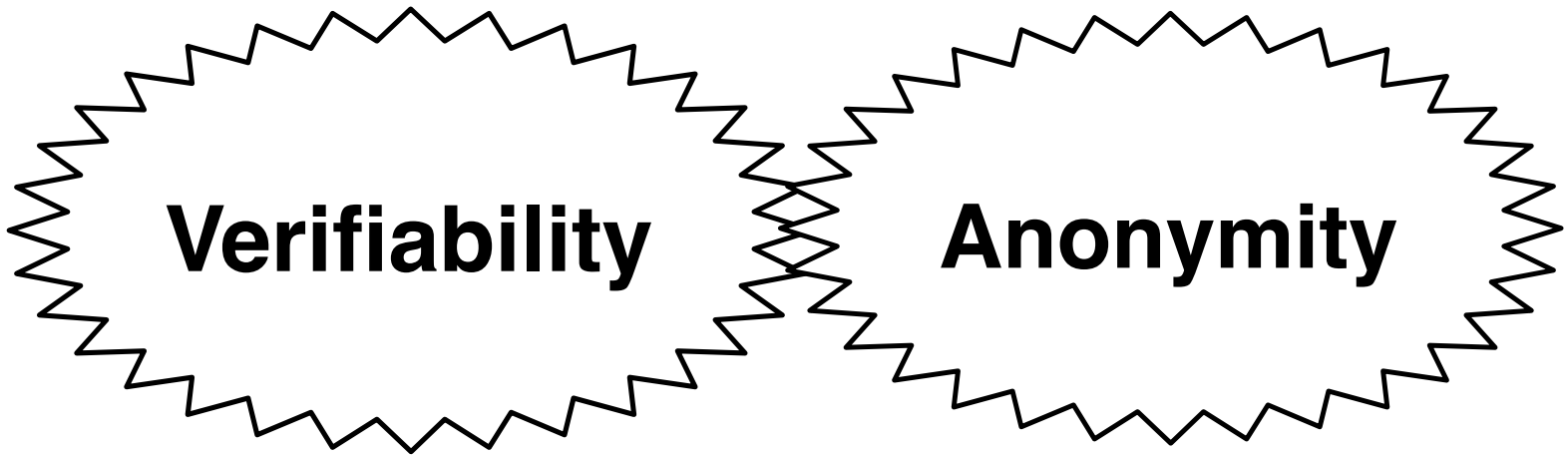
Cryptographic Voting: A Tutorial

Ben Adida
ben@mit.edu

12 February 2005

Voting is Hard



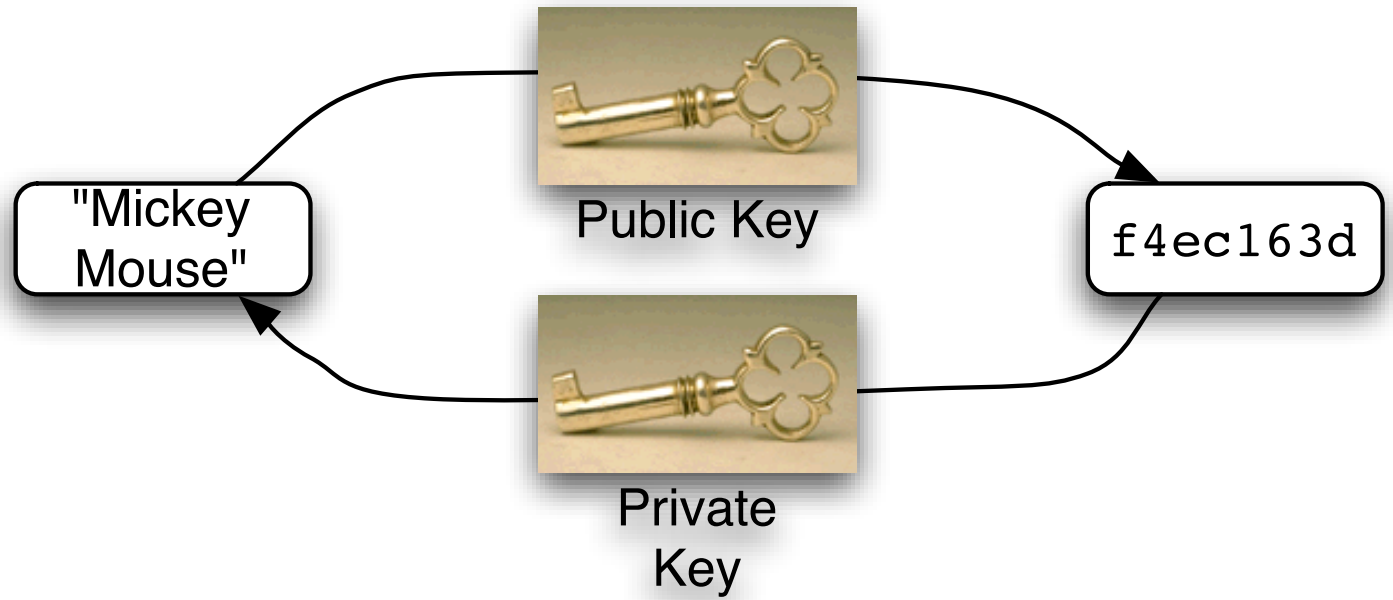
Cryptography is Useful!

"Cryptography solves problems that seem contradictory. There's such a thing as 'just the right level' of contradiction."

Prof. Ronald L. Rivest

- Public-Key Encryption
- Secret Sharing
- Zero-Knowledge Proofs

Public-Key Encryption

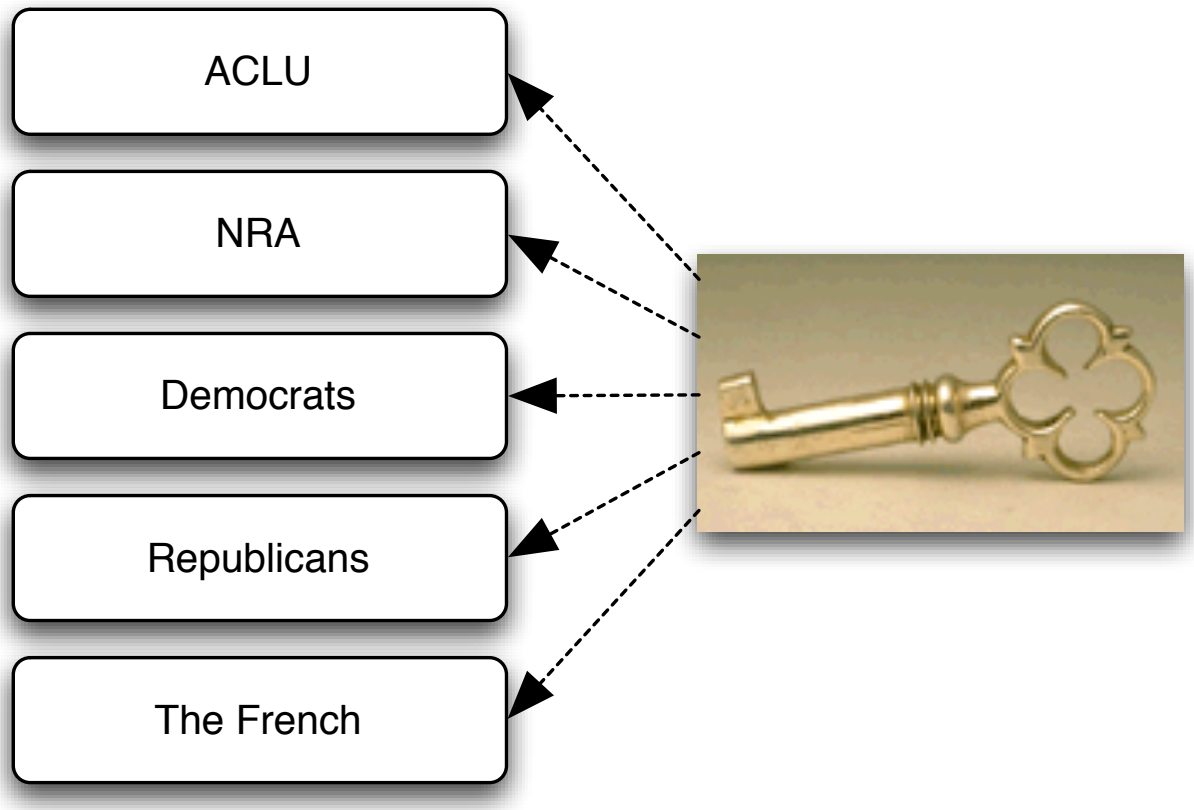


Encryption and Decryption
use ***different keys***

Reencryption

There are multiple ways to
encrypt the same message

Secret Sharing



A majority of the trustees is required to recover the secret.

Zero-Knowledge Proofs

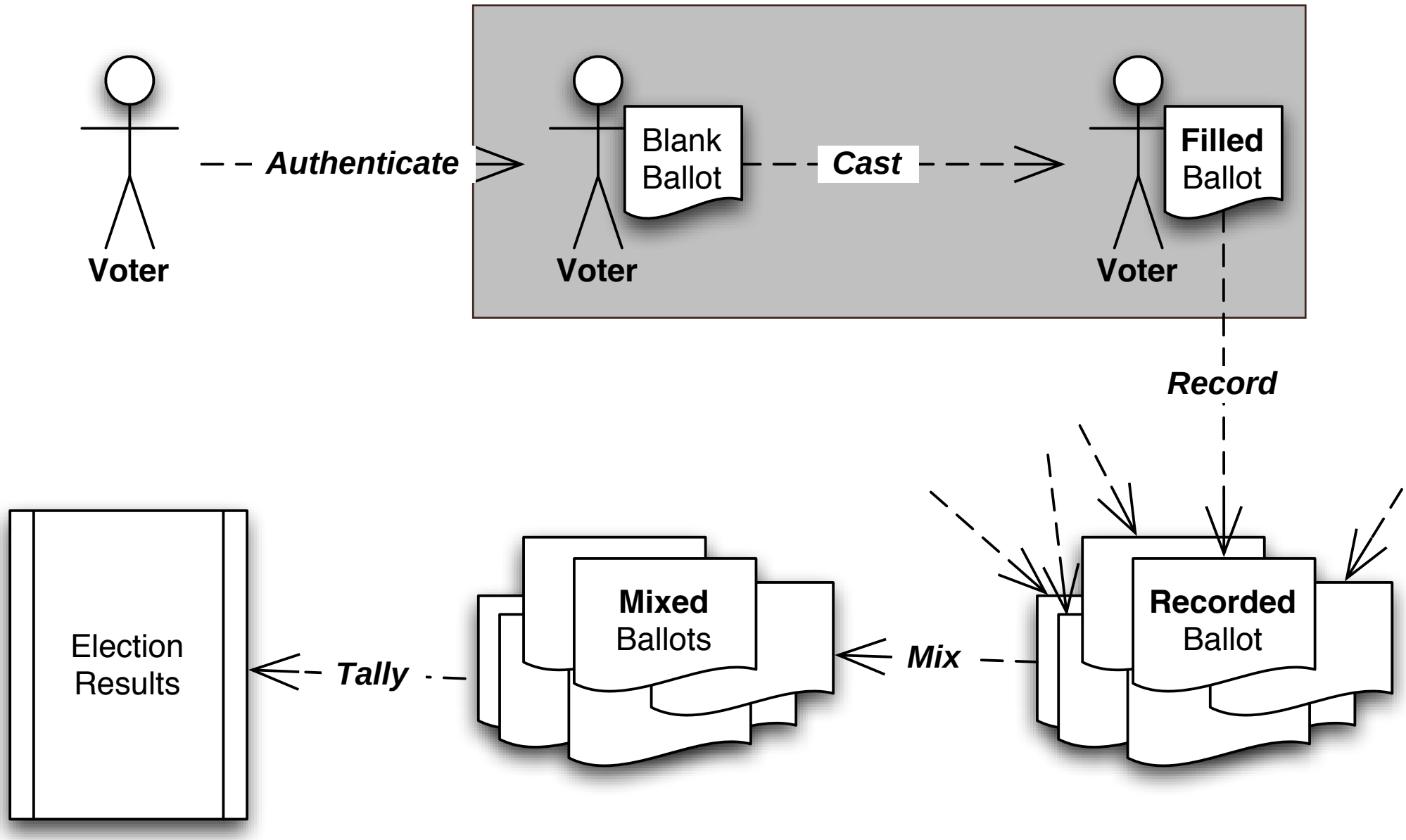
This ciphertext encodes a ballot for
“Mickey Mouse”

You are convinced, but
you cannot prove it to anyone else

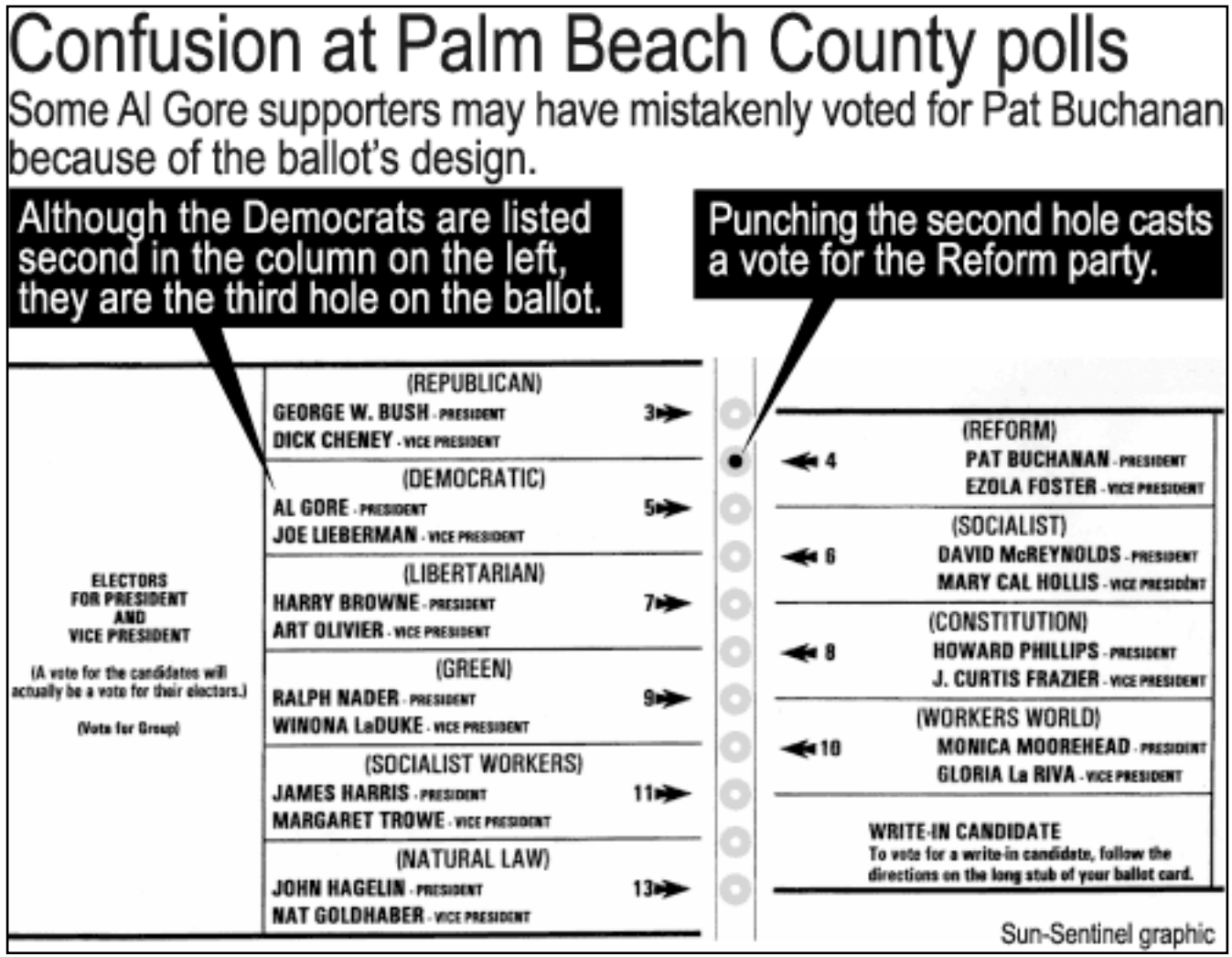
Voting Requirements

- Cast as Intended
- Recorded as Cast
- Tallied as Recorded

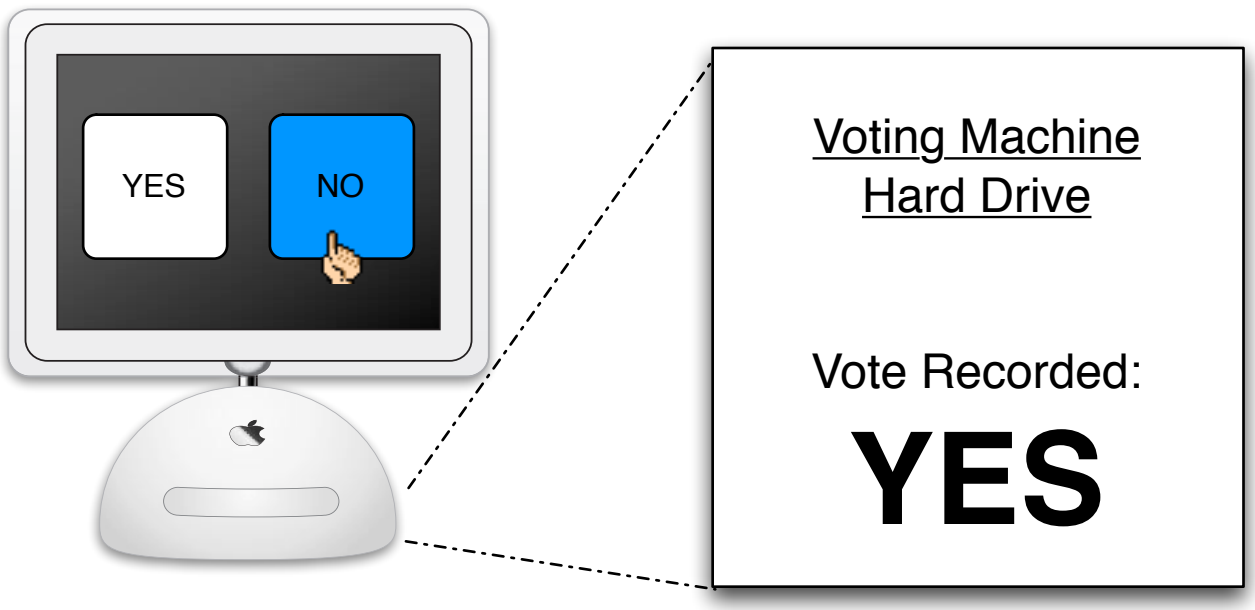
- No Vote Selling or Coercion!


Voter
Authenticate
Blank
Ballot
Voter
Cast
Filled
Ballot
Voter
Record
Election
Results
Tally
Mixed
Ballots
Mix
Recorded
Ballot

Cast as Intended



Recorded as Cast



Tallied as Recorded

Helicopter Crash Delays Afghan Vote Count

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

Absentee ballots 'lost' in Florida

October 28, 2004 09:28 IST

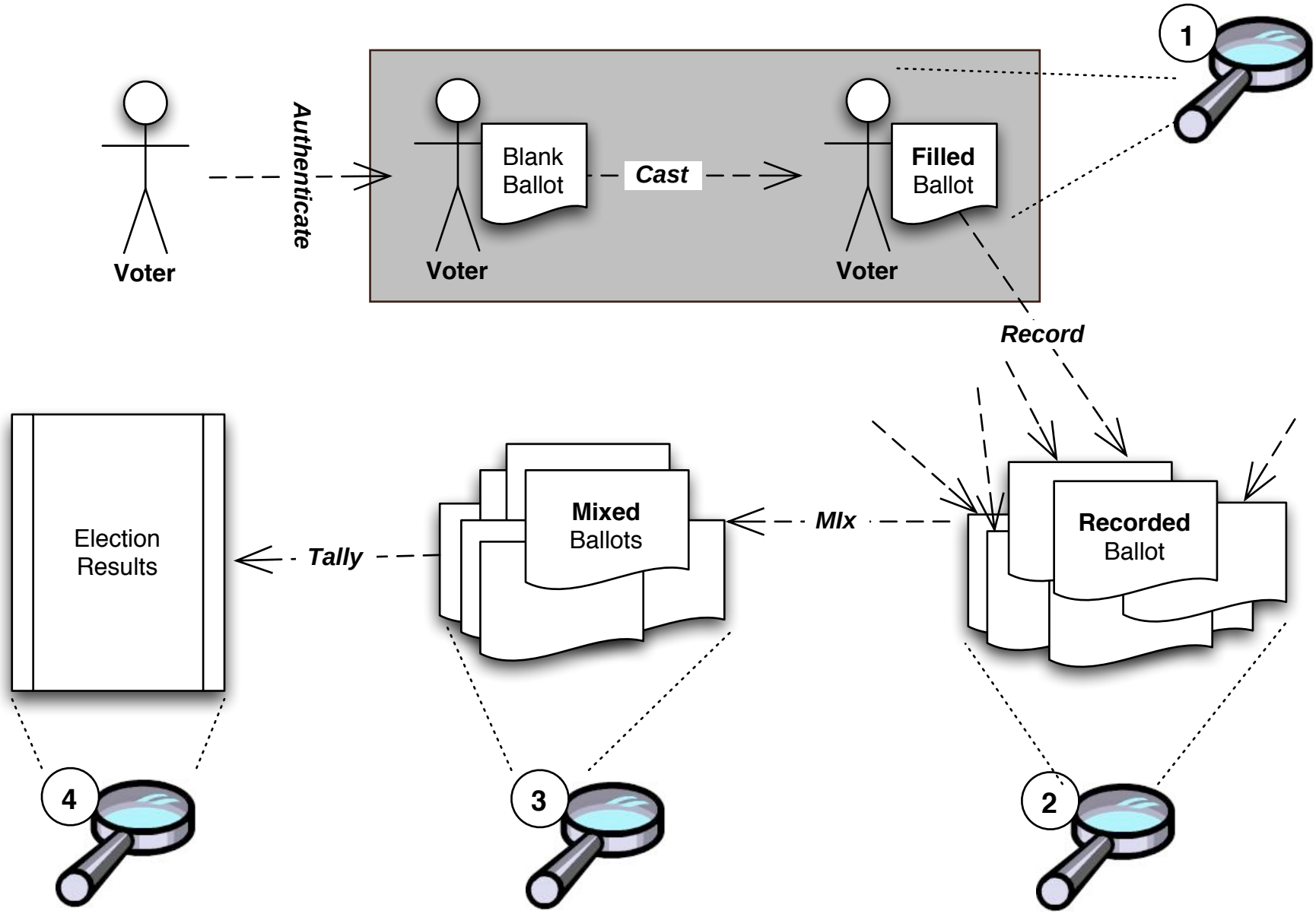
Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward County voters, who had requested them more than two weeks ago, election officials said.

Scavenged ballot box lids haunt S.F. elections

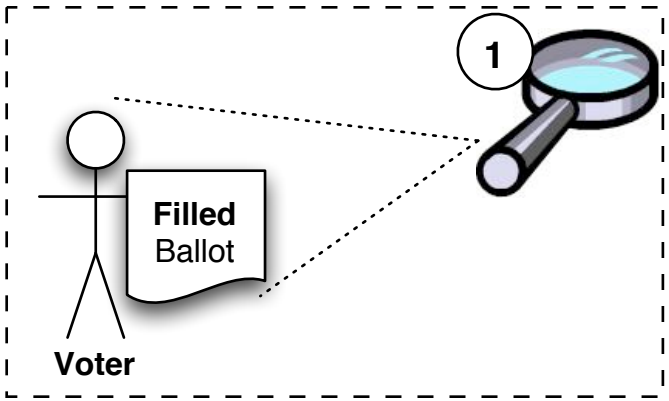
Erin McCormick, Chronicle Staff Writer

Monday, January 7, 2002

Cryptographic Voting & Universal Verifiability

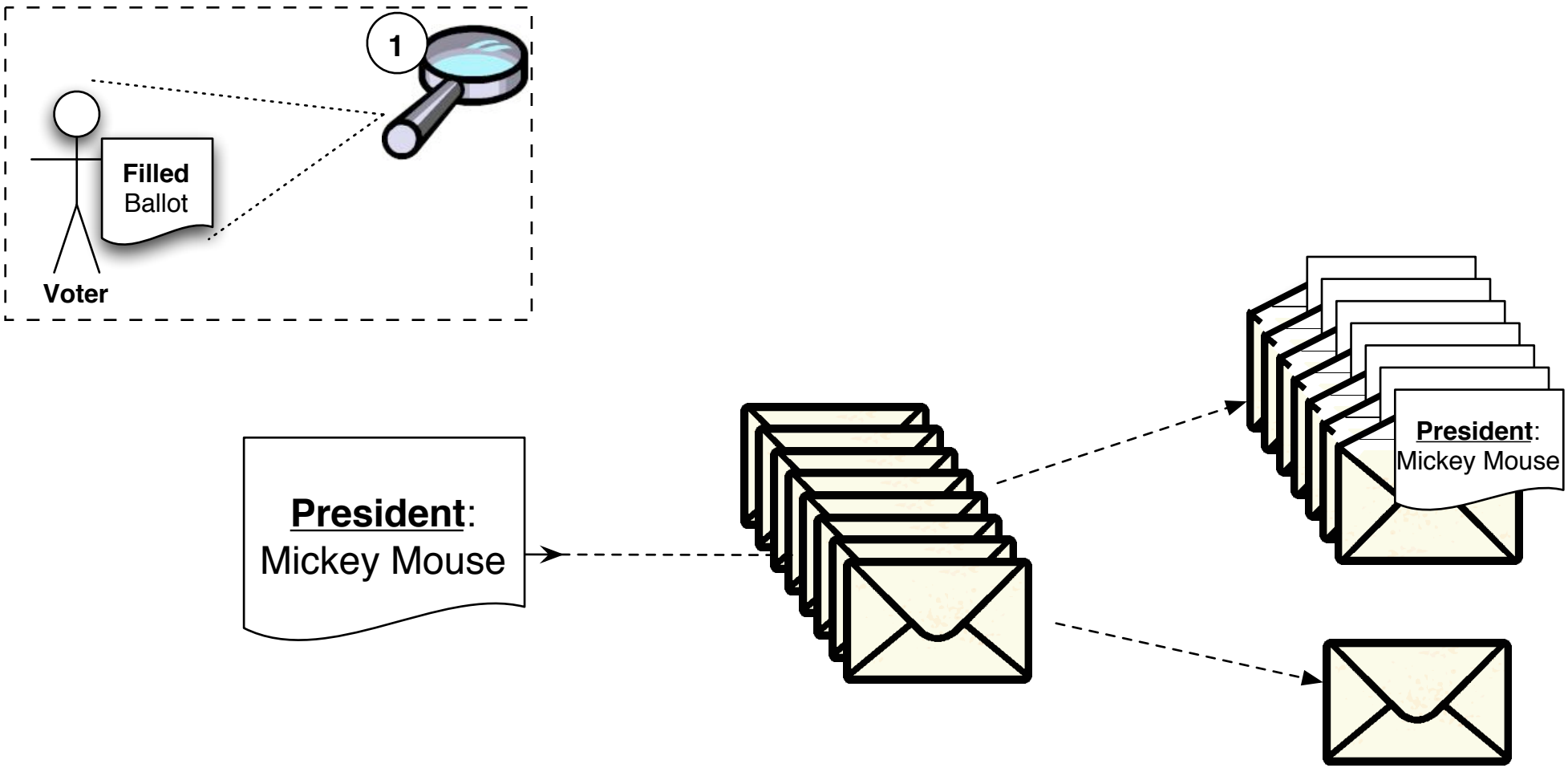

Voter
Authenticate
Blank
Ballot
Voter
Cast
Filled
Ballot
Voter
1
Record
Election
Results
Tally
Mixed
Ballots
Mix
Recorded
Ballot
4
3
2

Ballot Creation

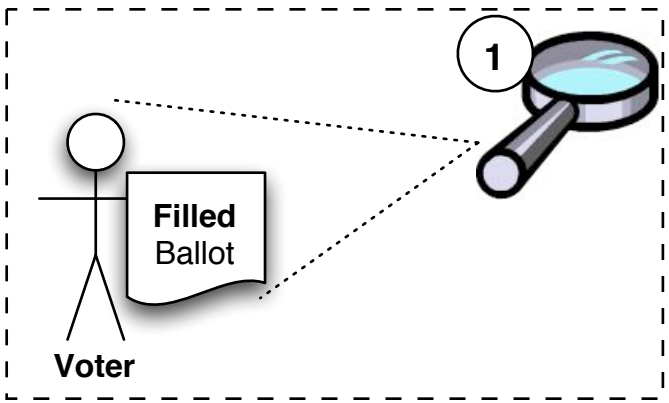


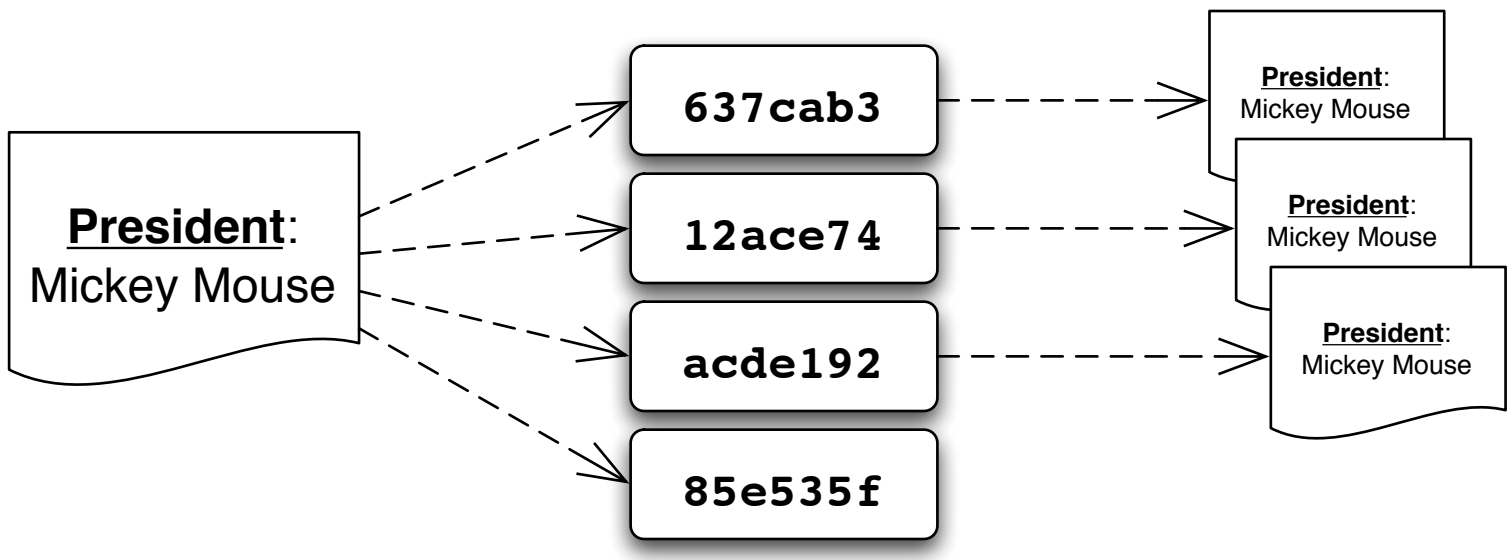
How can the voter
trust the voting machine to encrypt?

Proof of Ballot Content

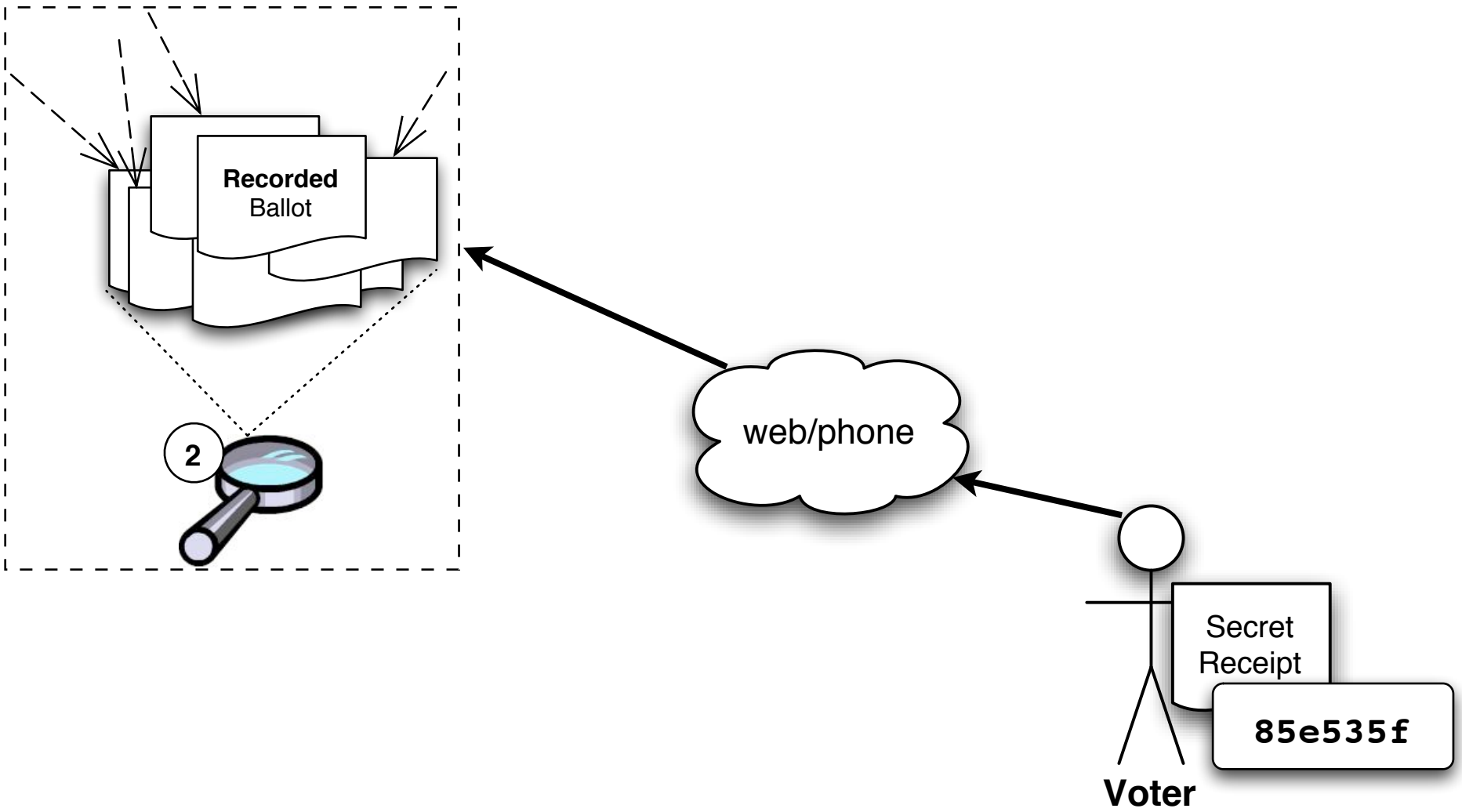


Proof of Ballot Content

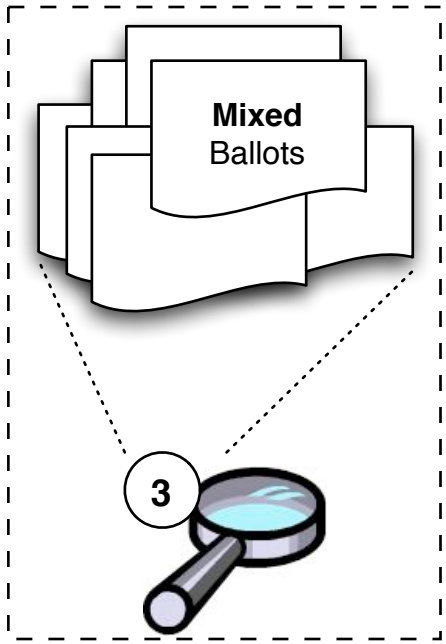


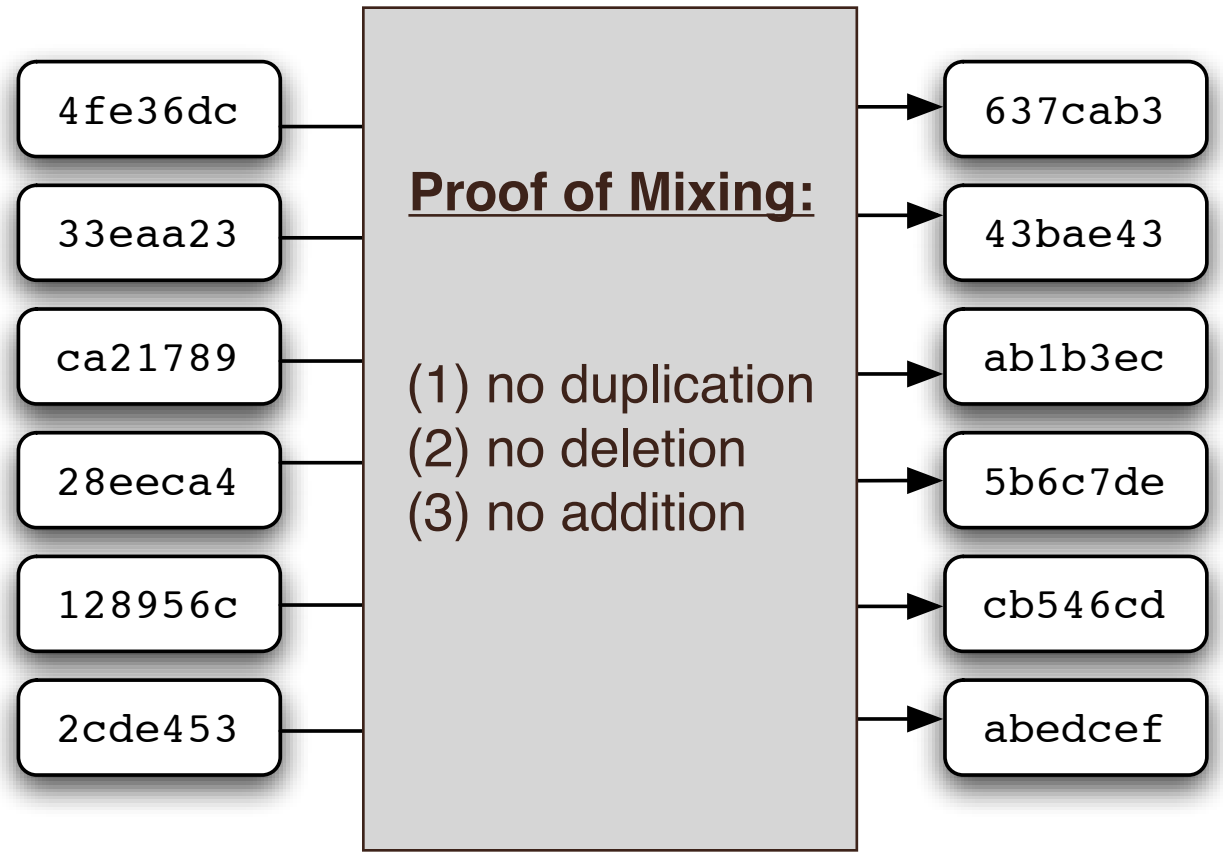


Ballot Record

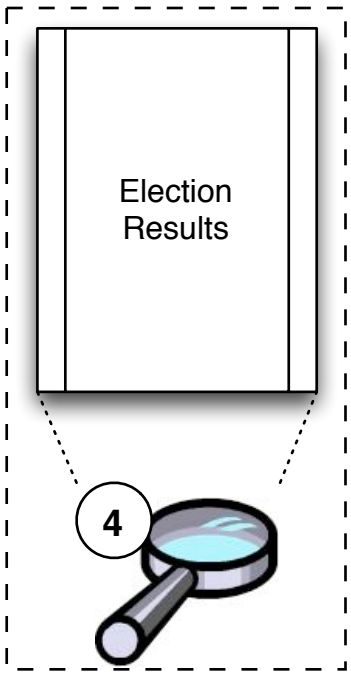


Anonymization





Tallying



637cab3	"Mickey Mouse"
43bae43	"Donald Duck"
ab1b3ec	"Donald Duck"
5b6c7de	"Mickey Mouse"
cb546cd	"Mickey Mouse"
abedcef	"Mickey Mouse"

Proof of Correct Decryption
by the Election Trustees

Summary

- Voting has contradictory requirements
- Cryptography is a useful tool
- Research is ongoing in terms of: practicality, efficiency, flexibility