“If you think cryptography is the solution to your problem....
... then you don’t understand cryptography...

... and you don’t understand your problem.”
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.
“But with cryptography, you’re just moving the black box. Few people really understand it or trust it.”

Debra Bowen
California Sec. of State, 7/30/2008
(paraphrased)
Three Points

1. Voting is a unique trust problem.
2. Cryptography is not just about secrets, it enables collaboration w/o blind trust, it democratizes auditing processes.
3. Truly Verifiable Voting is closing in on practicality.
I. 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

- Not just 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.
Voting Machine

/*
 * source
 * code
 */
if (...)

Polling Location

1
Vendor

4
Alice

3
Black Box

Results

5
Ballot Box Collection

6
Chain of Custody

Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, J

Helicopter Crash Delays Afghan 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 were somehow packed in Florida's Broward County, election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY
Published: Thursday July 6, 2006
WHERE IS MY VOTE?!
2. Cryptography is not just about secrets, it enables collaboration w/o blind trust.
Initially, cryptographers re-created physical processes in the digital arena.
Then, a realization: cryptography enables a new voting paradigm Secrecy + Auditability.
Public Ballots

Alice: Obama
Bob: McCain
Carol: Obama

Tally
Obama...2
McCain...1
Encrypted Public Ballots

Alice: Rice
Bob: Clinton
Carol: Rice

Alice verifies her vote
Everyone verifies the tally

Obama...2
McCain...1
End-to-End Verification

Alice

Polling Location

Voting Machine

Ballot Box / Bulletin Board

Vendor

Results

1

Receipt

2
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
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.
“Randomized” Encryption

Keypair consists of a public key $\text{pk}$ and a secret key $\text{sk}$.

- "Obama" $\xrightarrow{\text{Enc}_{\text{pk}}} 8b5637$
- "McCain" $\xrightarrow{\text{Enc}_{\text{pk}}} c5de34$
- "Obama" $\xrightarrow{\text{Enc}_{\text{pk}}} a4b395$
Threshold Decryption

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

\[ c = \text{Enc}_{pk_1} \left( \text{Enc}_{pk_2} \left( \text{Enc}_{pk_3}(m) \right) \right) \]

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

Vote For: Obama

This last envelope likely contains “Obama”
Zero-Knowledge Proof

Open envelopes don’t prove anything after the fact.
A little bit more math

\[ y = g^x \mod p \]

\[ S = g^r \mod p \]

\[ t = xc + r \]

\[ g^t \overset{?}{=} Sy^c \]
does this prove anything?

\[ y = g^x \mod p \]

\[ S = g^r \mod p \]

\[ t = xc + r \]
what’s so special about it?

\[ y = g^x \mod p \]

\[ S = g^r \mod p \]

\[ c \]

\[ t = xc + r \]

\[ g^t \overset{?}{=} Sy^c \]
Voter interacts with a voting machine
- Obtains a freshly printed receipt that displays the encrypted ballot
- Takes the receipt home and uses it as a tracking number.
- Receipts posted for public tally.
Paper Experience

- paper ballots with indirection between 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 (Truly Verifiable Voting) is closing in on practicality.
Benaloh Casting

Alice

"AUDIT"

"CAST"

"Obama"

Encrypted Ballot

 decrypted

 Signed

 Signed

 Encrypted

 Encrypted

 Decrypted

 Decrypted

 VERIFICATION
Many more great ideas

- Neff’s MarkPledge
  - high-assurance, human-verifiable, proofs of correct encryption
- Prêt-à-Voter by Ryan et al.
  - elegant, simple, paper-based
- STV: Ramchen, Teague, Benaloh & Moran.
  - handling complex election styles
- Scantegrity I & II
  - closely mirrors opscan voting
Deployments!

- Scantegrity II @ Takoma Park
  real municipal elections
- Université catholique de Louvain
  25,000 voters
- Scratch, Click & Vote
Three Points

1. Voting is a unique trust problem.

2. Cryptography is not just about secrets, it enables collaboration w/o blind trust, it democratizes the auditing process.

3. Truly Verifiable Voting is closing in on practicality.
My Fear: computerization of voting is inevitable. Without true verifiability, the situation is grim.
My Hope:

public auditing proofs will soon be as common as public-key crypto is now.
Challenges

**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?