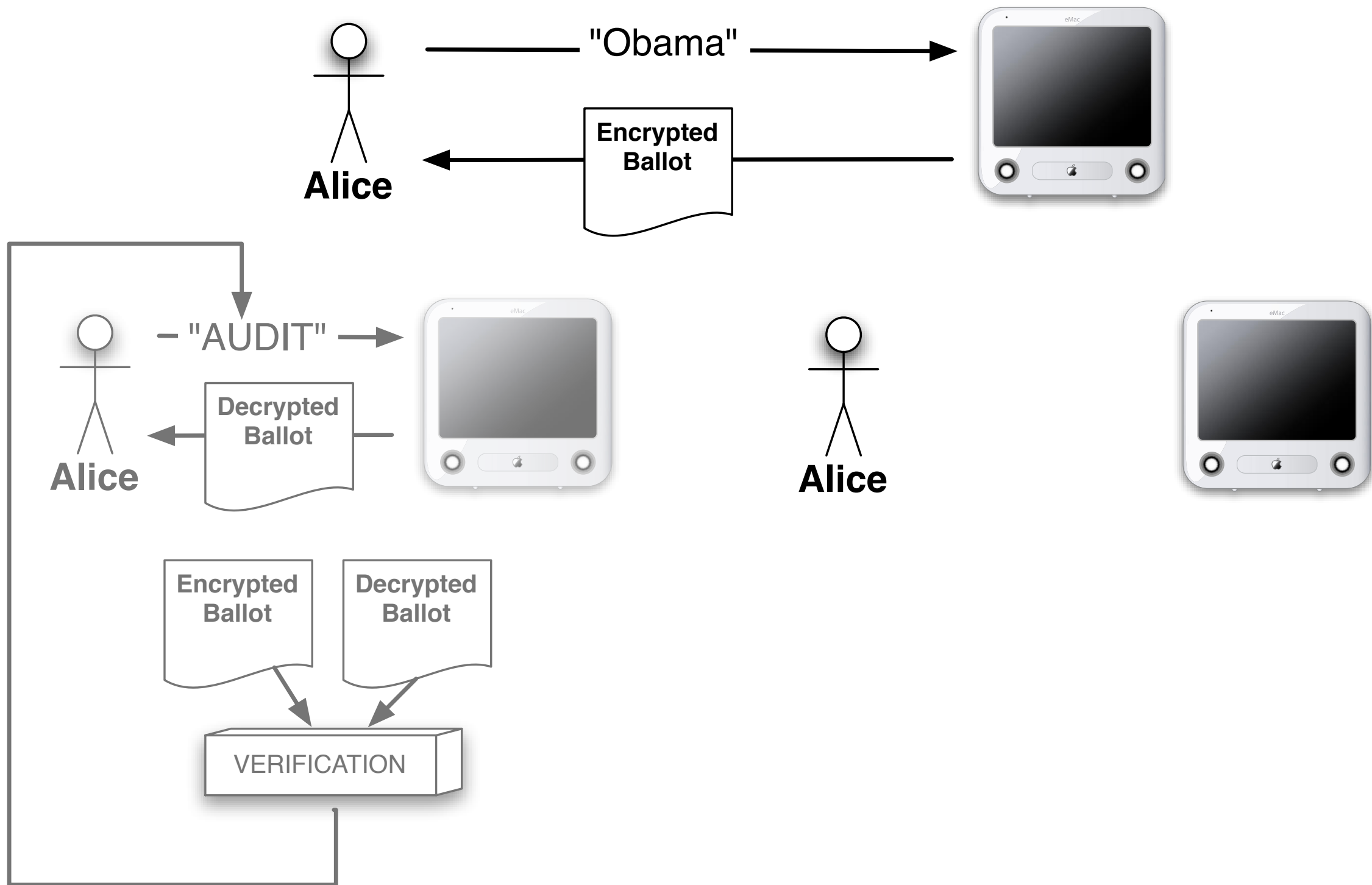
Benaloh Casting



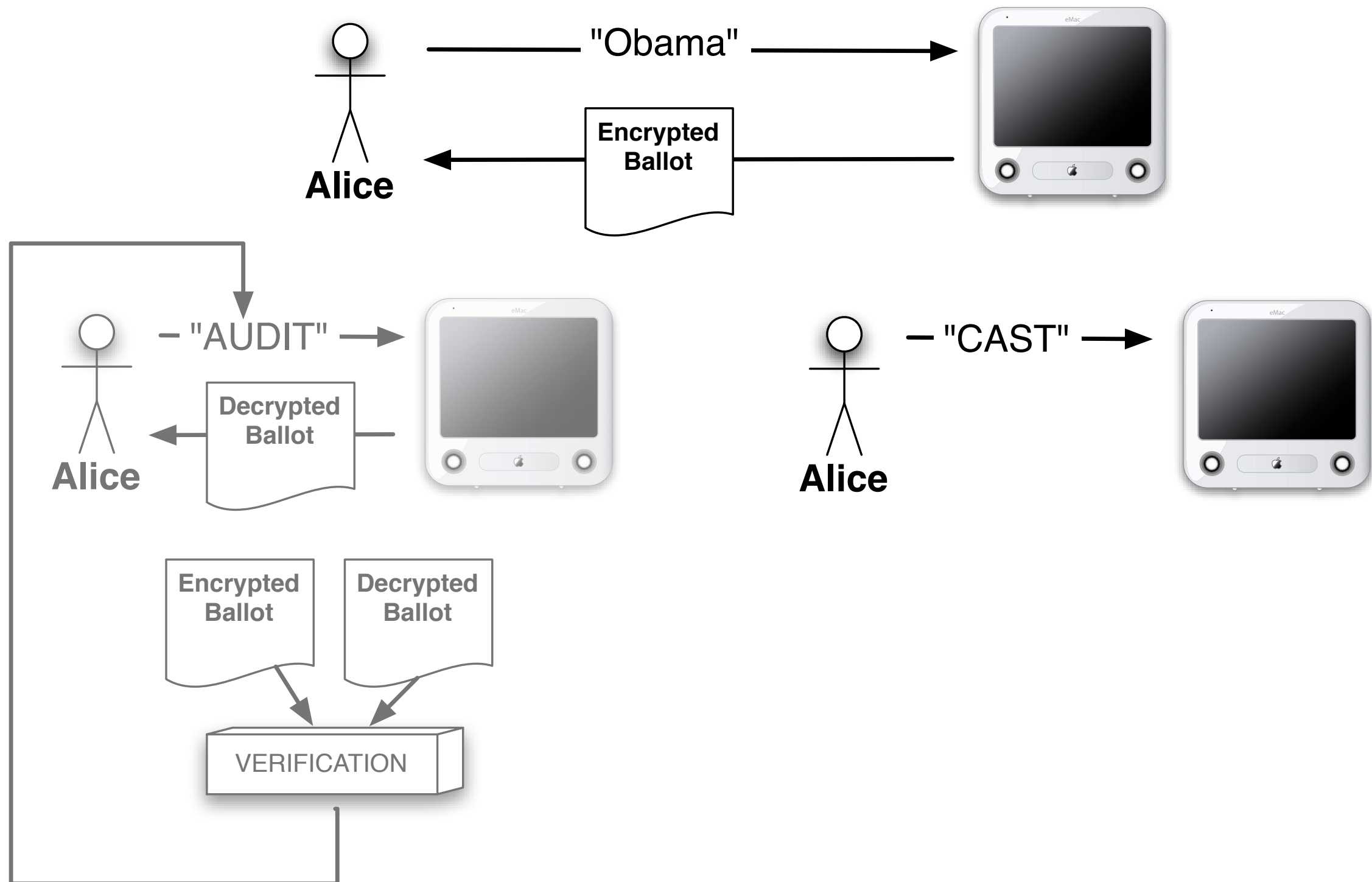
Benaloh Casting



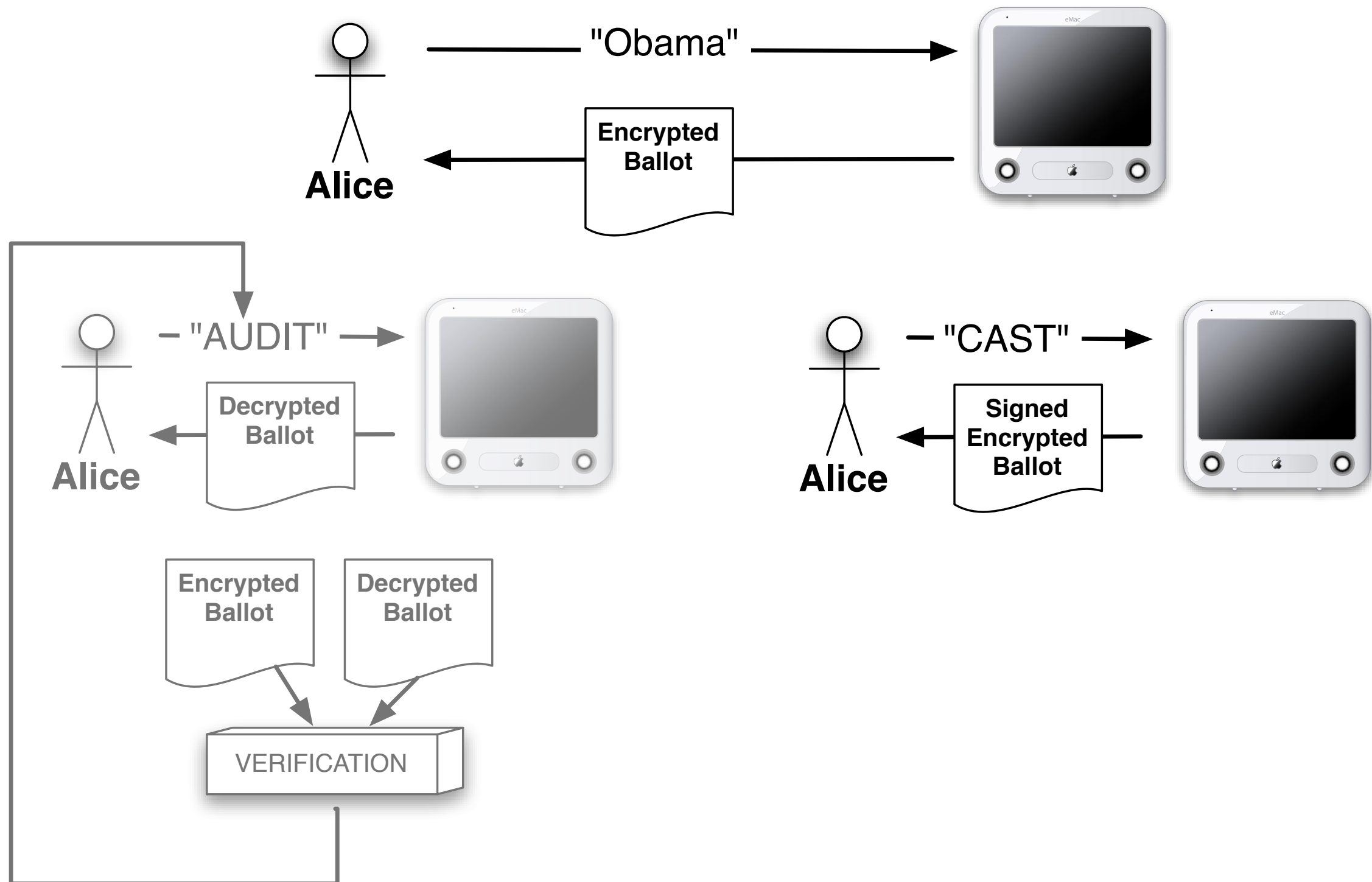
Benaloh Casting



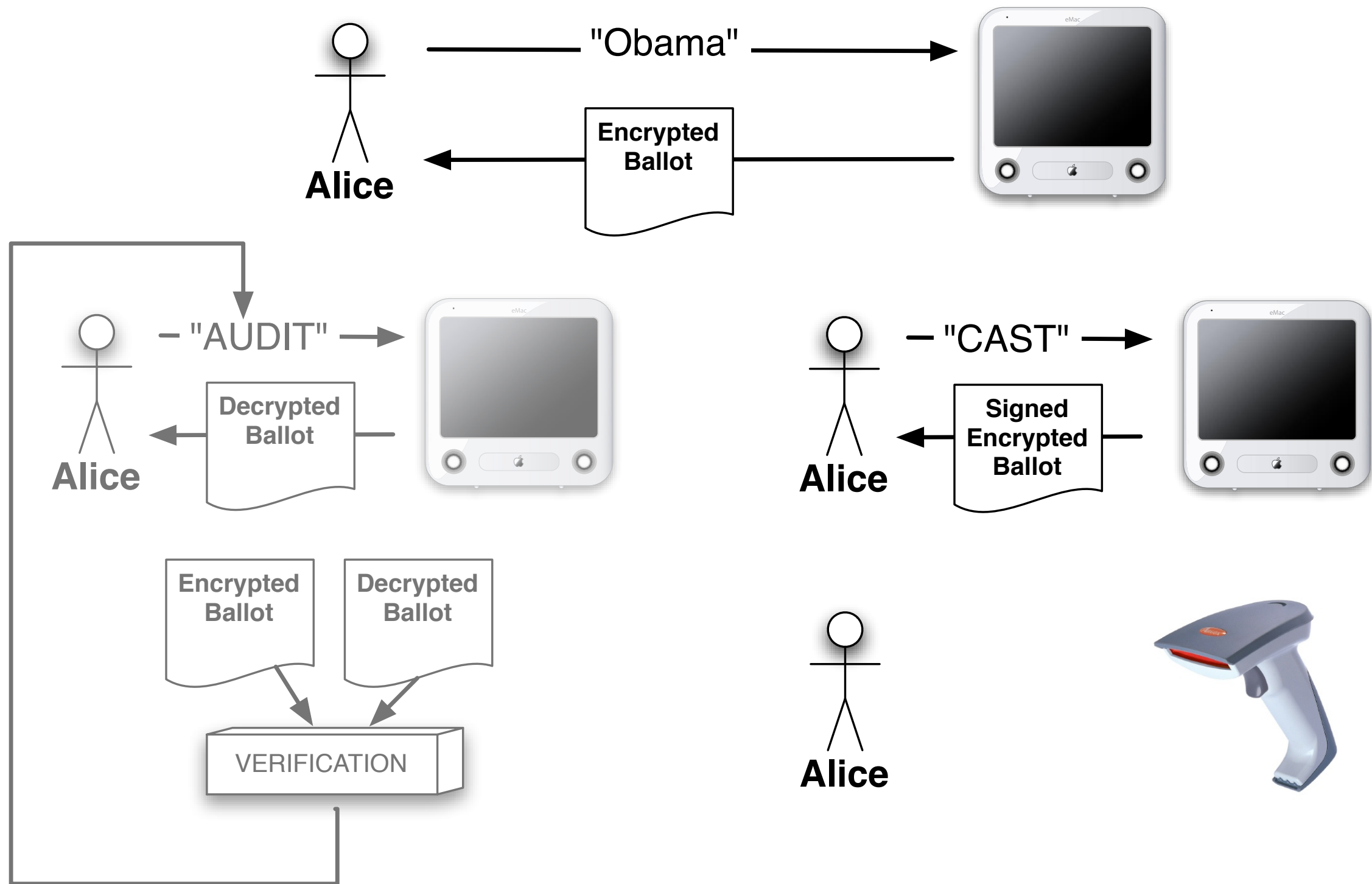
Benaloh Casting



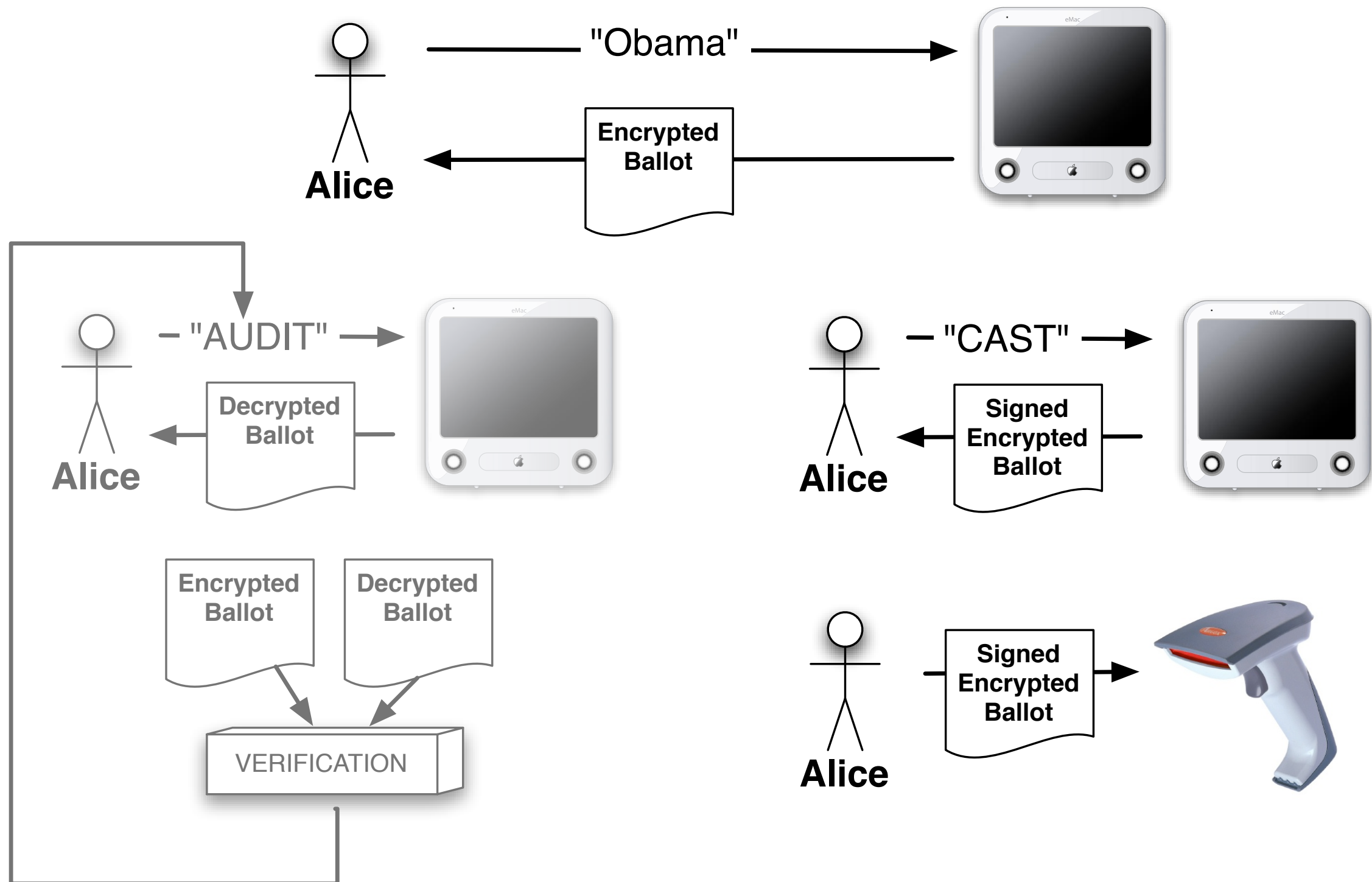
Benaloh Casting



Benaloh Casting



Benaloh Casting



Many more great ideas

- Neff's MarkPledge
 - ➔ high-assurance, human-verifiable, proofs of correct encryption
- Scantegrity
 - ➔ closely mirrors opscan voting
- ThreeBallot by Rivest
 - ➔ teaching the concept of open-audit without deep crypto
- STV: Ramchen, Teague, Benaloh & Moran.
 - ➔ handling complex election styles
- Prêt-à-Voter by Ryan et al.
 - ➔ elegant, simple, paper-based

Deployments!

- UCL (25,000 voters)
- Scantegrity @ Takoma Park
- SCV

Three Points

1. Voting is a unique trust problem.
2. Cryptography is not just about secrets, it creates trust between competitors, it democratizes the auditing process.
3. Open-Audit Voting is closing in on practicality.

My Fear:

computerization of
voting is inevitable.
without open-audit,
the situation is grim.

My Hope:

proofs for auditing
partially-secret
processes will soon be
as common as public-
key crypto is now.

Challenge:



Ed Felten: “you have no voter privacy, deal with it.”

Challenge:



Estonia to allow citizens to vote via cellphone by 2011

by [Darren Murph](#), posted Dec 13th 2008 at 2:18AM

Ed Felten: “you have no voter privacy, deal with it.”



Questions?