Cryptography and Voting

Ben Adida
Harvard University

EVT & WOTE
August 11th, 2009
Montreal, Canada
“If you think cryptography is the solution to your problem....
... then you don’t understand cryptography...
... then you don’t understand cryptography...

... and you don’t understand your problem.”

-Peter, Butler, Bruce
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.
Three Points

1. Voting is a unique trust problem.

2. Cryptography is not just about secrets, it creates trust between competitors, it democratizes the auditing process.

3. Open-Audit Voting is closing in on practicality.
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

- Dan Wallach’s great rump session talk.
- More than 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.
Vendor

```c
if (...) {
    /* source code */
}
```
/* source code */
if (...)
Voting
Machine

 Polling Location

Alice

Vendor

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

1

2

3

4
```c
/* source
 * code
*/
if (...) { /* code */
```
Chain of Custody
Scavenged ballot box lids haunt S.F. elections

Erin McCormick, Chronicle Staff Writer

Monday, January 7, 2002
Chain of Custody

Scavenged ballot box lids haunt S.F. elections

Erin McC

Helicopter Crash Delays Afghan Vote Count

Helicopter sent to pick up Afghan ballots in remote province crash-lands, delaying vote count
Scavenged ballot box lids haunt S.F. elections

Helicopter Crash Delays Afghan Vote Count

Absentee ballots 'lost' in Florida

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.
Chain of Custody

Scavenged ballot box lids haunt S.F. elections

Helicopter Crash Delays Afghan Vote Count

Absentee ballots 'lost' in Florida

Nearly 58,000 absentee ballots for the US presidential election were somehow misplaced, Florida's Broward County election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY
Published: Thursday July 6, 2006
Initially, cryptographers re-created physical processes in the digital arena.
Then, a realization: cryptography enables a new voting paradigm

Secrecy + Auditability.
WHERE IS MY VOTE?!
Public Ballots

Bob: McCain
Carol: Obama
Public Ballots

Alice

Bob: McCain

Carol: Obama
Public Ballots

Alice: Obama
Bob: McCain
Carol: Obama

Alice
Public Ballots

Alice: Obama
Bob: McCain
Carol: Obama

Tally
Obama: 2
McCain: 1
Encrypted Public Ballots

Alice: 
Bob: 
Carol: 

Tally

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

Alice: Rice
Bob: Clinton
Carol: Rice

Alice verifies her vote

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

Alice: Rice
Bob: Clinton
Carol: Rice

Obama: 2
McCain: 1

Alice verifies her vote
Everyone verifies the tally
End-to-End Verification
End-to-End Verification

Voting Machine

Vendor

Polling Location

/*
 * source
 * code
 */

if (...
End-to-End Verification

Voting Machine

Polling Location

Vendor

Ballot Box / Bulletin Board

Alice

Results

if (...)
End-to-End Verification

Voting Machine

Vendor

Polling Location

Ballot Box / Bulletin Board

Alice

Receipt

Results

/*
  * source
  * code
  */

if (...)

1
End-to-End Verification

1. Receipt
2. Results

Voting Machine

Polling Location

Vendor

Alice
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 Voting.
2. Cryptography is not just about secrets, creates trust between competitors.
NO!

Increased transparency when some data must remain secret.
So, yes, we encrypt, and then we operate on 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
“Randomized” Encryption

Keypair consists of a public key $pk$ and a secret key $sk$. 
“Randomized” Encryption

Keypair consists of a public key $pk$ and a secret key $sk$.

"Obama" $\xrightarrow{\text{Enc}_{pk}}$ 8b5637
“Randomized” Encryption

Keypair consists of a public key $pk$ and a secret key $sk$.

\[
\begin{align*}
\text{"Obama"} & \quad \text{Enc}_{pk} \quad 8b5637 \\
\text{"McCain"} & \quad \text{Enc}_{pk} \quad c5de34
\end{align*}
\]
“Randomized” Encryption

Keypair consists of a public key $pk$ and a secret key $sk$.

- Encrypted "Obama" with $pk$: $8b5637$
- Encrypted "McCain" with $pk$: $c5de34$
- Encrypted "Obama" with $pk$: $a4b395$
Threshold Decryption

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

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

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

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

\[ 8\text{b5637} \xrightarrow{\text{Dec}_{sk_1}} 739\text{cb} \]
\[ 8\text{b5637} \xrightarrow{\text{Dec}_{sk_2}} 261\text{ad7} \]
\[ 8\text{b5637} \xrightarrow{\text{Dec}_{sk_3}} 7231\text{bc} \]
Threshold Decryption

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

\[
\begin{align*}
\text{Dec}_{sk_1} & \rightarrow b739cb \\
\text{Dec}_{sk_2} & \rightarrow 261ad7 \\
\text{Dec}_{sk_3} & \rightarrow 7231bc \\
\text{Dec}_{sk_4} & \rightarrow 8239ba \\
\end{align*}
\]
Threshold Decryption

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

\[
\begin{align*}
\text{Dec}_{sk_1} & \rightarrow b739cb \\
\text{Dec}_{sk_2} & \rightarrow 261ad7 \\
\text{Dec}_{sk_3} & \rightarrow 7231bc \\
\text{Dec}_{sk_4} & \rightarrow 8239ba
\end{align*}
\]

"Obama"
Homomorphic Encryption
Homomorphic Encryption

\[ \text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 + m_2) \]
Homomorphic Encryption

\[ \text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 + m_2) \]
Homomorphic Encryption

\[ \text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 + m_2) \]

\[ g^{m_1} \times g^{m_2} = g^{m_1 + m_2} \]
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
Zero-Knowledge Proof

Vote For: Obama

Vote For: Obama
Zero-Knowledge Proof

Vote For: Obama

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

Open envelopes don’t prove anything after the fact.
Electronic Experience

- 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

- Pre-print paper ballots with some 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 (Open-Audit Voting) is closing in on practicality.
Benaloh Casting
Benaloh Casting
Benaloh Casting

Alice → "Obama" → [device image]
Benaloh Casting

Alice → "Obama" → Encrypted Ballot

38
Benaloh Casting

Alice

"Obama"

Encrypted Ballot

Alice
Benaloh Casting

Alice

"Obama"

Encrypted Ballot

Alice

"AUDIT"
Benaloh Casting

Alice

"Obama"

Encrypted Ballot

Alice

"AUDIT"

Decrypted Ballot
Benaloh Casting

Alice

"Obama"

Encrypted Ballot

Decrypted Ballot

"AUDIT"

Alice

Verification

Encrypted Ballot

Decrypted Ballot
Benaloh Casting

Alice

Encrypted Ballot

"Obama"

Decrypted Ballot

VERIFICATION

Encrypted Ballot

Decrypted Ballot
Benaloh Casting

Alice

"AUDIT"

Encrypted Ballot

"Obama"

Decrypted Ballot

VERIFICATION

Encrypted Ballot

Decrypted Ballot
Benalohh Casting

Alice

"Obama"

Encrypted Ballot

VERIFICATION

Decrypted Ballot

Decrypted Ballot

"AUDIT"

Alice

Alice

Encrypted Ballot

Decrypted Ballot
Benaloh Casting

Alice

"AUDIT"

Alice

"CAST"

Encrypted Ballot

"Obama"

Decrypted Ballot

VERIFICATION

Encrypted Ballot

Decrypted Ballot
Benaloh Casting

Alice

"AUDIT"

Decrypted Ballot

Alice

"CAST"

Signed Encrypted Ballot

VERIFICATION

Encrypted Ballot

Decrypted Ballot

"Obama"

Encrypted Ballot
Benaloh Casting

"AUDIT"

Alice

Encrypted Ballot

"Obama"

Signed Encrypted Ballot

"CAST"

Alice

VERIFICATION
Benaloh Casting

Alice

Encrypted Ballot

"Obama"

Alice

Decrypted Ballot

VERIFICATION

Alice

"AUDIT"

Decrypted Ballot

Alice

"CAST"

Signed Encrypted Ballot

Alice

Signed Encrypted Ballot

Alice

Encrypted Ballot

Decrypted Ballot
Many more great ideas

- Neff’s MarkPledge
  - high-assurance, human-verifiable, proofs of correct encryption

- Scantegrity
  - closely mirrors opscan voting

- ThreeBallot by Rivest
  - teaching the concept of open-audit without deep crypto

- STV: Ramchen, Teague, Benaloh & Moran.
  - handling complex election styles

- Prêt-à-Voter by Ryan et al.
  - elegant, simple, paper-based
Deployments!

- UCL (25,000 voters)
- Scantegrity @ Takoma Park
- SCV
Three Points

1. Voting is a unique trust problem.
2. Cryptography is not just about secrets, it creates trust between competitors, it democratizes the auditing process.
3. Open-Audit Voting is closing in on practicality.
My Fear:
computerization of voting is inevitable. Without open-audit, the situation is grim.
My Hope:
proofs for auditing partially-secret processes will soon be as common as public-key crypto is now.
Challenge:

Ed Felten: “you have no voter privacy, deal with it.”
Challenge:

Ed Felten: “you have no voter privacy, deal with it.”
Questions?