Practical Aspects of Modern Cryptography

Winter 2011

Josh Benaloh
Brian LaMacchia
Some Tools We’ve Developed

- Homomorphic Encryption
- Secret Sharing
- Verifiable Secret Sharing
- Threshold Encryption
- Interactive Proofs
Secret Sharing Homomorphisms

Many secret sharing methods have an additional useful feature:

If two secrets are separately shared amongst the same set of people in the same way, then the sum of the individual shares constitute shares of the sum of the secrets.
Secret Sharing Homomorphisms

**OR**

Secret: $a$ – Shares: $a, a, ..., a$

Secret: $b$ – Shares: $b, b, ..., b$

Secret sum: $a + b$

Share sums: $a + b, a + b, ..., a + b$
Secret Sharing Homomorphisms

AND

Secret: $a$ – Shares: $a_1, a_2, ..., a_n$
Secret: $b$ – Shares: $b_1, b_2, ..., b_n$

Secret sum: $a + b$
Share sums: $a_1 + b_1, a_2 + b_2, ..., a_n + b_n$
Secret Sharing Homomorphisms

THRESHOLD

Secret: $P_1(0)$ — Shares: $P_1(1), P_1(2), ..., P_1(n)$
Secret: $P_2(0)$ — Shares: $P_2(1), P_2(2), ..., P_2(n)$

Secret sum: $P_1(0) + P_2(0)$
Share sums: $P_1(1) + P_2(1), P_1(2) + P_2(2), ..., P_1(n) + P_2(n)$
Threshold Encryption

I want to encrypt a secret message $M$ for a set of $n$ recipients such that

- any $k$ of the $n$ recipients can uniquely decrypt the secret message $M$,
- but any set of fewer than $k$ recipients has no information whatsoever about the secret message $M$. 

March 3, 2011
Recall Diffie-Hellman

**Alice**

- Randomly select a large integer $a$ and send $A = g^a \mod p$.
- Compute the key $K = B^a \mod p$.

**Bob**

- Randomly select a large integer $b$ and send $B = g^b \mod p$.
- Compute the key $K = A^b \mod p$.

$B^a = g^{ba} = g^{ab} = A^b$
ElGamal Encryption
ElGamal Encryption

- Alice selects a large random private key $a$ and computes an associated public key $A = g^a \mod p$. 
ElGamal Encryption

- Alice selects a large random private key $a$ and computes an associated public key $A = g^a \mod p$.
- To send a message $M$ to Alice, Bob selects a random value $r$ and computes the pair $(X, Y) = (A^r M \mod p, g^r \mod p)$.
ElGamal Encryption

- Alice selects a large random private key $a$ and computes an associated public key $A = g^a \mod p$.
- To send a message $M$ to Alice, Bob selects a random value $r$ and computes the pair
  $$(X, Y) = (A^r M \mod p, g^r \mod p).$$
- To decrypt, Alice computes
  $$X/Y^a \mod p = A^r M/g^{ra} \mod p = M.$$
ElGamal Re-Encryption

If $A = g^a \mod p$ is a public key and the pair

$$(X, Y) = (A^r M \mod p, g^r \mod p)$$

is an encryption of message $M$, then for any value $c$, the pair

$$(A^c X, g^c Y) = (A^{c+r} M \mod p, g^{c+r} \mod p)$$

is an encryption of the same message $M$, for any value $c$. 
Group ElGamal Encryption
Group ElGamal Encryption

- Each recipient selects a large random private key $a_i$ and computes an associated public key $A_i = g^{a_i} \mod p$. 
Group ElGamal Encryption

- Each recipient selects a large random private key $a_i$ and computes an associated public key $A_i = g^{a_i} \text{ mod } p$.
- The group key is $A = \prod A_i \text{ mod } p = g^{\sum a_i} \text{ mod } p$. 
Group ElGamal Encryption

- Each recipient selects a large random private key $a_i$ and computes an associated public key $A_i = g^{a_i} \mod p$.
- The group key is $A = \prod A_i \mod p = g^{\sum a_i} \mod p$.
- To send a message $M$ to the group, Bob selects a random value $r$ and computes the pair $(X, Y) = (A^r M \mod p, g^r \mod p)$. 

March 3, 2011

Practical Aspects of Modern Cryptography

17
Group ElGamal Encryption

- Each recipient selects a large random private key $a_i$ and computes an associated public key $A_i = g^{a_i} \mod p$.
- The group key is $A = \prod A_i \mod p = g^\sum a_i \mod p$.
- To send a message $M$ to the group, Bob selects a random value $r$ and computes the pair $(X, Y) = (A^r M \mod p, g^r \mod p)$.
- To decrypt, each group member computes $Y_i = Y^{a_i} \mod p$. The message $M = X / \prod Y_i \mod p$. 
Threshold Encryption (ElGamal)
Threshold Encryption (ElGamal)

- Each recipient selects $k$ large random secret coefficients $a_{i,0}, a_{i,1}, ..., a_{i,k-2}, a_{i,k-1}$ and forms the polynomial $P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0}$
Threshold Encryption (ElGamal)

- Each recipient selects $k$ large random secret coefficients $a_{i,0}, a_{i,1}, \ldots, a_{i,k-2}, a_{i,k-1}$ and forms the polynomial
  \[ P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0} \]

- Each polynomial $P_i(x)$ is then verifiably shared with the other recipients by distributing each $g^{a_{i,j}}$. 
Threshold Encryption (ElGamal)

- Each recipient selects \( k \) large random secret coefficients \( a_{i,0}, a_{i,1}, ..., a_{i,k-2}, a_{i,k-1} \) and forms the polynomial
  \[ P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + ... + a_{i,1}x + a_{i,0} \]
- Each polynomial \( P_i(x) \) is then verifiably shared with the other recipients by distributing each \( g^{a_{i,j}} \).
- The joint (threshold) public key is \( \prod g^{a_{i,0}} \).
Threshold Encryption (ElGamal)

- Each recipient selects $k$ large random secret coefficients $a_{i,0}, a_{i,1}, ..., a_{i,k-2}, a_{i,k-1}$ and forms the polynomial $P_i(x) = a_{i,k-1}x^{k-1} + a_{i,k-2}x^{k-2} + \cdots + a_{i,1}x + a_{i,0}$
- Each polynomial $P_i(x)$ is then verifiably shared with the other recipients by distributing each $g^{a_{i,j}}$.
- The joint (threshold) public key is $\prod g^{a_{i,0}}$.
- Any set of $k$ recipients can form the secret key $\sum a_{i,0}$ to decrypt.
An Application

Verifiable Elections
Verifiable Election Technologies

As a voter, you can check that

• your vote is correctly recorded
• all recorded votes are correctly counted

...even in the presence of malicious software, hardware, and election officials.
Traditional Voting Methods
Traditional Voting Methods

- Hand-Counted Paper

Vote for one option.

- Joe Smith
- John Citizen
- Jane Doe
- Fred Rubble
- Mary Hill
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
- Touch-Screen Terminals
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
- Touch-Screen Terminals
- Various Hybrids
Vulnerabilities and Trust

- All of these systems have substantial vulnerabilities.

- All of these systems require trust in the honesty and expertise of election officials (and usually the equipment vendors as well).

Can we do better?
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective

- As a voter, you don’t really know what happens behind the curtain.
The Voter’s Perspective

- As a voter, you don’t really know what happens behind the curtain.

- You have no choice but to trust the people working behind the curtain.
The Voter’s Perspective

- As a voter, you don’t really know what happens behind the curtain.

- You have no choice but to trust the people working behind the curtain.

- You don’t even get to choose the people who you will have to trust.
Fully-Verifiable Election Technologies (End-to-End Verifiable)
Fully-Verifiable Election Technologies (End-to-End Verifiable)

Allows voters to track their individual (sealed) votes and ensure that they are properly counted...
Fully-Verifiable Election Technologies (End-to-End Verifiable)

Allows voters to track their individual (sealed) votes and ensure that they are properly counted...

... even in the presence of faulty or malicious election equipment ...
Fully-Verifiable Election Technologies (End-to-End Verifiable)

Allows voters to track their individual (sealed) votes and ensure that they are properly counted...

... even in the presence of faulty or malicious election equipment ...

... and/or careless or dishonest election personnel.
Voters can check ...
Voters can check ...

... that their (sealed) votes have been properly recorded
Voters can check ...

... that their (sealed) votes have been properly recorded

... and that *all* recorded votes have been properly counted
Voters can check ...

... that their (sealed) votes have been properly recorded

... and that all recorded votes have been properly counted

This is not just checking a claim that the right steps have been taken ...
Voters can check ...

... that their (sealed) votes have been properly recorded

... and that all recorded votes have been properly counted

This is *not* just checking a claim that the right steps have been taken ...

This is actually a check that the counting is correct.
Where is My Vote?
Where is My Vote?

- Alice Johnson, 123 Main – Yes
- Bob Ramirez, 79 Oak – No
- Carol Wilson, 821 Market – No
End-to-End Verifiability
End-to-End Verifiability

As a voter, I can be sure that
End-to-End Verifiability

As a voter, I can be sure that

- My vote is
End-to-End Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
End-to-End Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
  - Counted as cast
End-to-End Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
  - Counted as cast
- All votes are counted as cast
End-to-End Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
  - Counted as cast
- All votes are counted as cast

... without having to trust *anyone* or *anything*.
One Thing Missing ...
One Thing Missing ...

... that pesky little secret-ballot requirement.
One Thing Missing ...

... that pesky little *secret-ballot* requirement.

Elections would be sooooooo... much easier without it.
Full Voter-Verifiability is Possible
Full Voter-Verifiability is Possible

Even though this “toy” public election is not secret-ballot, it’s enough to show that voter-verifiability is possible
Full Voter-Verifiability is Possible

Even though this “toy” public election is not secret-ballot, it’s enough to show that voter-verifiability is possible ... and also to falsify arguments that electronic elections are inherently untrustworthy.
Privacy
Privacy

- The only ingredient missing from this *transparent* election is privacy – and the things which flow from privacy (e.g. protection from coercion).
Privacy

- The only ingredient missing from this *transparent* election is privacy – and the things which flow from privacy (e.g. protection from coercion).

- Performing tasks while preserving privacy is the bailiwick of cryptography.
Privacy

- The only ingredient missing from this *transparent* election is privacy – and the things which flow from privacy (e.g. protection from coercion).

- Performing tasks while preserving privacy is the bailiwick of cryptography.

- Cryptographic techniques can enable *end-to-end verifiable* elections while preserving voter privacy.
Where is My Vote?

Alice Johnson, 123 Main

Bob Ramirez, 79 Oak

Carol Wilson, 821 Market
Where is My Vote?

Alice Johnson, 123 Main

Bob Ramirez, 79 Oak

Carol Wilson, 821 Market
Where is My Vote?
Where is *My* Vote?
Where is My Vote?

No – 2
Yes – 1
Where is *My* Vote?

No – 2
Yes – 1

Mathematical Proof
The Voter’s Perspective
The Voter’s Perspective

Verifiable election systems can be built to look exactly like current systems ...
The Voter’s Perspective

Verifiable election systems can be built to look exactly like current systems ...

... with one addition ...
A Verifiable Receipt
A Verifiable Receipt
A Verifiable Receipt

Precinct 37 – Machine 4
Nov. 6, 2012  1:39PM

Vote receipt tag:
7A34ZR9K4BX

***VOTE CONFIRMED***
The Voter’s Perspective
The Voter’s Perspective

Voters can ...
The Voter’s Perspective

Voters can ...

- Use receipts to check their results are properly recorded on a public web site.
The Voter’s Perspective

Voters can ...

- Use receipts to check their results are properly recorded on a public web site.
- Throw their receipts in the trash.
The Voter’s Perspective

Voters can ...
The Voter’s Perspective

Voters can ...

- Write their own applications to verify the mathematical proof of the tally.
The Voter’s Perspective

Voters can ...

- Write their own applications to verify the mathematical proof of the tally.
- Download verification apps from sources of their choice.
The Voter’s Perspective

Voters can ...

- Write their own applications to verify the mathematical proof of the tally.
- Download verification apps from sources of their choice.
- Believe verifications done by their political parties, LWV, ACLU, etc.
The Voter’s Perspective

Voters can ...

- Write their own applications to verify the mathematical proof of the tally.
- Download verification apps from sources of their choice.
- Believe verifications done by their political parties, LWV, ACLU, etc.
- Accept the results without question.
So How Does It Work?
Secure MPC is not Enough
Secure MPC is *not* Enough

- Secure Multi-Party Computation allows *any* public function to be computed on any number of private inputs *without* compromising the privacy of the inputs.
Secure MPC is *not* Enough

- Secure Multi-Party Computation allows *any* public function to be computed on any number of private inputs *without* compromising the privacy of the inputs.

- But secure MPC does not prevent parties from revealing their private inputs if they so choose.
End-to-End Verifiable Elections

Two principle phases ...
End-to-End Verifiable Elections

Two principle phases ... 

1. Voters publish their names and encrypted votes.
End-to-End Verifiable Elections

Two principle phases...

1. Voters publish their names and encrypted votes.

2. At the end of the election, administrators compute and publish the tally together with a cryptographic proof that the tally “matches” the set of encrypted votes.
End-to-End Verifiable Elections

Two questions must be answered ...
End-to-End Verifiable Elections

Two questions must be answered ...

• How do voters turn their preferences into encrypted votes?
End-to-End Verifiable Elections

Two questions must be answered ...

• How do voters turn their preferences into encrypted votes?

• How are voters convinced that the published set of encrypted votes corresponds to the announced tally?
Is it *Really* This Easy?
Is it *Really* This Easy?

Yes ...
Is it Really This Easy?

Yes ...

... but there are lots of details to get right.
Fundamental Tallying Decision
Fundamental Tallying Decision

There are essentially two paradigms to choose from ...
Fundamental Tallying Decision

There are essentially two paradigms to choose from ...

- Anonymized Ballots
Fundamental Tallying Decision

There are essentially two paradigms to choose from ...

- Anonymized Ballots (Mix Networks)
Fundamental Tallying Decision

There are essentially two paradigms to choose from ... 

- Anonymized Ballots
  (Mix Networks)

- Ballotless Tallying
Fundamental Tallying Decision

There are essentially two paradigms to choose from ... 

• Anonymized Ballots
  (Mix Networks)

• Ballotless Tallying
  (Homomorphic Encryption)
Anonymized Ballots
Ballotless Tallying
Homomorphic Tallying
Homomorphic Encryption

Some Homomorphic Functions

- **RSA:** $E(m) = me \mod n$
- **ElGamal:** $E(m, r) = (g^r, mhr) \mod p$
- **GM:** $E(b, r) = r^2g^b \mod n$
- **Benaloh:** $E(m, r) = r^e g^m \mod n$
- **Pallier:** $E(m, r) = r^n g^m \mod n^2$
# Homomorphic Elections

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>
Homomorphic Elections

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ \sum = \]
Homomorphic Elections

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

\[ \Sigma = 2 \]
## Homomorphic Elections

<table>
<thead>
<tr>
<th>Name</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>
Homomorphic Elections

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>
Homomorphic Elections

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ \times = 2 \]
Homomorphic Elections

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

\[ \otimes = 2 \]
Homomorphic Elections

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>

$\otimes = 2$
## Multiple Authorities

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Homomorphic Encryption

The *product* of the *encryptions* of the votes constitutes an *encryption* of the *sum* of the votes.
Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>X₁</th>
<th>X₂</th>
<th>X₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>= Σ</td>
<td>3</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>= Σ</td>
<td>-4</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>= Σ</td>
<td>2</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>= Σ</td>
<td>-2</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>= Σ</td>
<td>4</td>
</tr>
</tbody>
</table>
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>$= \Sigma$</td>
<td>3</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>$= \Sigma$</td>
<td>-4</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>$= \Sigma$</td>
<td>2</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>$= \Sigma$</td>
<td>-2</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>$= \Sigma$</td>
<td>4</td>
</tr>
</tbody>
</table>

$$\Sigma = \Sigma = \Sigma =$$
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>$0 = \Sigma$</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>$0 = \Sigma$</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>$1 = \Sigma$</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>$0 = \Sigma$</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>$1 = \Sigma$</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

\[ \Sigma = \begin{array}{c} 3 \\ -5 \\ 4 \end{array} \]
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

$\sum = 3 \quad \sum = -5 \quad \sum = 4$
## Multiple Authorities

<table>
<thead>
<tr>
<th>Name</th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>$= \Sigma$</td>
<td>3</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>$= \Sigma$</td>
<td>-4</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>$= \Sigma$</td>
<td>2</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>$= \Sigma$</td>
<td>-2</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>$= \Sigma$</td>
<td>4</td>
</tr>
</tbody>
</table>

$\Sigma = \Sigma = \Sigma =$

| 2 | $= \Sigma$ | 3 | -5 | 4 |
### Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

**Σ =**

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>-5</td>
<td>4</td>
</tr>
</tbody>
</table>
Multiple Authorities

The sum of the shares of the votes constitute shares of the sum of the votes.
# Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>X1</th>
<th>X2</th>
<th>X3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

$$\Sigma = 2$$

$$\Sigma = 3$$

$$\Sigma = -5$$

$$\Sigma = 4$$
# Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

\[ \otimes = \otimes = \otimes = \]
Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>-1</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>3</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-2</td>
</tr>
</tbody>
</table>

$\otimes = \otimes = \otimes =\
3 \quad -5 \quad 4$
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>X₁</th>
<th>X₂</th>
<th>X₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

\[ \otimes = 3, \quad \otimes = -5, \quad \otimes = 4 \]
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

$$\otimes = \Sigma$$

<table>
<thead>
<tr>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-5</td>
<td>4</td>
</tr>
</tbody>
</table>
## Multiple Authorities

<table>
<thead>
<tr>
<th></th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>3</td>
<td>-5</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>-4</td>
<td>5</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>2</td>
<td>-3</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>-2</td>
<td>1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>4</td>
<td>-1</td>
</tr>
</tbody>
</table>

$$\otimes = \otimes = \otimes =$$

$$2 = \Sigma \quad 3 = -5 \quad 4$$
Double Commutivity

The *product* of the *encryptions* of the *shares* of the votes constitute an *encryption* of a *share* the *sum* of the votes.
Robust Sharing
Robust Sharing

Note that votes can be “shared” with a polynomial threshold scheme instead of a simple sum.
Robust Sharing

• Note that votes can be “shared” with a polynomial threshold scheme instead of a simple sum.
• This provides robustness in case one or more trustees fails to properly decrypt their shares.
Mix-Based Elections
The Mix-Net Paradigm
The Mix-Net Paradigm
The Mix-Net Paradigm
The Mix-Net Paradigm
The Mix-Net Paradigm
The Mix-Net Paradigm

![Diagram of Mix-Net Paradigm]
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Multiple Mixes
Decryption Mix-net
Decryption Mix-net

Each object is encrypted with a pre-determined set of encryption layers.
Decryption Mix-net

Each object is encrypted with a pre-determined set of encryption layers. Each mix, in pre-determined order performs a decryption to remove its associated layer.
Re-encryption Mix-net
Re-encryption Mix-net

The decryption and shuffling functions are decoupled.
Re-encryption Mix-net

The decryption and shuffling functions are decoupled.
Mixes can be added or removed dynamically with robustness.
Re-encryption Mix-net

The decryption and shuffling functions are decoupled.
Mixes can be added or removed dynamically with robustness.
Proofs of correct mixing can be published and independently verified.
More Homomorphic Encryption

We can construct a public-key encryption function $E$ such that if $A$ is an encryption of $a$ and $B$ is an encryption of $b$ then $A \otimes B$ is an encryption of $a \oplus b$. 

$A$ is *an* encryption of $a$ and $B$ is *an* encryption of $b$ then $A \otimes B$ is *an* encryption of $a \oplus b$. 

$A \otimes B$ is *an* encryption of $a \oplus b$. 

March 3, 2011
Practical Aspects of Modern Cryptography
Re-encryption (additive)

\[ A \text{ is an encryption of } a \text{ and } Z \text{ is an encryption of 0 then } A \otimes Z \text{ is another encryption of } a. \]
Re-encryption (multiplicative)

\[ A \text{ is } an \text{ encryption of } a \text{ and } \]
\[ I \text{ is } an \text{ encryption of } 1 \text{ then } \]
\[ A \otimes I \text{ is another encryption of } a. \]
A Re-encryption Mix
A Re-encryption Mix
A Re-encryption Mix
A Re-encryption Mix
A Re-encryption Mix
A Re-encryption Mix
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets
Re-encryption Mix-nets

March 3, 2011
Practical Aspects of Modern Cryptography
Verifiability
Verifiability

Each re-encryption mix provides a mathematical proof that its output is a permutation of re-encryptions of its input.
Verifiability

Each re-encryption mix provides a mathematical proof that its output is a permutation of re-encryptions of its input.

Any observer can verify this proof.
Verifiability

Each re-encryption mix provides a mathematical proof that its output is a permutation of re-encryptions of its input.

Any observer can verify this proof.

The decryptions are also proven to be correct.
Verifiability

Each re-encryption mix provides a mathematical proof that its output is a permutation of re-encryptions of its input.

Any observer can verify this proof. The decryptions are also proven to be correct. If a mix’s proof is invalid, its mixing will be bypassed.
Recent Mix Work

- 1993  Park, Itoh, and Kurosawa
- 1995  Sako and Kilian
- 2001  Furukawa and Sako
- 2001  Neff
- 2002  Jakobsson, Juels, and Rivest
- 2003  Groth
Re-encryption Mix Operation
Re-encryption Mix Operation

Input Ballot Set

MIX
Re-encryption Mix Operation

Input Ballot Set  Output Ballot Set

MIX
Re-encryption Mix Operation

Input Ballot Set

Re-encryptions

Output Ballot Set
Re-encryption
Re-encryption

• Each value is *re-encrypted* homomorphically.
Re-encryption

- Each value is re-encrypted homomorphically.
- This can be done without knowing the decryptions.
Verifying a Re-encryption
Verifying a Re-encryption

- A prover could simply reveal the specifics of the “blinding factors” used for re-encryption, but this would also reveal the permutation.
Verifying a Re-encryption

- A prover could simply reveal the specifics of the “blinding factors” used for re-encryption, but this would also reveal the permutation.
- Instead, an interactive proof can be performed to demonstrate the equivalence of the input and output ballot sets.
Verifying a Re-encryption

- A prover could simply reveal the specifics of the “blinding factors” used for re-encryption, but this would also reveal the permutation.
- Instead, an interactive proof can be performed to demonstrate the equivalence of the input and output ballot sets.
- The Fiat-Shamir heuristic can be used to “publish” the proof.
The Encryption
The Encryption

- Anyone with the decryption key can read all of the votes – even before mixing.
The Encryption

• Anyone with the decryption key can read all of the votes – even before mixing.
• A threshold encryption scheme is used to distribute the decryption capabilities.
Most Verifiable Election Protocols
Most Verifiable Election Protocols

Step 1
Most Verifiable Election Protocols

Step 1

Encrypt your vote and ...
Most Verifiable Election Protocols

Step 1
Encrypt your vote and ...

How?
How do Humans Encrypt?
How do Humans Encrypt?

- If voters encrypt their votes with devices of their own choosing, they are subject to coercion and compromise.
How do Humans Encrypt?

- If voters encrypt their votes with devices of their own choosing, they are subject to coercion and compromise.
- If voters encrypt their votes on “official” devices, how can they trust that their intentions have been properly captured?
The Human Encryptor

We need to find ways to engage humans in an *interactive proof* process to ensure that their intentions are accurately reflected in encrypted ballots cast on their behalf.
# MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>
# MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Bob</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>Carol</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>David</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>
**MarkPledge Ballot**

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>367</td>
<td>248</td>
<td>792</td>
<td>141</td>
<td>390</td>
<td>863</td>
<td>427</td>
<td>015</td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>

Device commitment to voter: “You’re candidate’s number is 863.”
MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
<th>Column 5</th>
<th>Column 6</th>
<th>Column 7</th>
<th>Column 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>367</td>
<td>248</td>
<td>792</td>
<td>141</td>
<td>390</td>
<td>863</td>
<td>427</td>
<td>015</td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>

Device commitment to voter: “You’re candidate’s number is 863.”

Voter challenge: “Decrypt column number 5.”
MarkPledge Ballot

<table>
<thead>
<tr>
<th>Voter</th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
<th>Column 5</th>
<th>Column 6</th>
<th>Column 7</th>
<th>Column 8</th>
<th>Column 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>367</td>
<td>248</td>
<td>792</td>
<td>141</td>
<td>390</td>
<td>863</td>
<td>427</td>
<td>015</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
<td></td>
</tr>
</tbody>
</table>

Device commitment to voter: “You’re candidate’s number is 863.”

Voter challenge: “Decrypt column number 5.”
### MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Bob</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>Carol</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>David</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>
Prêt à Voter Ballot

<table>
<thead>
<tr>
<th>Bob</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Eve</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td></td>
</tr>
<tr>
<td>Alice</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>17320508</td>
</tr>
</tbody>
</table>
## Prêt à Voter Ballot

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>17320508</td>
</tr>
</tbody>
</table>
Prêt à Voter Ballot

X

17320508
PunchScan Ballot

Y – Alice
X – Bob

#001
PunchScan Ballot

Y – Alice
X – Bob

#001
PunchScan Ballot

X – Alice
Y – Bob

Y
X

#001
PunchScan Ballot

X – Alice
Y – Bob

#001
PunchScan Ballot

X – Alice
Y – Bob

#001

March 3, 2011
Practical Aspects of Modern Cryptography
Scantegrity

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>choose one:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(b) the v</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(a) the v</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. VOT

Voters will be allowed to vote in the polling place automat

(a) the v

(b) the v

for others

the rec

6. VOT

Voters will be allowed to vote in the polling place automat

(a) the v

(b) the v

for others

the rec

choose one: FY

for others

the rec
Three-Ballot

President
Alice
Bob
Charles

Vice President
David
Erinca

r9>k*oe!4$%

Ballot

President
Alice
Bob
Charles

Vice President
David
Erinca

*t3]a&;nzs^_=

Ballot

President
Alice
Bob
Charles

Vice President
David
Erinca

u)+8c$@.?(
Voter-Initiated Auditing
Voter-Initiated Auditing

- Voter can use “any” device to make selections (touch-screen DRE, OpScan, etc.)
Voter-Initiated Auditing

- Voter can use “any” device to make selections (touch-screen DRE, OpScan, etc.)
- After selections are made, voter receives an encrypted receipt of the ballot.
Voter-Initiated Auditing

Encrypted Vote

734922031382
Voter-Initiated Auditing

Voter choice: Cast or Challenge

Encrypted Vote

734922031382
Voter-Initiated Auditing

Cast

Ballots

734922031382
Voter-Initiated Auditing

Challenge

734922031382
Voter-Initiated Auditing

Challenge
Voter-Initiated Auditing

Challenge
Ballot Casting Assurance

The voter front ends shown here differ in both their human factors qualities and the level of assurance that they offer.

All are feasible and provide greater integrity than current methods.
True Verifiability

- The end-to-end verifiable election technologies described here allow individuals to choose who to trust.
- Individuals are not forced to trust officials with special status. They can depend on verifications from entities of their choice.
- Sufficiently paranoid individuals can check everything for themselves.
Real-World Deployments
Real-World Deployments

- Helios (www.heliosvoting.org) – Ben Adida and others
  - Remote electronic voting system using voter-initiated auditing and homomorphic backend.
  - Used to elect president of UC Louvain, Belgium.
  - Used in Princeton University student government.
  - Used to elect IACR Board of Directors.
Real-World Deployments

- **Helios** ([www.heliosvoting.org](http://www.heliosvoting.org)) – Ben Adida and others
  - Remote electronic voting system using voter-initiated auditing and homomorphic backend.
  - Used to elect president of UC Louvain, Belgium.
  - Used in Princeton University student government.
  - Used to elect IACR Board of Directors.

- **Scantegrity II** ([www.scantegrity.org](http://www.scantegrity.org)) – David Chaum, Ron Rivest, many others.
  - Optical scan system with codes revealed by invisible ink markers and “plugboard-mixnet” backend.
  - Used for municipal elections in Takoma Park, MD.
End-to-End Verifiability
End-to-End Verifiability

... is a fundamentally different paradigm,
End-to-End Verifiability

- ... is a fundamentally different paradigm,

- ... is not just a security enhancement,
End-to-End Verifiability

- ... is a fundamentally different paradigm,
- ... is not just a security enhancement,
- ... democratizes the electoral process,
End-to-End Verifiability

- ... is a fundamentally different paradigm,

- ... is not just a security enhancement,

- ... democratizes the electoral process,

- ... but it is not a panacea.
End-to-End System Properties
End-to-End System Properties

- Accuracy/Integrity
End-to-End System Properties

- Accuracy/Integrity
  - enormously improved
End-to-End System Properties

- Accuracy/Integrity
  - enormously improved
- Privacy/Coercion
End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved
- Privacy/Coercion
  - not substantially changed
End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved
- Privacy/Coercion
  - not substantially changed
- Reliability/Survivability
End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved
- Privacy/Coercion
  - not substantially changed
- Reliability/Survivability
  - not substantially changed
End-to-End System Properties

- Accuracy/Integrity
  - *enormously* improved
- Privacy/Coercion
  - not substantially changed
- Reliability/Survivability
  - not substantially changed
- Usability/Comprehensibility
End-to-End System Properties

- **Accuracy/Integrity**
  - enormously improved
- **Privacy/Coercion**
  - not substantially changed
- **Reliability/Survivability**
  - not substantially changed
- **Usability/Comprehensibility**
  - not substantially changed
Is There any Deployment Hope?

- The U.S. Election Assistance Commission is considering new guidelines.
- These guidelines explicitly include an “innovation class” which could be satisfied by truly verifiable election systems.
- Election supervisors must choose to take this opportunity to change the paradigm.
- However, a bill was recently introduced in Congress that explicitly precludes use of crypto.