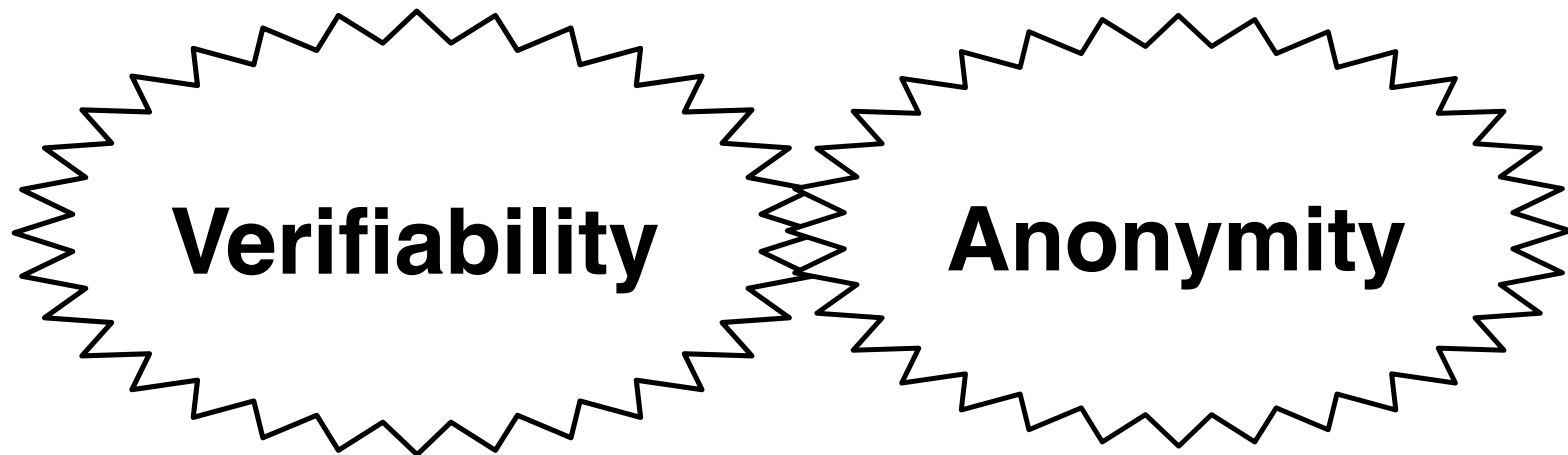


Cryptographic Voting: A Tutorial

Ben Adida
ben@mit.edu

12 February 2005

Voting is Hard



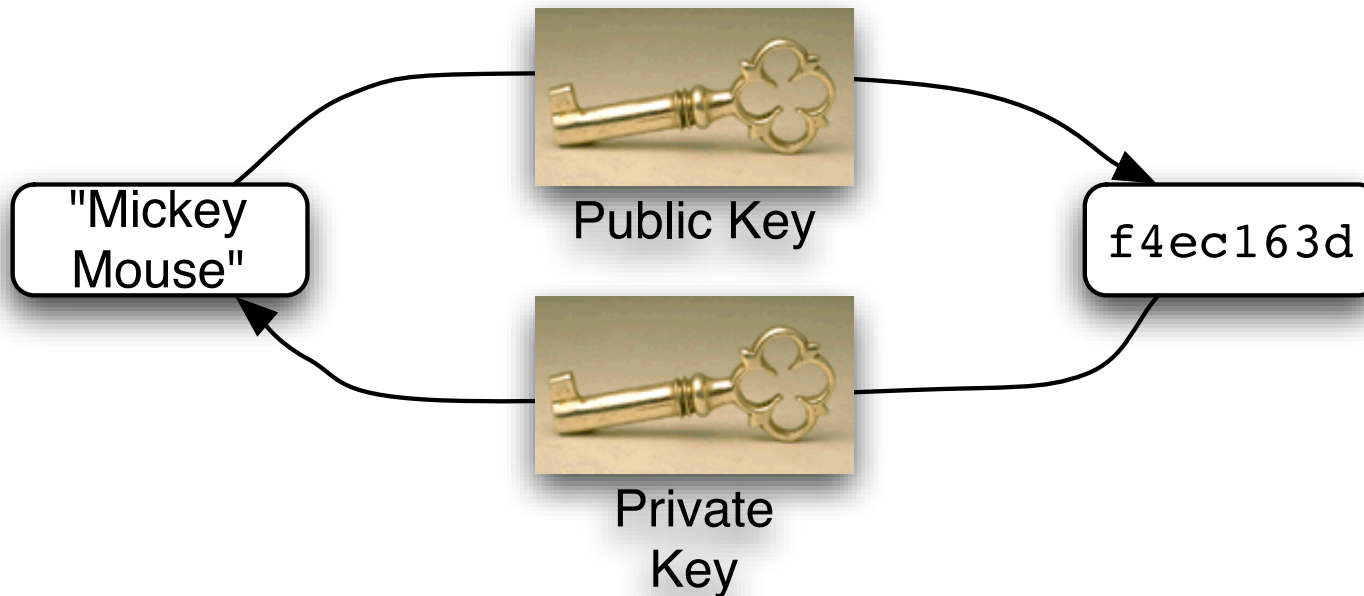
Cryptography is Useful!

“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



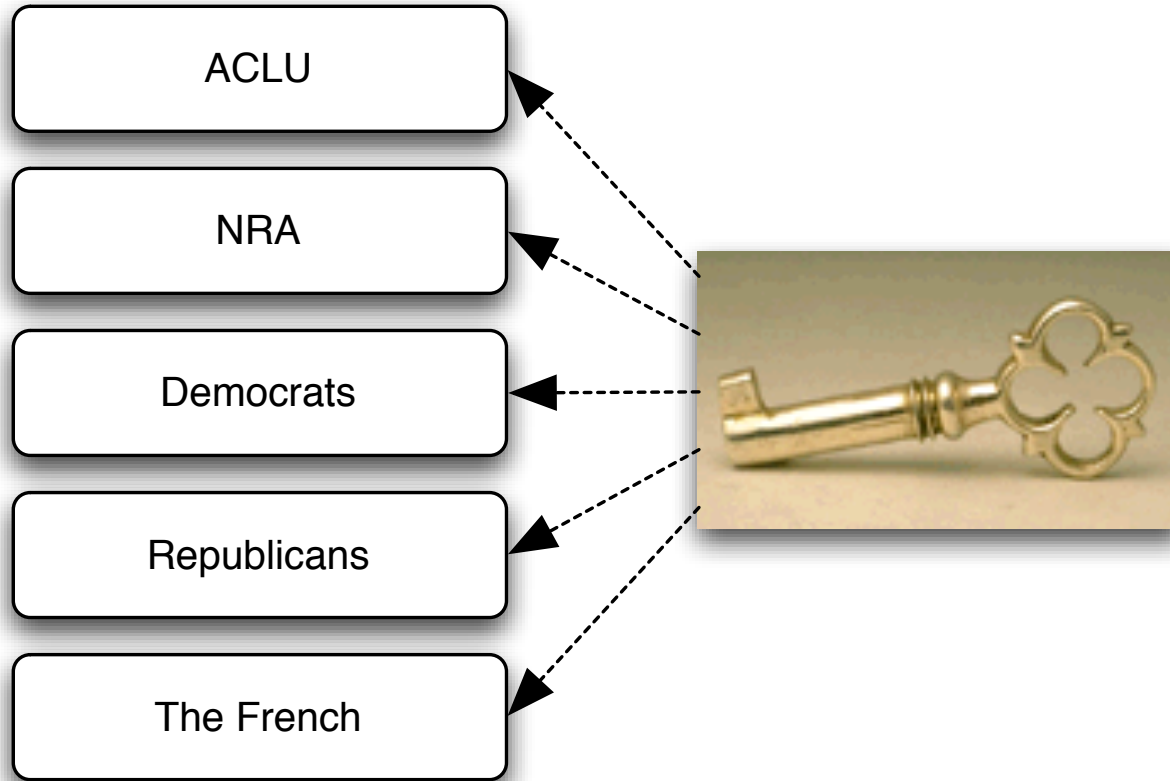
Encryption and Decryption
use **different keys**

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

f4ec163d

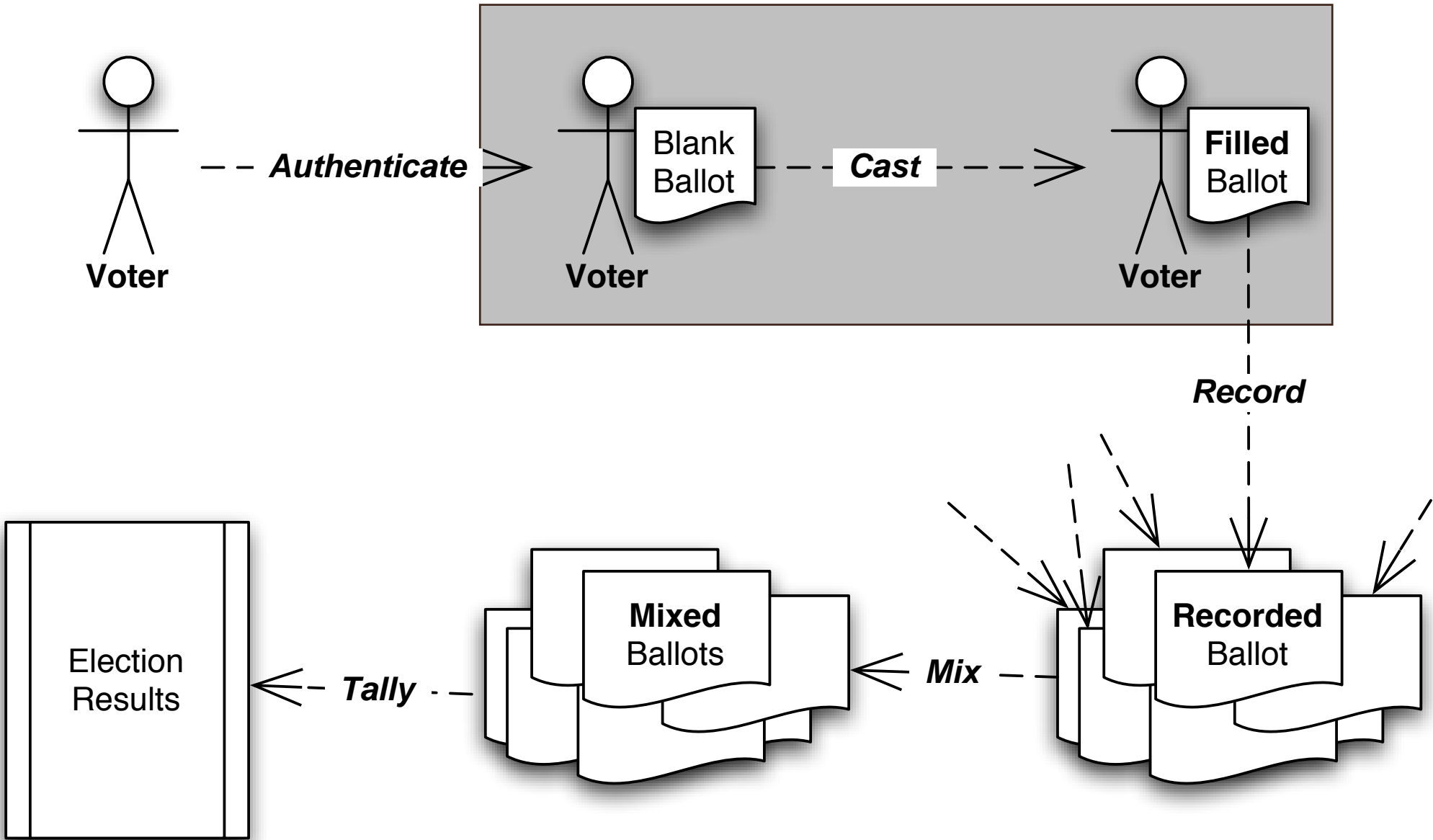
This ciphertext encodes a ballot for
“Mickey Mouse”

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!



Cast as Intended

Confusion at Palm Beach County polls

Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot's design.

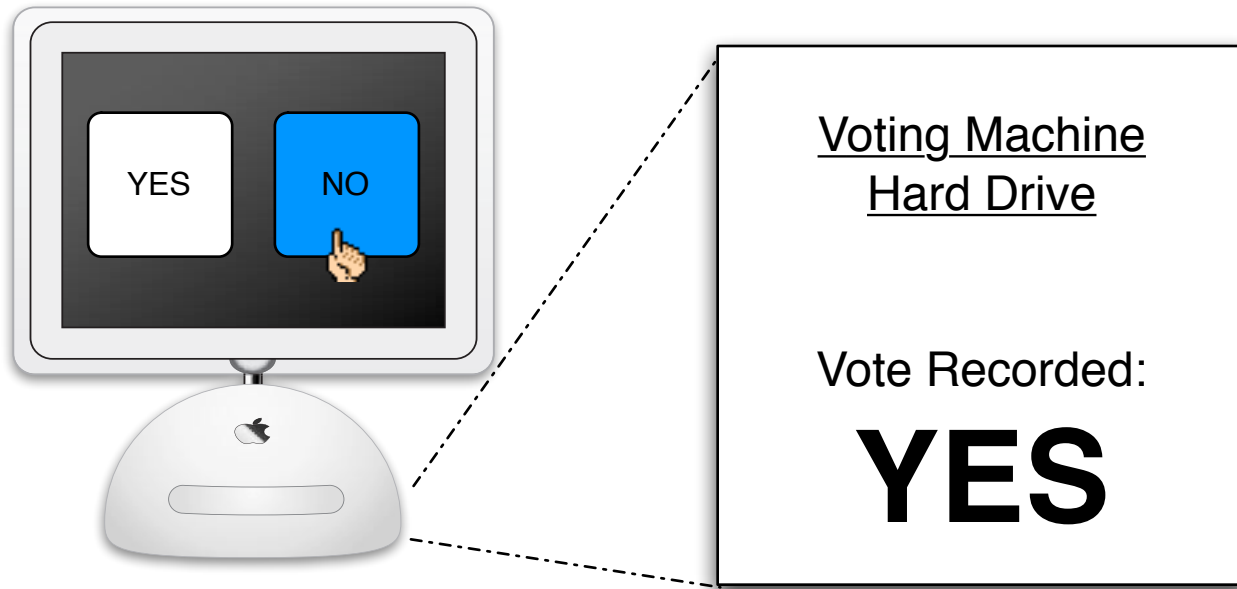
Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

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

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

Sun-Sentinel graphic

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

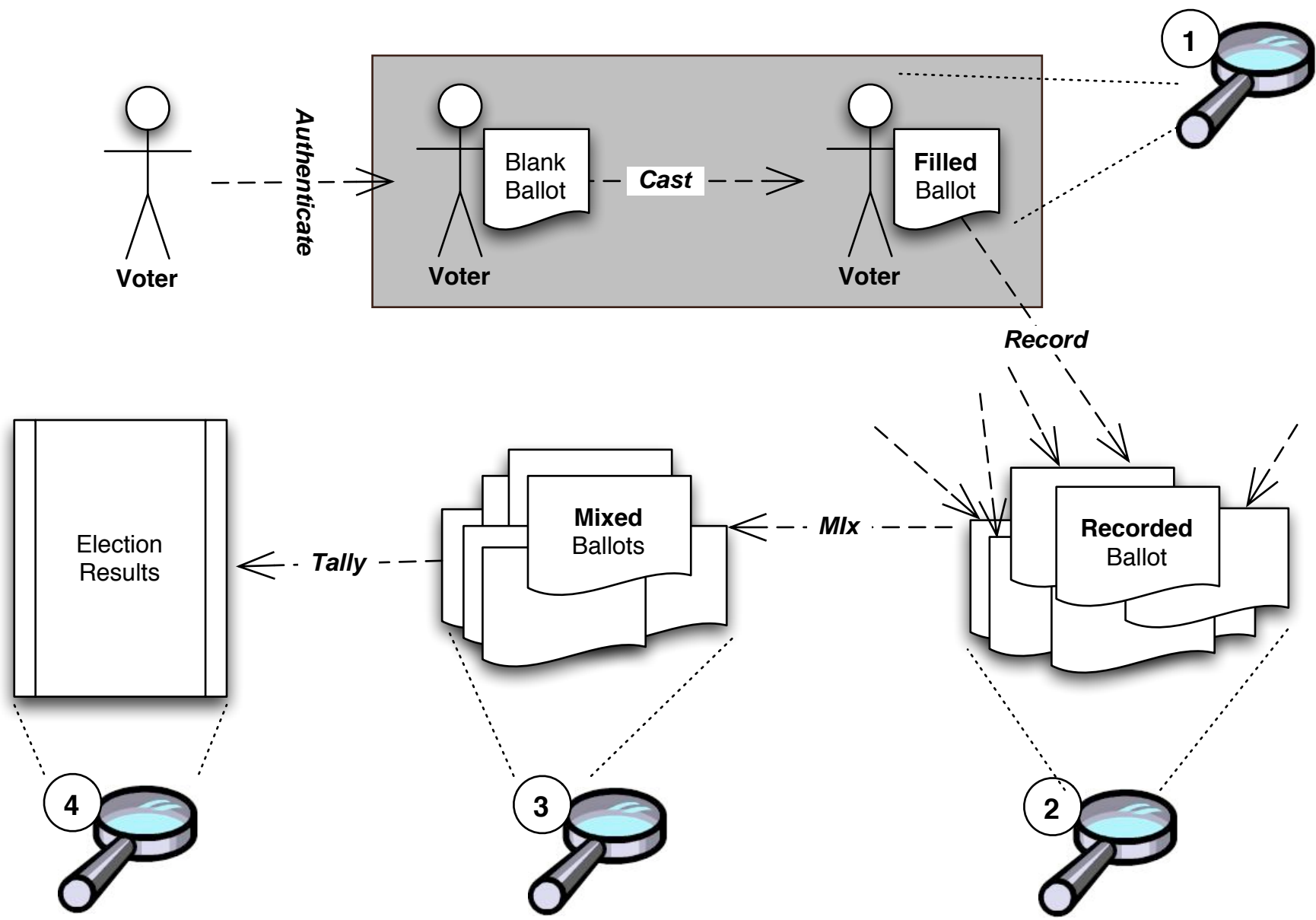
Nearly 58,000 absentee ballots for the US presidential election may never have reached Florida's Broward County voters, who had requested them more than two weeks ago, election officials said.

Scavenged ballot box lids haunt S.F. elections

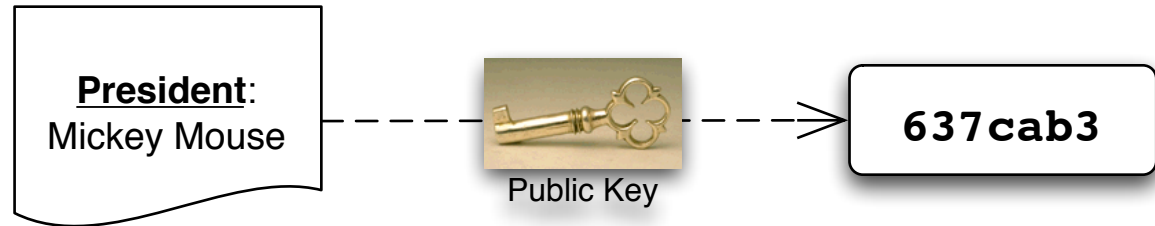
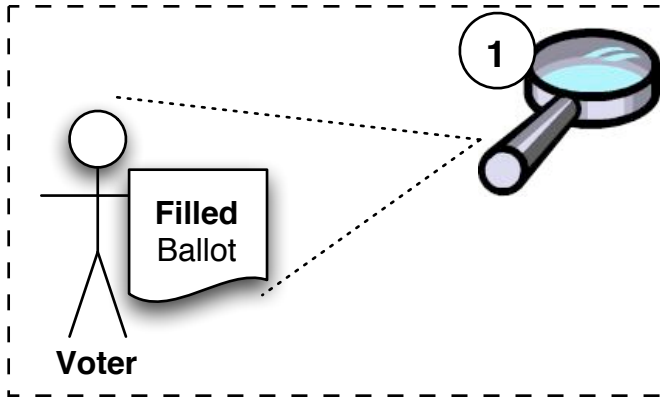
[Erin McCormick, Chronicle Staff Writer](#)

Monday, January 7, 2002

Cryptographic Voting & Universal Verifiability

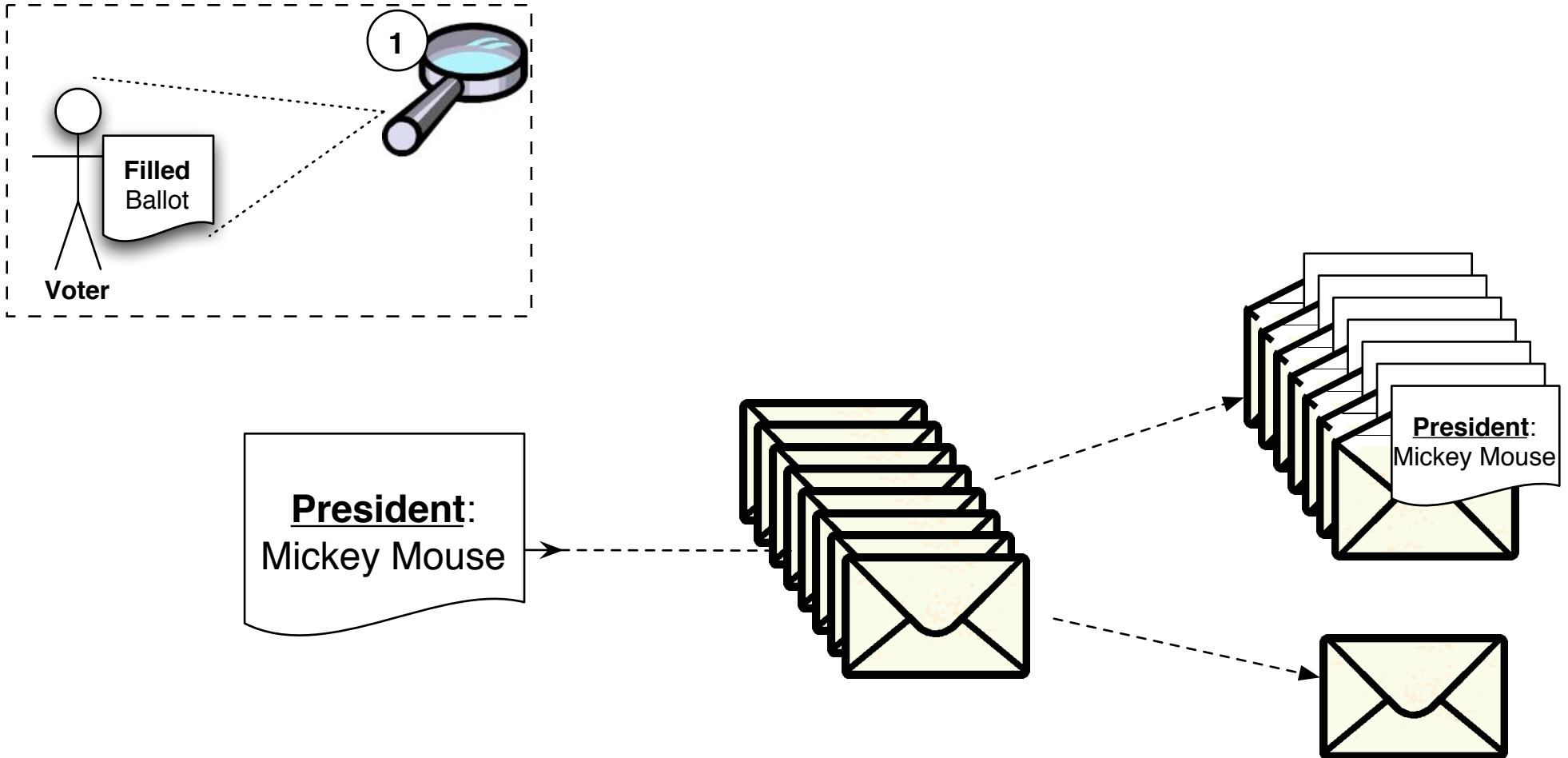


Ballot Creation

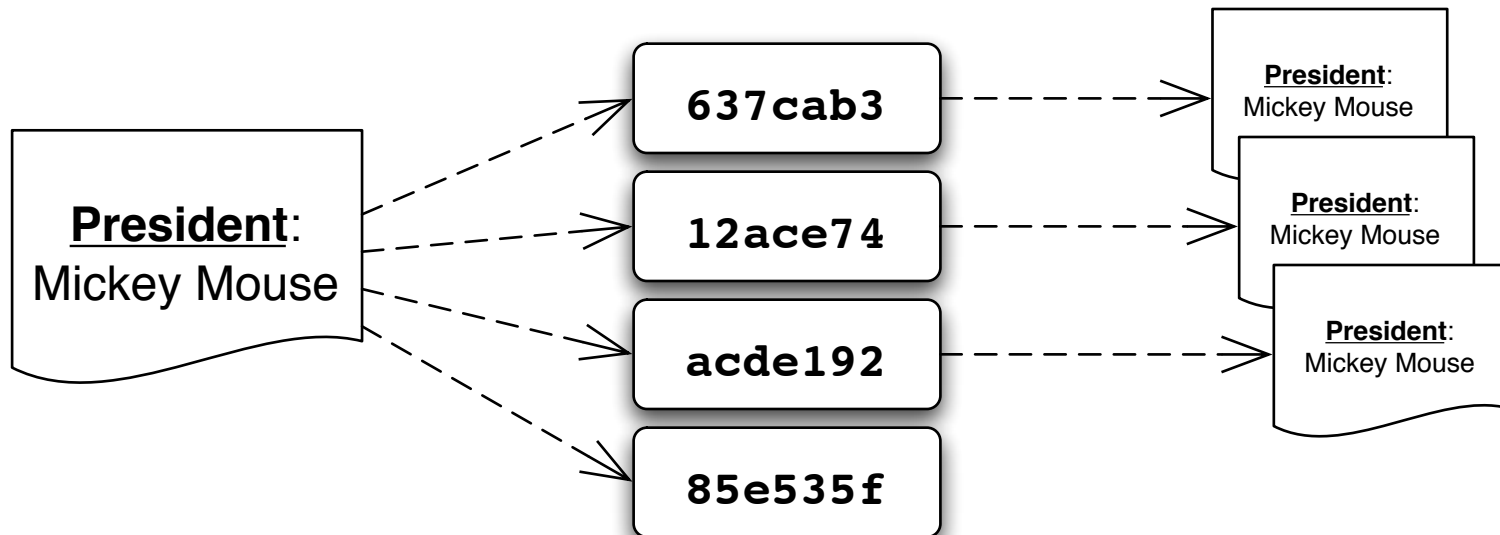
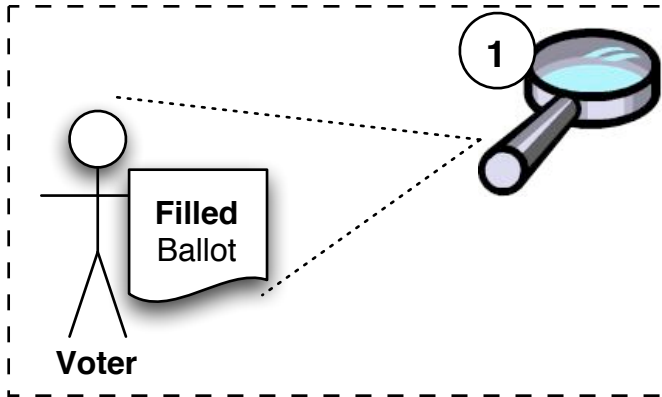


How can the voter trust the voting machine to encrypt?

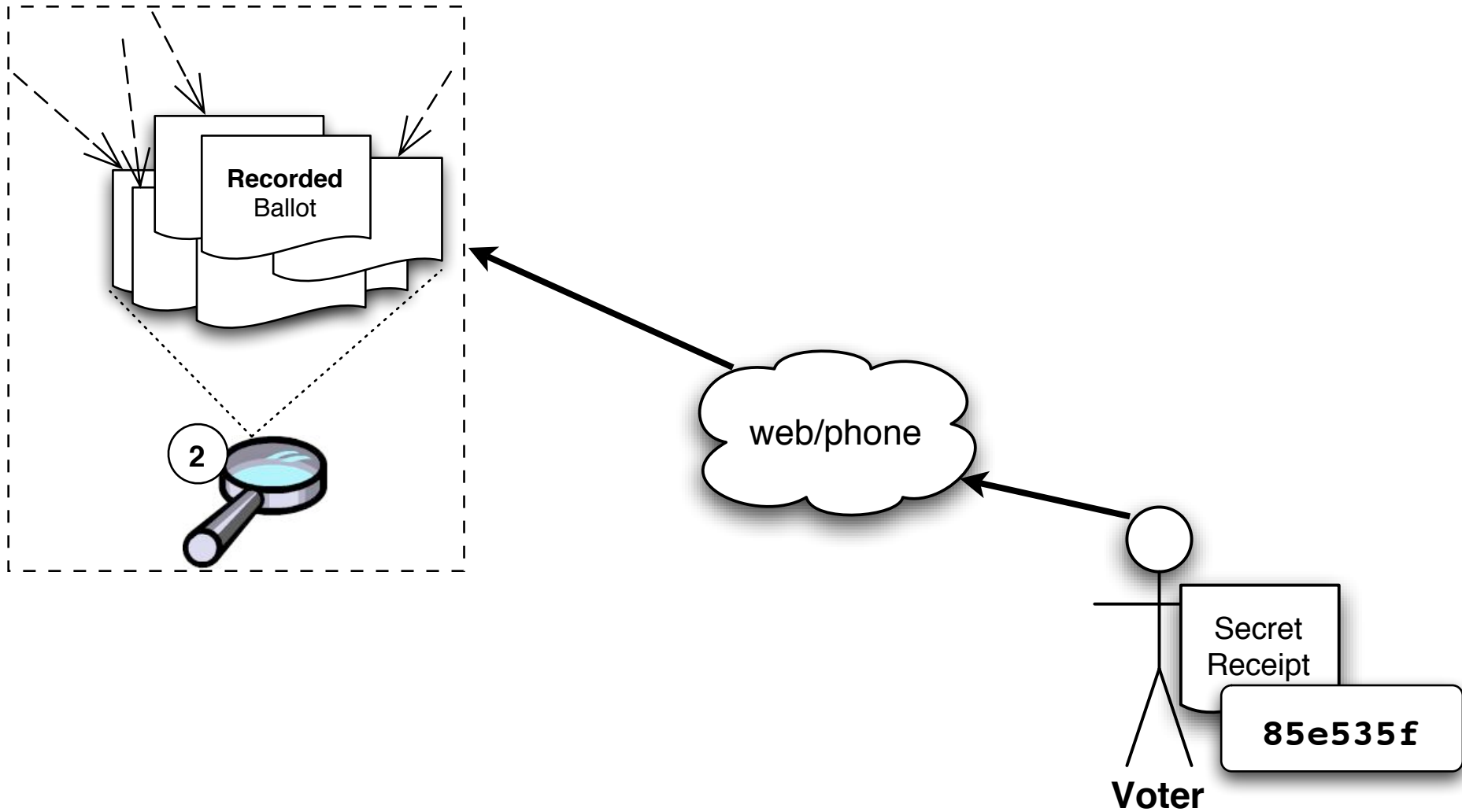
Proof of Ballot Content



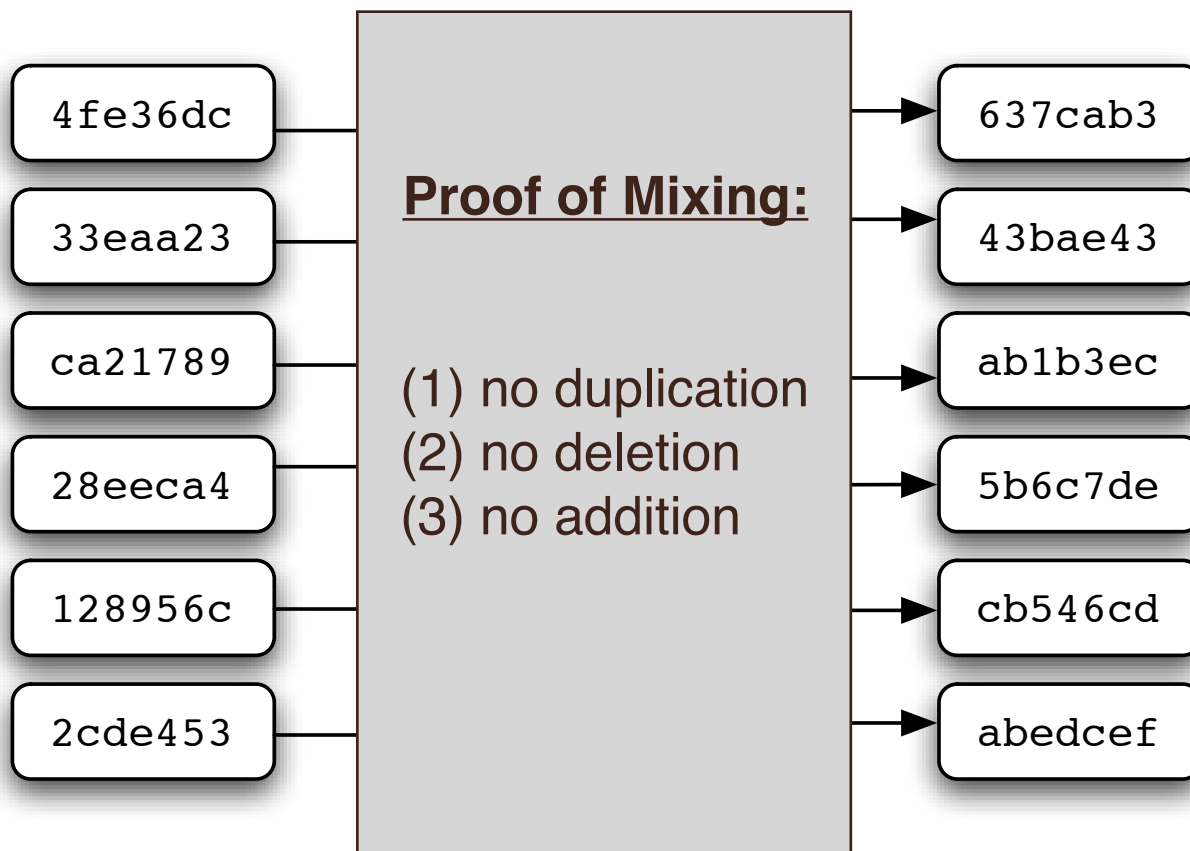
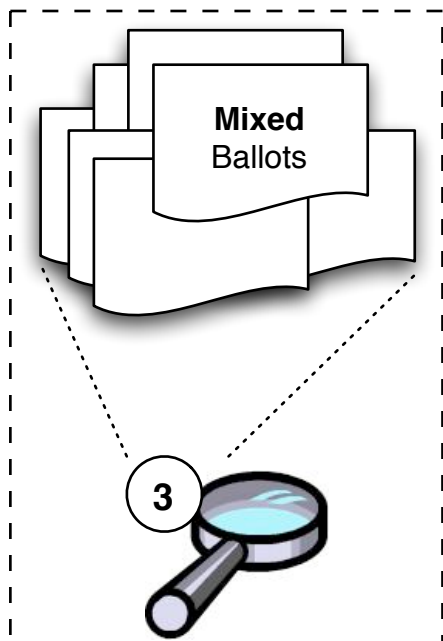
Proof of Ballot Content



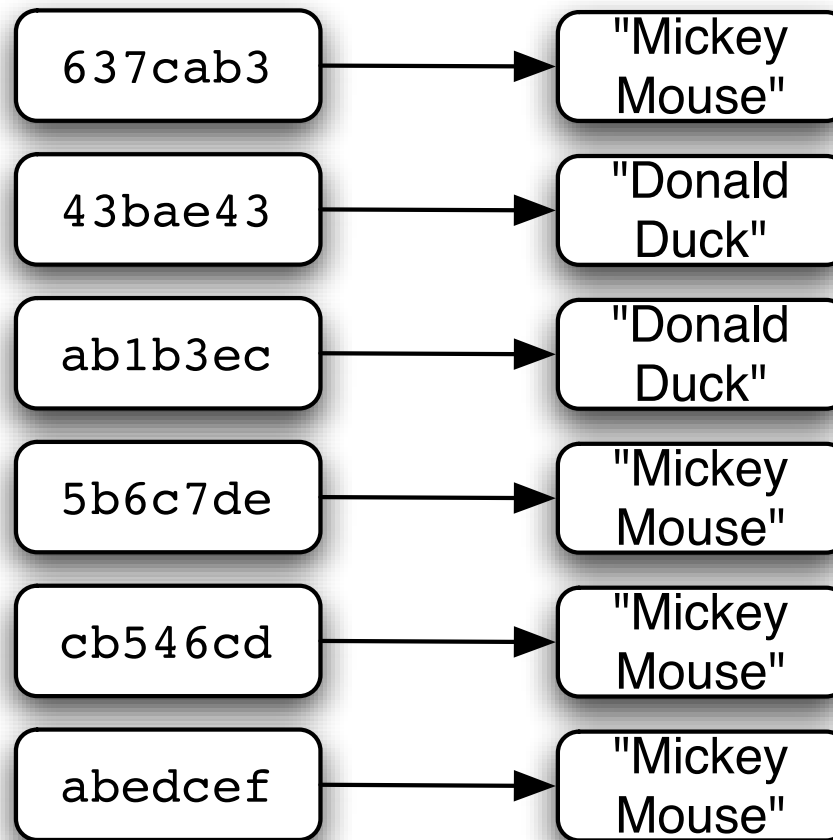
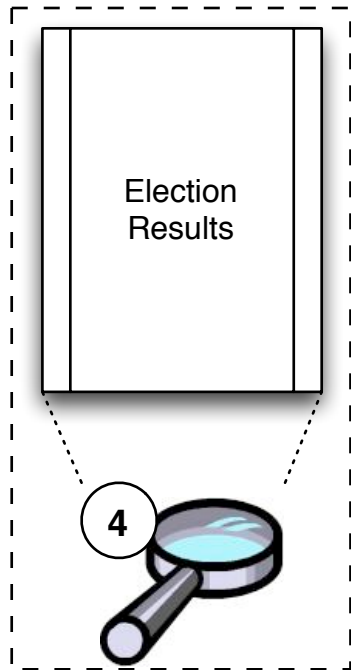
Ballot Record



Anonymization



Tallying



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