Cryptographic Voting: A Tutorial

Ben Adida
ben@mit.edu

12 February 2005
Voting is Hard

Verifiability

Anonymity
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.

"Mickey Mouse" f4ec163d

Public Key

Private Key

f4ec163d
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!
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.
Recorded as Cast

Voting Machine
Hard Drive
Vote Recorded:
YES
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?

President: Mickey Mouse

Public Key

637cab3
Proof of Ballot Content

President: Mickey Mouse

Voter Filled Ballot

1
Proof of Ballot Content

President: Mickey Mouse

Voter

Filled Ballot

1

637cab3
12ace74
acde192
85e535f

President: Mickey Mouse
President: Mickey Mouse
President: Mickey Mouse
Ballot Record

Recorded Ballot

web/phone

Voter Secret Receipt

85e535f
Anonymization

Proof of Mixing:
(1) no duplication
(2) no deletion
(3) no addition
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