Voting is a ***fundamentally*** difficult problem.

The Point of An Election

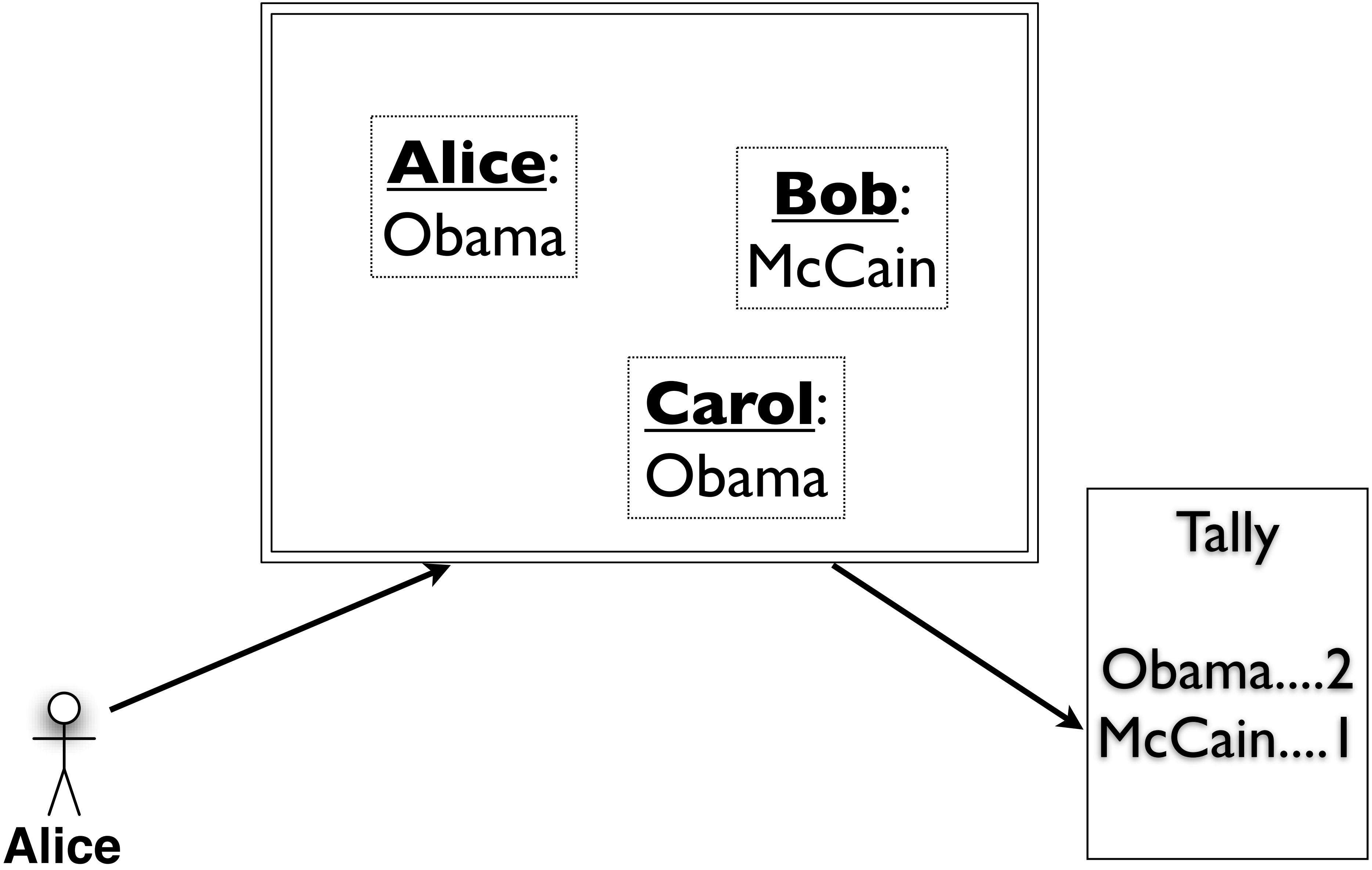
The Point of An Election

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

Dick Tuck
1966 Concession Speech

Provide enough evidence
to convince the loser.

Public Ballots



Alice: Obama

Bob: McCain

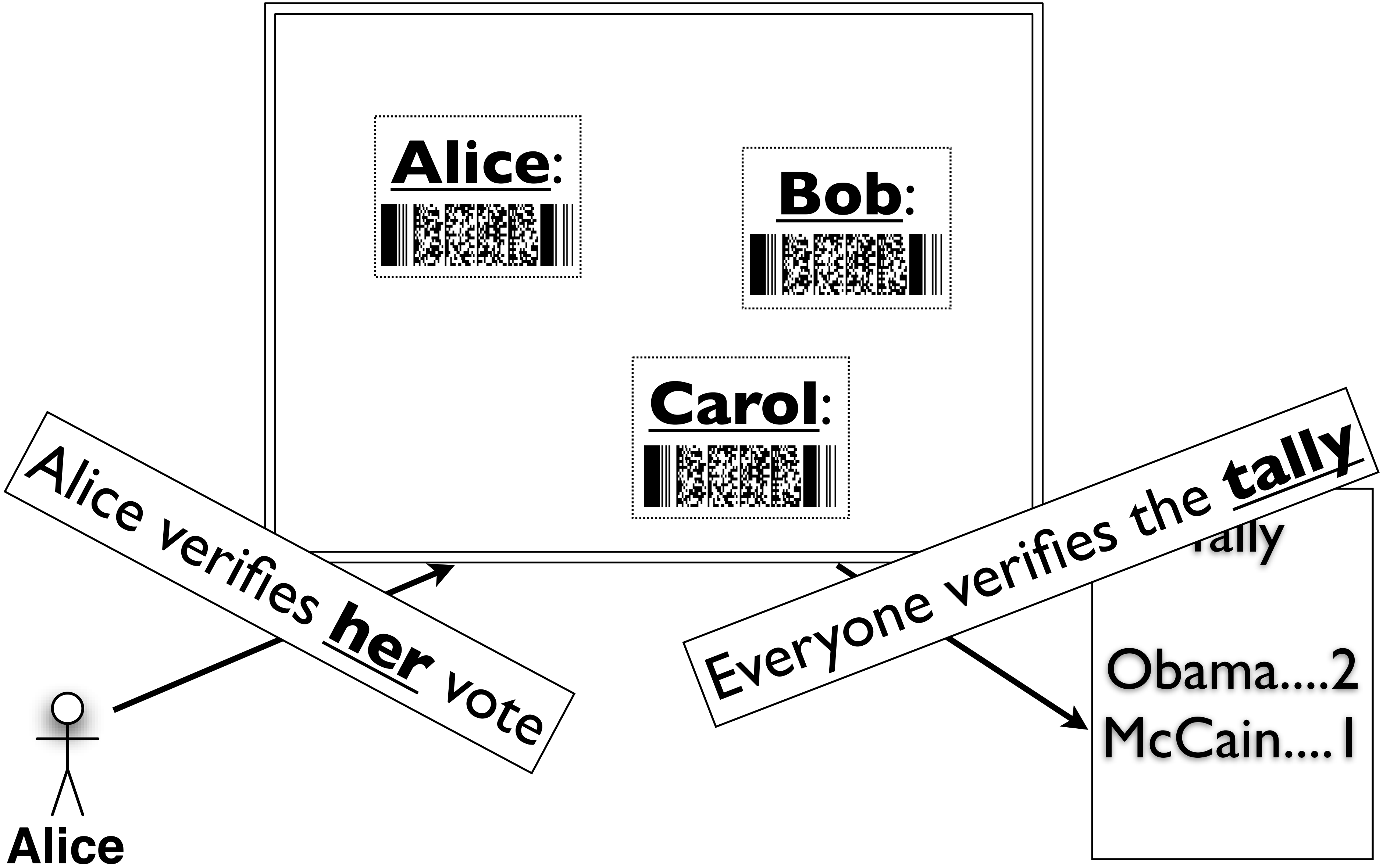
Carol: Obama

Tally

Obama....2
McCain....1

Alice

Encrypted Public Ballots



Alice:

Bob:

Carol:

Alice verifies **her** vote

Everyone verifies the **tally**

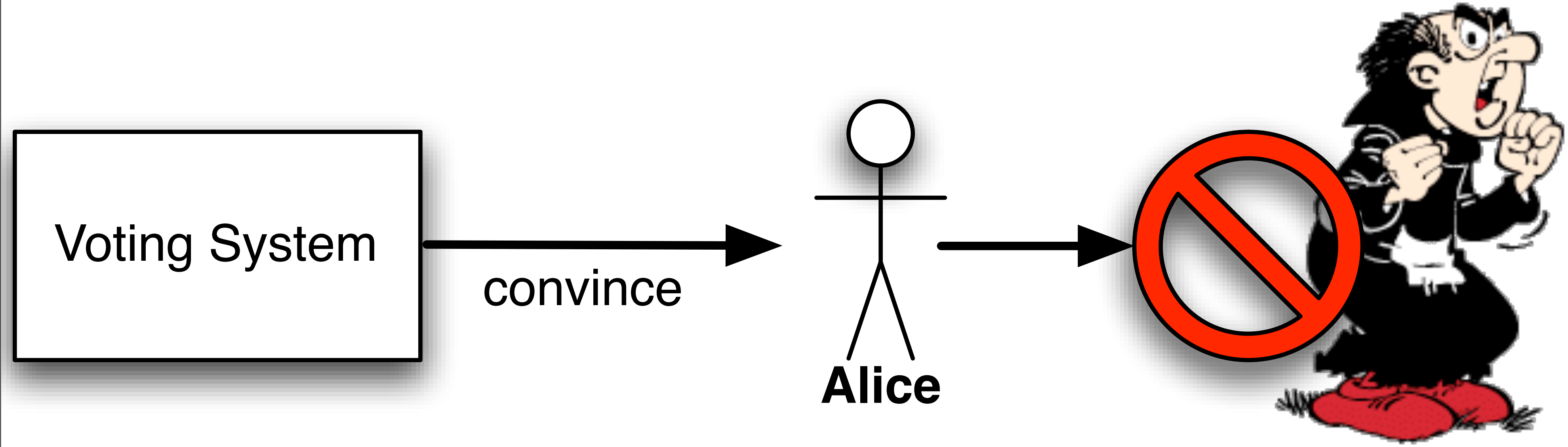
Tally

Obama....2
McCain....1

Alice

Enforced Privacy
to ensure each voter
votes in his/her
own interest

Secret Ballot *vs.* Verifiability



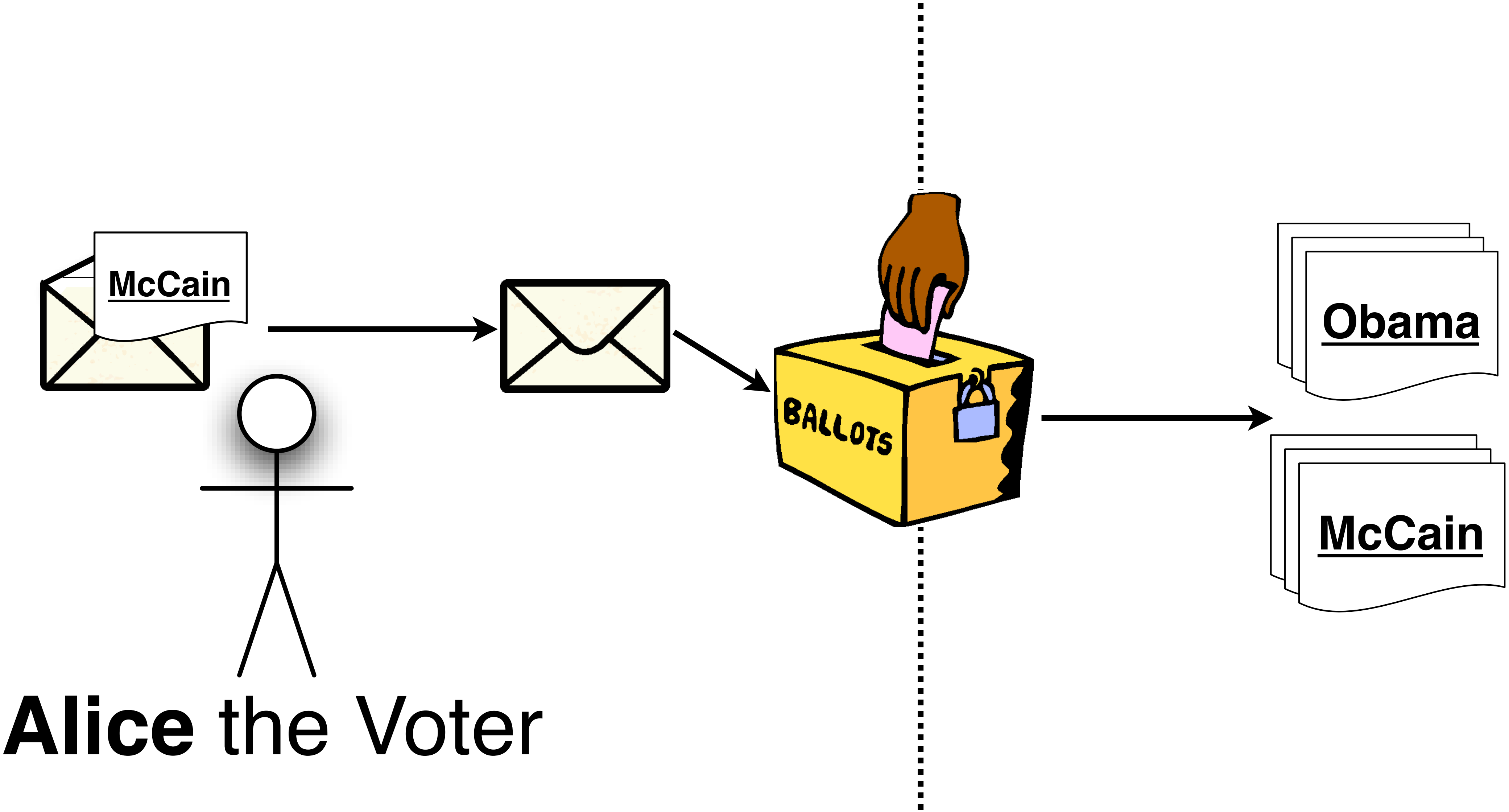
Voting System

convince

Alice

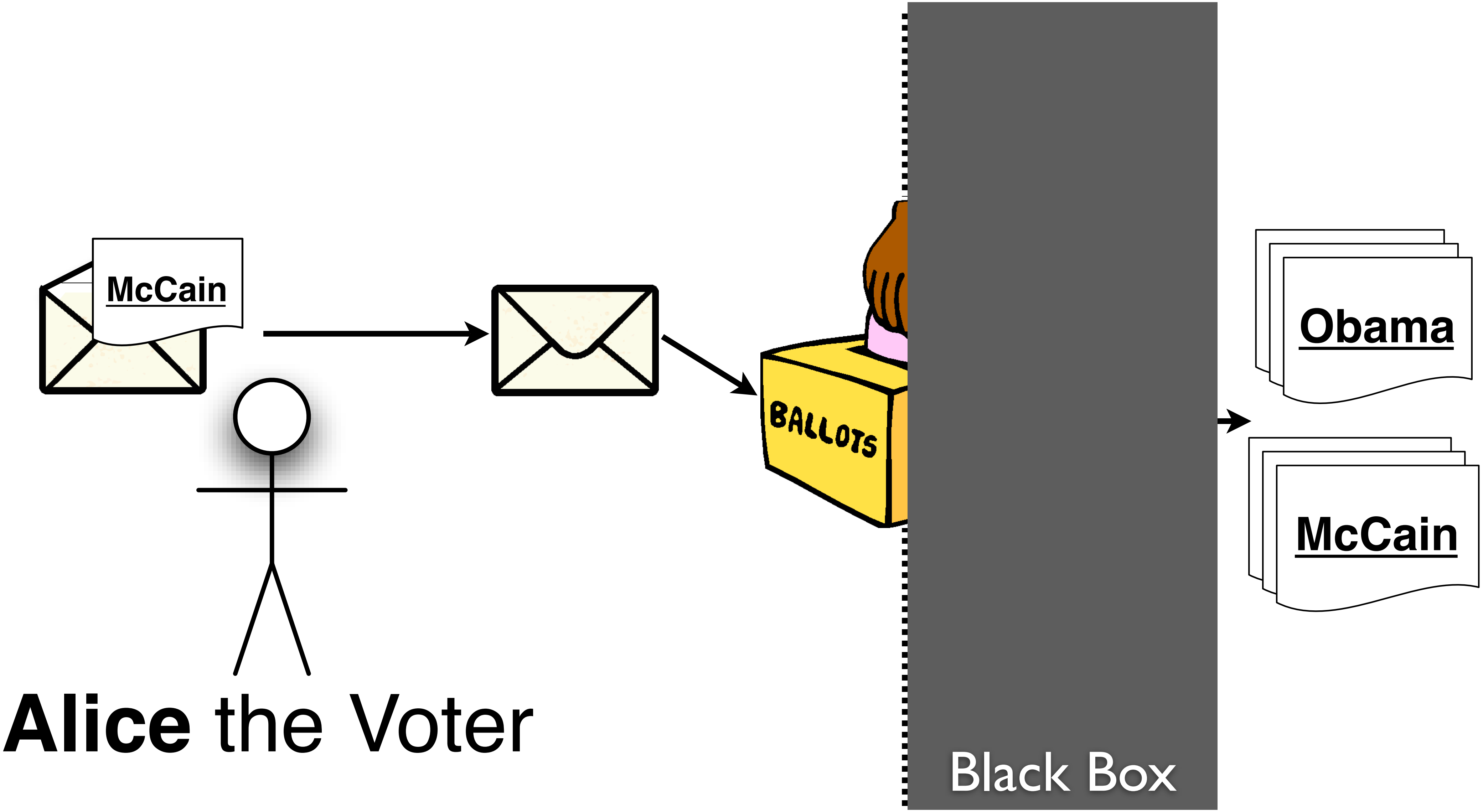
Carl the Coercer

The Ballot Handoff



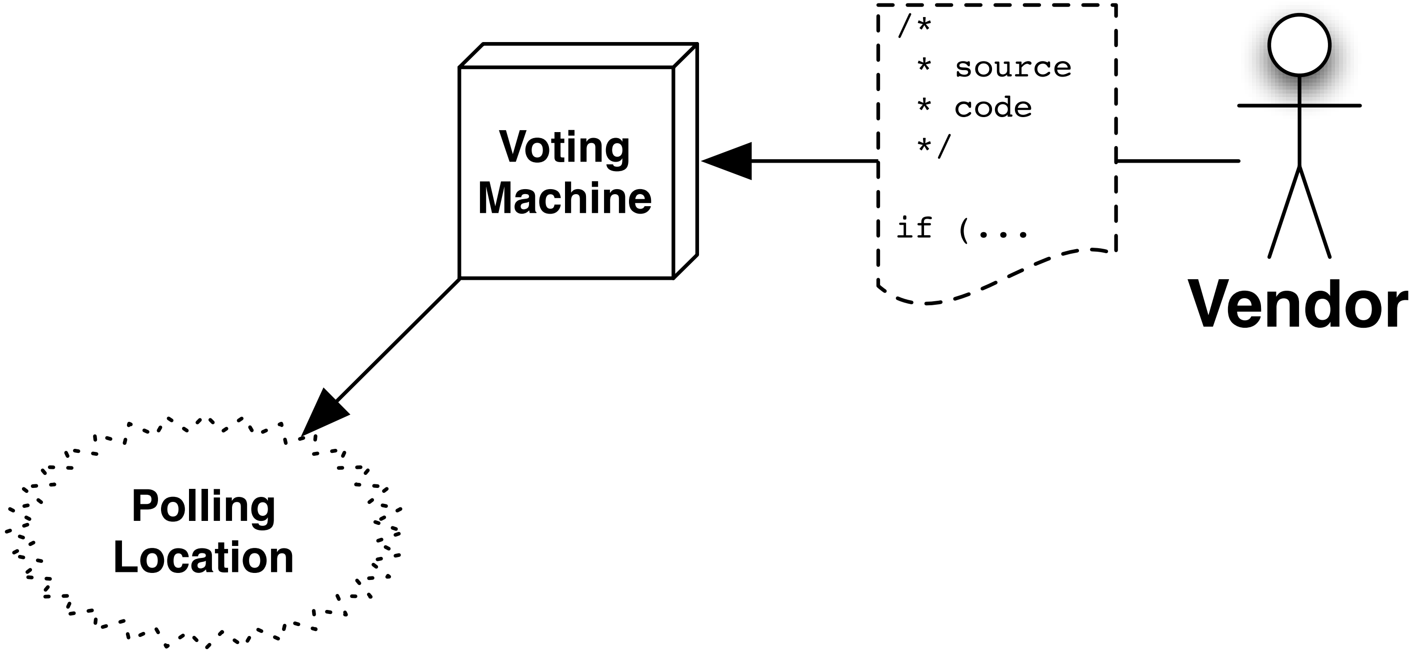
Alice the Voter

The Ballot Handoff

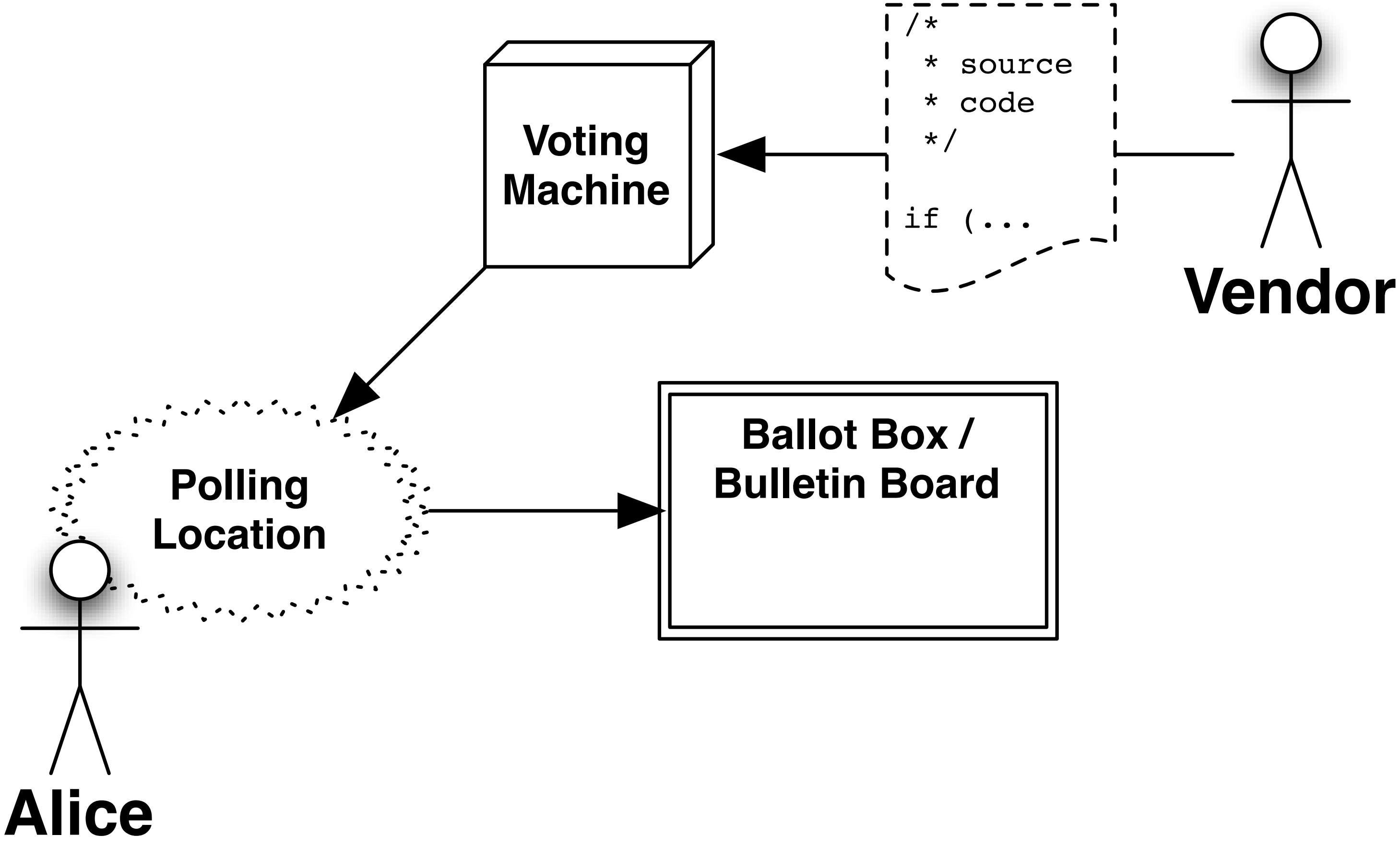


End-to-End Verification

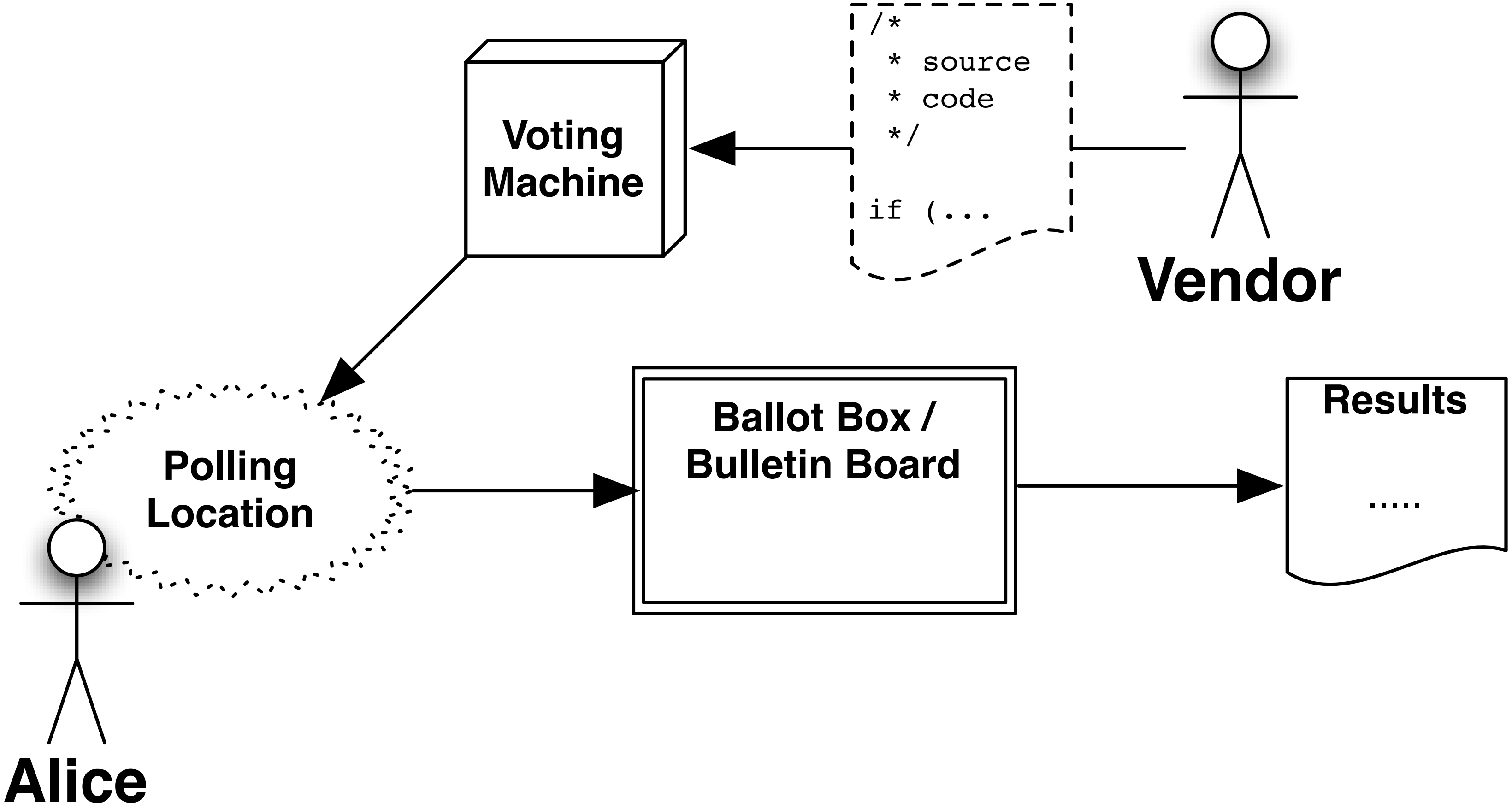
End-to-End Verification



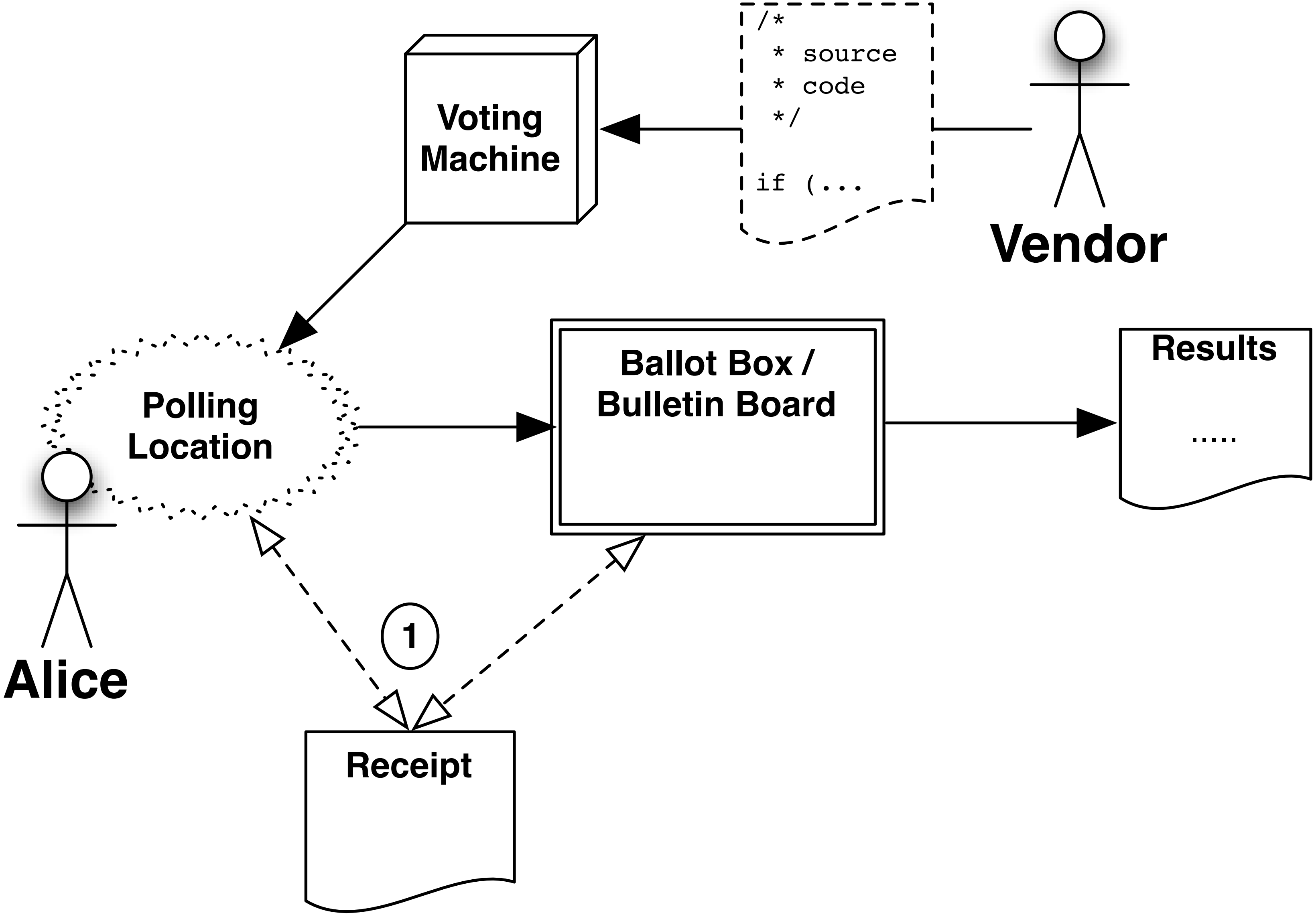
End-to-End Verification



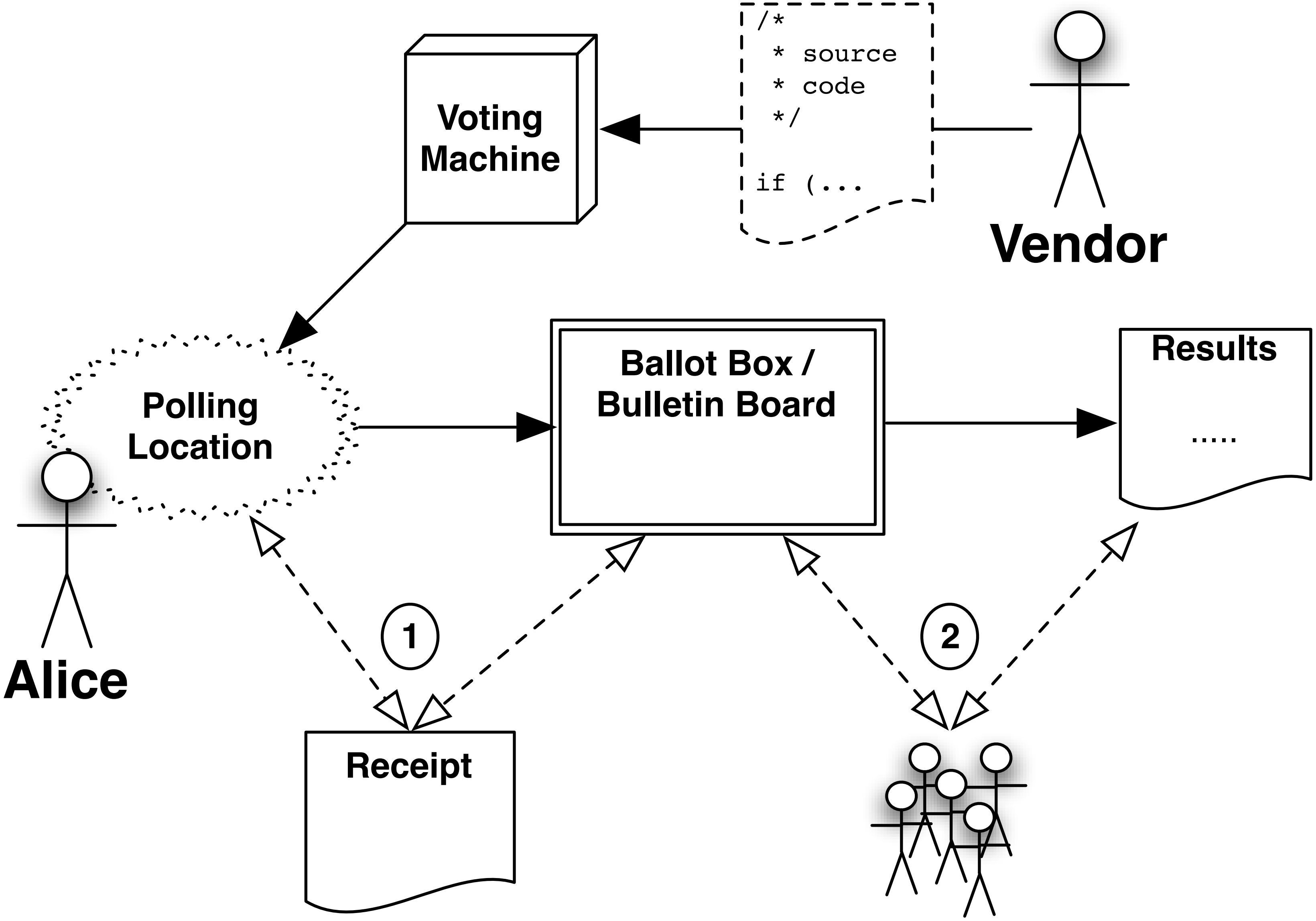
End-to-End Verification



End-to-End Verification



End-to-End Verification



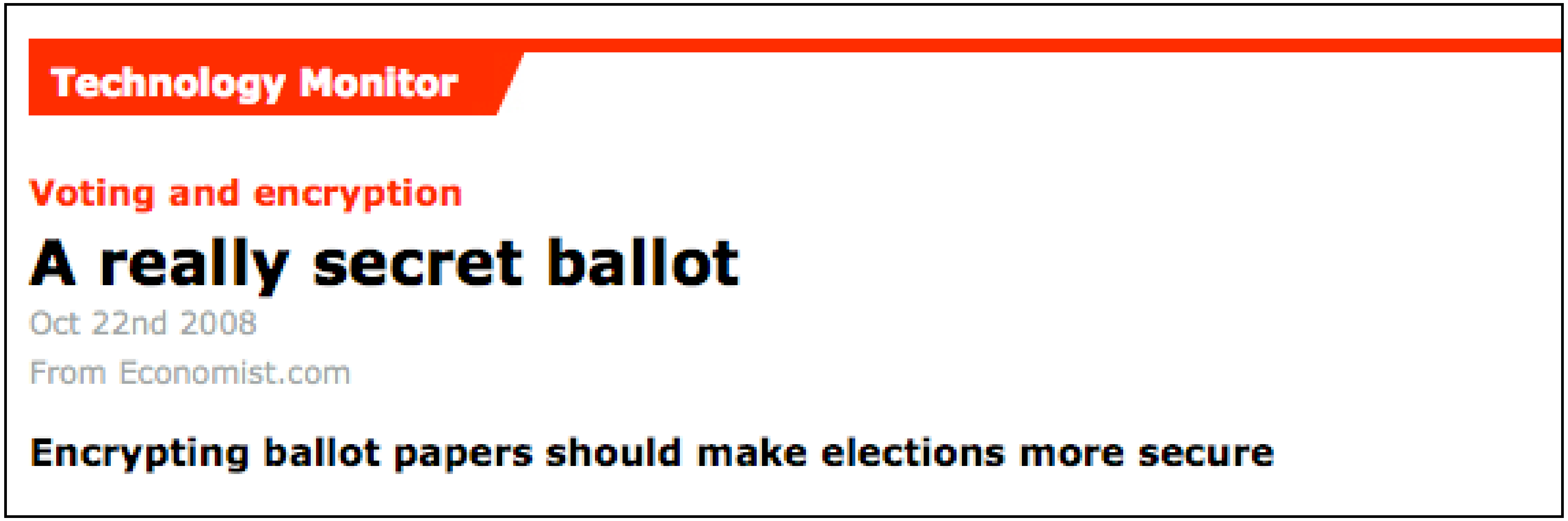
```
/*
 * source
 * code
 */

if (...
```

Then, a realization: cryptography enables a new voting paradigm

Secrecy + Auditability.

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" or
  truly-verifiable voting



Technology Monitor

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 ***work with*** the encrypted data in public, so everyone can see.

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

Homomorphic Encryption

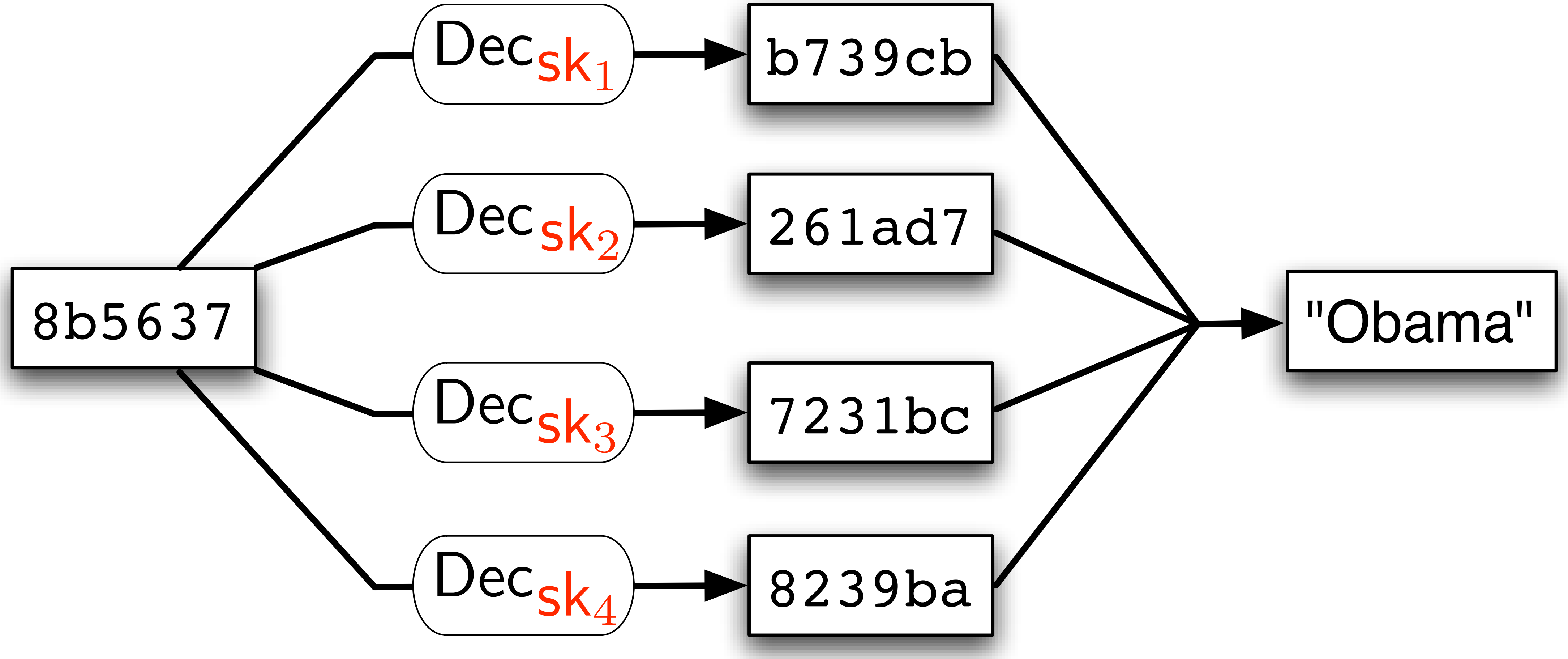
$$\mathsf{Enc}(m_1) \times \mathsf{Enc}(m_2) = \mathsf{Enc}(m_1 + m_2)$$

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

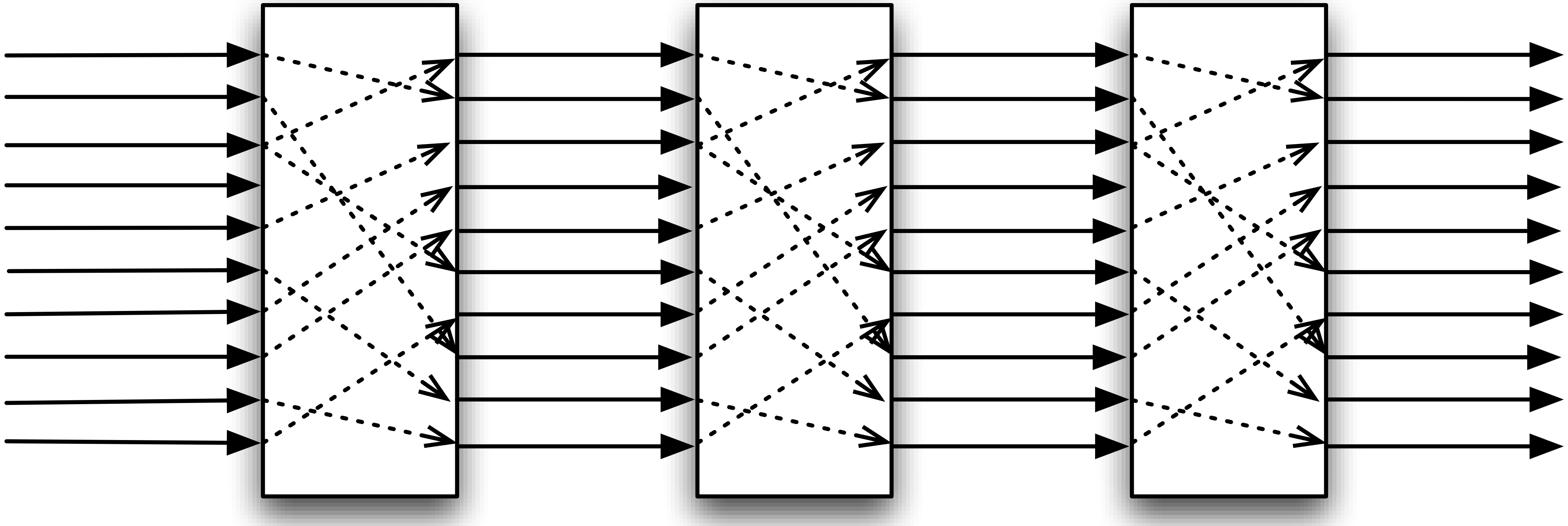
then we can simply add "under cover" of encryption!

Threshold Decryption

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



Mixnets



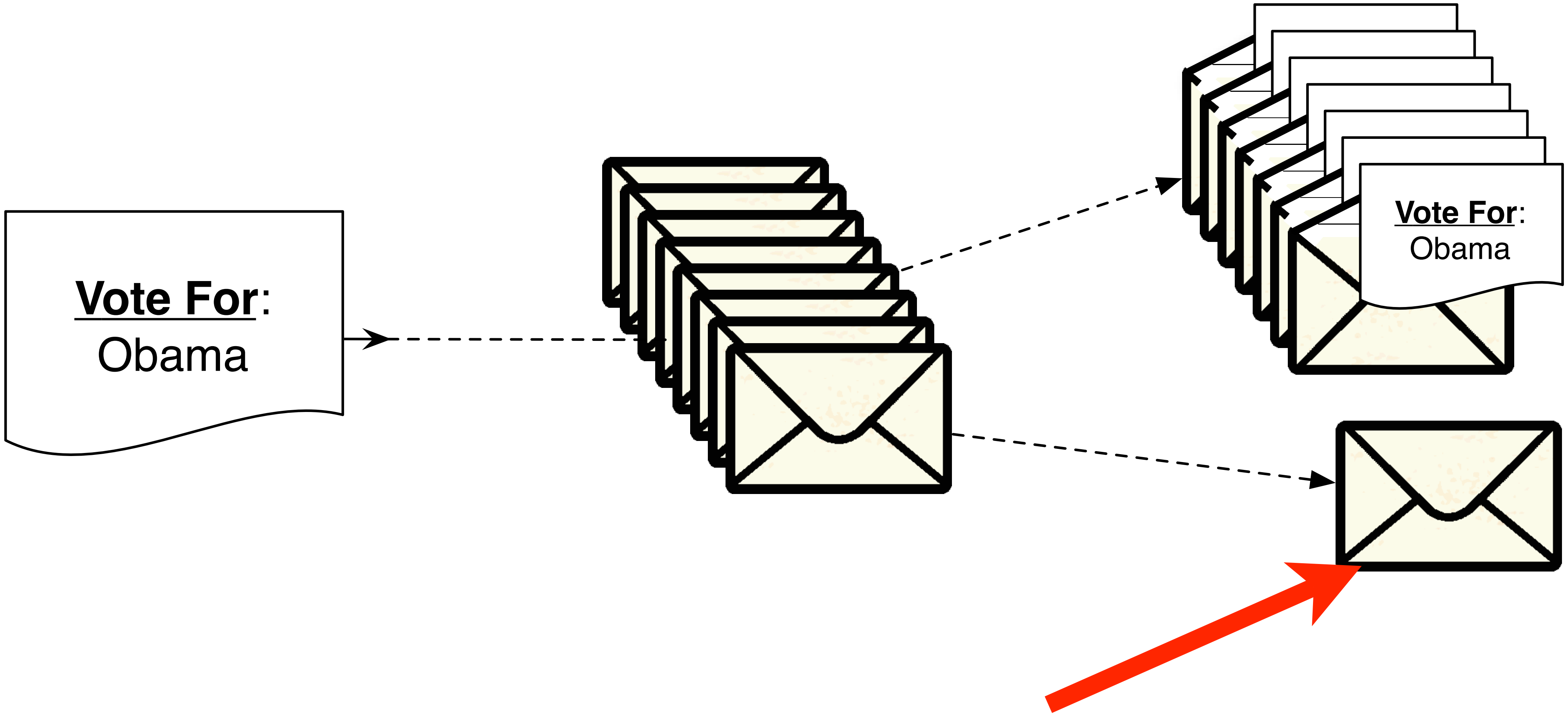
$$c = \mathsf{Enc}_{pk_1}(\mathsf{Enc}_{pk_2}(\mathsf{Enc}_{pk_3}(m)))$$

Each mix server "unwraps"
a layer of this encryption onion.

Proving certain details while keeping others secret.

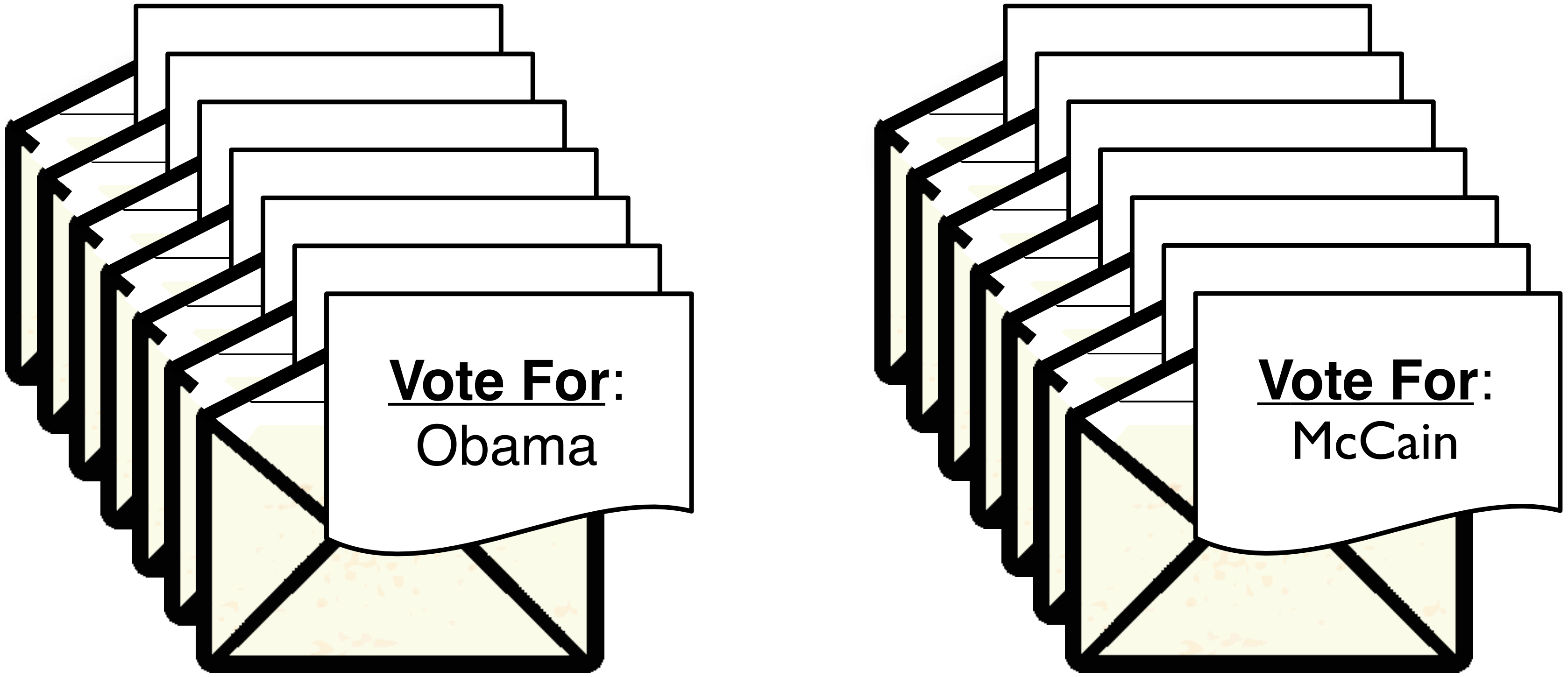
Proving a ciphertext encodes a given message without revealing its random factor.

Zero-Knowledge Proof



This last envelope likely contains “Obama”

Zero-Knowledge Proof



Open envelopes don’t prove anything after the fact.