Secure Voting Protocols

Ben Adida
ben@eecs.harvard.edu

MIT CSAIL Distributed Systems Group
29 September 2006
2 Weeks Ago: Princeton Report

• Diebold touch-screen runs executable code loaded from memory card

• All audit logs modified to be consistent

• Can spread virally by memory card.
Why is Voting so Hard?
1893

DEVELOPED

FOR MAYOR,
AUGUST LEUZ, JR.
CORNER BURLINGTON AND JOHNSON STREETS.

FOR TREASURER,
GEORGE W. KOONTZ
NO. 620 EAST BURLINGTON STREET.

FOR CITY SOLICITOR,
FRANK J. HORAK
NO. 120 DODGE STREET.

FOR ASSESSOR,
F. A. HEINSIUS
NO. 948 EAST MARKET STREET.

FOURTH WARD.
FOR TRUSTEE,
JOHN U. MILLER
EAST MARKET STREET.

REPUBLICAN

FOR MAYOR,
CHAS. LEWIS
NO. 227 NORTH CLINTON STREET.

FOR TREASURER,

FOR SOLICITOR,
L. H. FULLER
NO. 422 SOUTH DUBUQUE STREET.

FOR ASSESSOR,
H. W. LATHROP
NO. 518 IOWA AVENUE.

FOURTH WARD.
FOR TRUSTEE,
J. C. LEASURE
COR. VAN BUREN ST. AND IOWA AVENUE.

1892 - Australian Ballot

http://www.cs.uiowa.edu/~jones/voting/pictures/
Secret Ballot vs. Verifiability

Protection from Undue Influence: Alice cannot prove how she voted.

Verifiability: Alice gains confidence that her vote was properly recorded.
The Next Harvard Pres!

SOURCES: HARVARD WANTS CONDOLEEZZA RICE OR BILL CLINTON FOR NEXT PRES...

The Ballot Handoff

Alice the Voter

Clinton
The Ballot Handoff

Alice the Voter

Clinton

→
The Ballot Handoff

Alice the Voter
The Ballot Handoff

Clinton

Alice the Voter

[Diagram showing a flow from Clinton to a ballot box, indicating the ballot handoff process.]
The Ballot Handoff

Alice the Voter

Clinton

Rice
Chain of Custody
Chain of Custody

Vendor

/*
 * source
 * code
 */
if (...
Chain of Custody

Vendor

/*
 * source
 * code
 */

if (...)
Chain of Custody

Polling Location → Voting Machine → Vendor

Vendor

/*
 * source
 * code
 */
if (...
1

Polling Location

Voting Machine
Chain of Custody

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

2. Voting Machine

3. Polling Location

4. Alice

Polling Location
Chain of Custody

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

2. Voting Machine

3. Polling Location

4. Alice

Alice casts her vote at Polling Location.
Chain of Custody

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

Polling Location

Alice

Ballot Box Collection
Chain of Custody

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

Polling Location

Alice

Ballot Box Collection

Results
Chain of Custody

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

2. Voting Machine

3. Polling Location

4. Alice
   VVPAT

5. Ballot Box Collection

6. Results
   ......

Legend:
- Ballots
- Voting Machine
- Polling Location
- Vendor
- Alice
- Results
The Cost of Secrecy
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McCormick, Chronicle Staff Writer

Monday, January 7, 2002
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McC

Monday, 3

Helicopter Crash Delays Afghan Vote Count

Helicopter Sent to Pick Up Afghan Ballots in Remote Province Crash-Lands, Delaying Vote Count
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin Mcc

Helicopter Crash Delays Afghan 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.
The Cost of Secrecy

Scavenged ballot box lids haunt S.F. elections

Erin McClelland

Monday, 3

Helicopter Crash Delays Afghan 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, election officials said.

Mexico Presidential Election Ballots Found in Dump

RAW STORY
Published: Thursday July 6, 2006
Cryptographic Voting achieves verifiability \textit{and} secrecy without depending on equipment correctness.
End-to-End Verification
End-to-End Verification

Voting Machine

Polling Location

Vendor

/*
 * source
 * code
 */

if (...
End-to-End Verification

- Polling Location
- Voting Machine
- Ballot Box / Bulletin Board
- Vendor
- /* source code */
  
```c
if (...)
```

Alice
End-to-End Verification

Alice

Polling Location

Voting Machine

Ballot Box / Bulletin Board

Vendor

Results

/*
 * source
 * code
 */
if (...
End-to-End Verification

Vendor

Voting Machine

Ballot Box / Bulletin Board

Polling Location

Receipt

Alice

Results

/*
 * source
 * code
 */

if (...
End-to-End Verification

- Polling Location
- Voting Machine
- Ballot Box / Bulletin Board
- Receipt
- Results

1. Polling Location
2. Vendor

Alice

Vendor

/*
 * source
 * code
 */

if (...)

[SRC81]
A Bulletin Board

**Alice:** Rice

**Bob:** Clinton

**Charlie:** Rice

**Tally**

Clinton: 1
Rice: 2
An Encrypted Bulletin Board!

Bulletin Board

Alice: Croissant
Bob: Croissant
Charlie: Eggs & Bacon

Tally
Clinton: 1
Rice: 2
An Encrypted Bulletin Board!

Bulletin Board

**Alice:**

**Bob:**

**Charlie:**

Ballot Casting Assurance

Tally
- Clinton: 1
- Rice: 2
An Encrypted Bulletin Board!

Bulletin Board

Alice:

Bob:

Charlie:

Ballot Casting Assurance

Universal Verifiability

Tally
Clinton: 1
Rice: 2
Crypto Voting Schemes
Crypto Voting Schemes

Alice

Adrienne

Encrypted Votes

Encryption

Verification

Ballot Data Flow
Crypto Voting Schemes

Verification
Ballot Data Flow

Encrypted Votes

Alice

Adrienne

encryption
Crypto Voting Schemes

Verification

Ballot Data Flow

Encrypted Votes

anonymization
Crypto Voting Schemes

Verification

Ballot Data Flow

Encryption

Anonymization

Decryption
Crypto Voting Schemes

Alice

Adrienne

Verification

Ballot Data Flow
Crypto Voting Schemes

Encryption

Registration Database

Encrypted Votes

Anonymization

Decryption

Tally

Results

Ballot Data Flow

Verification
Homomorphic Schemes

Encrypted Votes -> Encrypted Tallying -> Encrypted Aggregate Tally

decryption

Results
Homomorphic Encryption

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

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

\[ \text{Enc}_{pk}(m) = y^m r^s \mod n \]

\[ \text{Enc}_{pk}(m) = (g^r, g^m y^r) \mod p \]

s residuosity encryption

Exponential El-Gamal
Binary (Approval) Voting

Yes = Enc(1)
No = Enc(0)
Binary (Approval) Voting

Yes = Enc(1)
No = Enc(0)

[CohenFischer85, Benaloh86]
Binary (Approval) Voting

Yes = Enc(1)
No = Enc(0)

Encrypted Tally = Enc(m_a) \times Enc(m_b) \times Enc(m_c) = Enc(m_a + m_b + m_c)

[BraunFischer85, Benaloh86]
Needs Proofs!

[CohenFischer85, Benaloh86]
Needs Proofs!

Eve: $\text{Enc}(1000)$

Cannot trust that voters submit honest votes.

[CohenFischer85, Benaloh86]
Eve: Enc(1000)  Cannot trust that voters submit honest votes.

ZK proof that each vote is Enc(0) or Enc(1)

[CohenFischer85, Benaloh86]
Multi-Candidate Elections

<table>
<thead>
<tr>
<th>$2^{20}$</th>
<th>0001</th>
<th>0000</th>
<th>0000</th>
<th>Vote for Clinton</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{10}$</td>
<td>0000</td>
<td>0001</td>
<td>0000</td>
<td>Vote for Rice</td>
</tr>
<tr>
<td>$2^0$</td>
<td>0000</td>
<td>0000</td>
<td>0001</td>
<td>Vote for None</td>
</tr>
</tbody>
</table>

Tally: 0004 0001 0008

[P99, BFPSP2001]
Write-Ins? 
Preserving Ballots?
Anonymous Tallying

Anonymization

Decryption

Results

Encrypted Votes

Tally

Results
Mixnets

Republicans  Democrats  Independents
Mixnets

Mix servers operated by mutually suspicious organizations.
Chaumian Mixnet (Onions)

\[ c_j = \operatorname{Enc}_{pk_1} \left( \operatorname{Enc}_{pk_2} \left( \operatorname{Enc}_{pk_3} (m_j) \right) \right) \]

[Chaum81]
Chaumian Mixnet (Onions)

Each mix server “unwraps” a layer of this encryption onion.

$c_j = \text{Enc}_{p\text{k}_1}(\text{Enc}_{p\text{k}_2}(\text{Enc}_{p\text{k}_3}(m_j)))$

[Chaum81]
El Gamal Reencryption
El Gamal Reencryption

\[ sk = x \mod q \quad pk = y = g^x \mod p \]
El Gamal Reencryption

\[ sk = x \mod q \quad pk = y = g^x \mod p \]

\[ \text{Enc}_{pk}(m; r) = (\alpha, \beta) = (g^r, m \cdot y^r) \]

\[ \text{Dec}_{sk}(c) = \frac{\beta}{\alpha^x} \]
El Gamal Reencryption

\[ sk = x \mod q \quad pk = y = g^x \mod p \]

\[ Enc_{pk}(m; r) = (\alpha, \beta) = (g^r, m \cdot y^r) \]

\[ Dec_{sk}(c) = \frac{\beta}{\alpha^x} \]

\[ Reenc_{pk}(c; r') = c \cdot Enc_{pk}(1, r') = (g^{r+r'}, m \cdot y^{r+r'}) \]
Reencryption Mixnet

\[ c_{\pi(j)} = \text{Reenc}(c_j; r_j) \]
First Proof of Mixnet

\[ \pi, \{ r_j \} \]

Primary Mix

\[ \pi', \{ r'_j \} \]

Secondary Mix

[SK94]
First Proof of Mixnet

On 1-bit challenge, reveal secondary mix, or secondary-to-primary difference.

[SK94]
Verifying a Mixnet (II)

- Neff’s Proof is fastest to date 8N modular exponentiations. 2000 ballots mixed in a few minutes.

- **Intuition**: dot product of input exponents with a random vector = dot product of output exponents with permuted random vector.

- Implemented in VoteHere technology.

[Neff2001]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet

[JJR2002]
Verifying any Mixnet
Verifying any Mixnet

Tricks to ensure no complete path is revealed.

[JJR2002]
Anonymous Tallying

Private

Public
Anonymous Tallying

Homomorphic
Anonymous Tallying

Homomorphic

- Encrypted
- Identified
- Ballots

Private →

Public ←
Anonymous Tallying

Homomorphic

Private

Public

Encrypted Identified Ballots → Encrypted Tally
Anonymous Tallying

Homomorphic

1. Encrypted Identified Ballots
2. Encrypted Tally
3. Decrypted Tally

Directions:
- Red: Private
- Blue: Public
Anonymous Tallying

Homomorphic

Encrypted Identified Ballots → Encrypted Tally → Decrypted Tally

Mixnet
Anonymous Tallying

Homomorphic

- Encrypted Identified Ballots
- Encrypted Tally
- Decrypted Tally

Mixnet

- Encrypted Identified Ballots
Anonymous Tallying

Homomorphic
- Encrypted Identified Ballots
- Encrypted Tally
- Decrypted Tally

Mixnet
- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
Anonymous Tallying

Homomorphic

- Encrypted Identified Ballots
- Encrypted Tally
- Decrypted Tally

Mixnet

- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
- Decrypted De-Identified Ballots

Private

Public
Anonymous Tallying

**Homomorphic**

1. Encrypted Identified Ballots → Encrypted Tally
2. Encrypted Tally → Decrypted Tally

**Mixnet**

1. Encrypted Identified Ballots → Encrypted De-Identified Ballots
2. Encrypted De-Identified Ballots → Decrypted De-Identified Ballots
3. Decrypted De-Identified Ballots → Decrypted Tally
Anonymous Tallying

Homomorphic

Mixed Identifiable Ballots → Encrypted Ballots → Encrypted Tally → Decrypted Tally

Mixnet

Mixed Identifiable Ballots → Encrypted De-Identifiable Ballots → Encrypted De-Identifiable Ballots → Decrypted Tally
Best of Both Worlds?

<table>
<thead>
<tr>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c_1$</td>
<td>$c'_1$</td>
</tr>
<tr>
<td>$c_2$</td>
<td>$c'_2$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$c_n$</td>
<td>$c'_n$</td>
</tr>
</tbody>
</table>

[AW2006]
Best of Both Worlds?

Private

Public

\[ \pi, \{r'_i\} \]

[AW2006]
Best of Both Worlds?

what if we could replace the private mixnet with a public program?

[AW2006]
Best of Both Worlds?

<table>
<thead>
<tr>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pi, {r'_i}$</td>
<td>$c_1$</td>
</tr>
<tr>
<td></td>
<td>$c'_1$</td>
</tr>
<tr>
<td></td>
<td>$c_2$</td>
</tr>
<tr>
<td></td>
<td>$c'_2$</td>
</tr>
<tr>
<td></td>
<td>$\vdots$</td>
</tr>
<tr>
<td></td>
<td>$c_n$</td>
</tr>
<tr>
<td></td>
<td>$c'_n$</td>
</tr>
</tbody>
</table>

What if we could replace the private mixnet with a public program?

[AW2006]
Best of Both Worlds?

what if we could replace the private mixnet with a public program?

Private

\(\pi, \{r'_i\}\)

Public

\(c_1\)
\(c_2\)
\(\vdots\)
\(c_n\)

\(c'_1\)
\(c'_2\)
\(\vdots\)
\(c'_n\)

[AW2006]

what if we could replace the **private** mixnet with a **public** program?
Best of Both Worlds?

what if we could replace the private mixnet with a public program?

\[ \pi, \{ r'_i \} \]

Private

Public

\[ c_1, c_2, \ldots, c_n \]

\[ c'_1, c'_2, \ldots, c'_n \]

[AW2006]

what if we could replace the private mixnet with a public program?
So What?

- **public program**
  anyone can run it

- **pre-proven**
  all proofs before mixing

- **unbiased leaking**
  permutation and random factors are fixed before inputs are provided.
So What?

\( \pi, \{ r'_i \} \)

\[ \begin{align*}
P & \longrightarrow \text{public program} \\
& \quad \text{anyone can run it} \\
& \longrightarrow \text{pre-proven} \\
& \quad \text{all proofs before mixing} \\
& \longrightarrow \text{unbiased leaking} \\
& \quad \text{permutation and random factors are fixed before inputs are provided.}
\end{align*} \]

That's great, but can it really be done? [BG+2001, GK2005]
BGN Cryptosystem

\( G_1, G_2, \text{order } n = p_1 p_2 \)
\( e : G_1 \times G_1 \rightarrow G_2 \)
\( e(g^a, h^b) = e(g, h)^{ab} \)
BGN Cryptosystem

\[ G_1, G_2, \text{order } n = p_1 p_2 \]
\[ e : G_1 \times G_1 \to G_2 \]
\[ e(g^a, h^b) = e(g, h)^{ab} \]
\[ pk = (n, g, h = u^{p_1}) \quad sk = p_2 \]
**BGN Cryptosystem**

$G_1, G_2$, order $n = p_1 p_2$

$e : G_1 \times G_1 \rightarrow G_2$

$e(g^a, h^b) = e(g, h)^{ab}$

$pk = (n, g, h = u^{p_1})$  
$sk = p_2$

$Enc_{pk}(m) = g^m h^r$  
$Dec_{sk}(c) = \log_{g^{p_2}}(c^{p_2})$
BGN Cryptosystem

\[ G_1, G_2, \text{order } n = p_1 p_2 \]

\[ e : G_1 \times G_1 \to G_2 \]

\[ e(g^a, h^b) = e(g, h)^{ab} \]

\[ pk = (n, g, h = u^{p_1}) \quad sk = p_2 \]

\[ \text{Enc}_{pk}(m) = g^m h^r \]

\[ \text{Dec}_{sk}(c) = \log_{g^{p_2}}(c^{p_2}) \]

\[ \text{Enc}_{pk}(m_1) \cdot \text{Enc}_{pk}(m_2) = \text{Enc}_{pk}(m_1 + m_2) \]
BGN Cryptosystem

$G_1, G_2$, order $n = p_1 p_2$

$e : G_1 \times G_1 \rightarrow G_2$

$e(g^a, h^b) = e(g, h)^{ab}$

$pk = (n, g, h = u^{p_1})$

$sk = p_2$

$Enc_{pk}(m) = g^m h^r$

$Dec_{sk}(c) = \log_{g^{p_2}}(c^{p_2})$

$Enc_{pk}(m_1) \cdot Enc_{pk}(m_2) = Enc_{pk}(m_1 + m_2)$

$e(Enc_{pk}(m_1), Enc_{pk}(m_2)) = Enc_{pk}(m_1 \cdot m_2)$
Oblivious Cancellation / Selection

\[ \text{Enc}_{p_k}(m) \otimes \text{Enc}_{p_k}(0) = \text{Enc}_{p_k}(0) \]

\[ \text{Enc}_{p_k}(m) \otimes \text{Enc}_{p_k}(1) = \text{Enc}_{p_k}(m) \]

\text{Enc}_{p_k}(0) \text{ and } \text{Enc}_{p_k}(1) \text{ are indistinguishable}
Oblivious Cancellation / Selection

\[ \text{Enc}_{pk}(m) \otimes \text{Enc}_{pk}(0) = \text{Enc}_{pk}(0) \]

\[ \text{Enc}_{pk}(m) \otimes \text{Enc}_{pk}(1) = \text{Enc}_{pk}(m) \]

Enc\(_{pk}(0)\) and Enc\(_{pk}(1)\) are indistinguishable

Clearly Useful for PIR and OT [BGN2005].
In fact, it’s more powerful still.
Matrix Multiplication

\[
\begin{pmatrix}
  a_{11} & \ldots & a_{1l} \\
  a_{21} & \ldots & a_{2l} \\
  \vdots & \ddots & \vdots \\
  a_{n1} & \ldots & a_{nl}
\end{pmatrix}
\times
\begin{pmatrix}
  b_{11} & \ldots & b_{1n} \\
  b_{21} & \ldots & b_{2n} \\
  \vdots & \ddots & \vdots \\
  b_{l1} & \ldots & b_{ln}
\end{pmatrix}
=
\begin{pmatrix}
  c_{11} & \ldots & c_{1n} \\
  c_{21} & \ldots & c_{2n} \\
  \vdots & \ddots & \vdots \\
  c_{m1} & \ldots & c_{mn}
\end{pmatrix}
\]
Matrix Multiplication

\[
\begin{bmatrix}
a_{11} & \ldots & a_{1l} \\
a_{21} & \ldots & a_{2l} \\
\vdots & \ddots & \vdots \\
a_{n1} & \ldots & a_{nl}
\end{bmatrix}
\times
\begin{bmatrix}
b_{11} & \ldots & b_{1n} \\
b_{21} & \ldots & b_{2n} \\
\vdots & \ddots & \vdots \\
b_{l1} & \ldots & b_{ln}
\end{bmatrix}
= 
\begin{bmatrix}
c_{11} & \ldots & c_{1n} \\
c_{21} & \ldots & c_{2n} \\
\vdots & \ddots & \vdots \\
c_{m1} & \ldots & c_{mn}
\end{bmatrix}
\]
Matrix Multiplication

\[
\begin{bmatrix}
    a_{11} & \cdots & a_{1l} \\
    a_{21} & \cdots & a_{2l} \\
    \vdots & \ddots & \vdots \\
    a_{n1} & \cdots & a_{nl}
\end{bmatrix}
\times
\begin{bmatrix}
    b_{11} & \cdots & b_{1n} \\
    b_{21} & \cdots & b_{2n} \\
    \vdots & \ddots & \vdots \\
    b_{l1} & \cdots & b_{ln}
\end{bmatrix}
= 
\begin{bmatrix}
    c_{11} & \cdots & c_{1n} \\
    c_{21} & \cdots & c_{2n} \\
    \vdots & \ddots & \vdots \\
    c_{m1} & \cdots & c_{mn}
\end{bmatrix}
\]

\[
c_{ij} = \sum_{k=1}^{l} a_{ik} b_{kj}
\]
Matrix Multiplication

\[
\begin{bmatrix}
  a_{11} & \ldots & a_{1l} \\
  a_{21} & \ldots & a_{2l} \\
  \vdots & \ddots & \vdots \\
  a_{n1} & \ldots & a_{nl}
\end{bmatrix}
\times
\begin{bmatrix}
  b_{11} & \ldots & b_{1n} \\
  b_{21} & \ldots & b_{2n} \\
  \vdots & \ddots & \vdots \\
  b_{l1} & \ldots & b_{ln}
\end{bmatrix}
= 
\begin{bmatrix}
  c_{11} & \ldots & c_{1n} \\
  c_{21} & \ldots & c_{2n} \\
  \vdots & \ddots & \vdots \\
  c_{m1} & \ldots & c_{mn}
\end{bmatrix}
\]

\[
c_{ij} = \sum_{k=1}^{l} a_{ik} b_{kj}
\]

Degree is exactly 2: only one multiplication!
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
\otimes
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
= 
\begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
\times
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
= 
\begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
\times
\begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
= 
\begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
\times
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
= 
\begin{bmatrix}
m_3 \\
m_5 \\
m_2 \\
m_1 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
= 
\begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\otimes
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
= 
\begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic MM

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
\otimes
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4 \\
m_5 \\
\end{bmatrix}
= \begin{bmatrix}
m_3 \\
m_1 \\
m_5 \\
m_2 \\
m_4 \\
\end{bmatrix}
\]
Homomorphic matrix multiplication by an encrypted permutation matrix = Mixing!
Public Mixing

Private

Public

$\pi$
Public Mixing

| Private | \( \pi \) | \[
\begin{bmatrix}
0 & \ldots & 1 \\
\vdots & \ddots & \vdots \\
1 & \ldots & 0
\end{bmatrix}
\] | Public |
Public Mixing

Private

\[ \pi \rightarrow \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix} \rightarrow \{r_i\} \]

Public

\[ \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix} \]
### Public Mixing

**Private:**

\[
\pi \rightarrow \begin{bmatrix}
0 & \ldots & 1 \\
\vdots & \ddots & \vdots \\
1 & \ldots & 0
\end{bmatrix}
\rightarrow \{r_i\}
\]

**Public:**

\[
\begin{align*}
c_1 & \rightarrow \begin{bmatrix} 0 & \ldots & 1 \end{bmatrix} \\
c_2 & \rightarrow \begin{bmatrix} \vdots & \ddots & \vdots \end{bmatrix} \\
\vdots & \\
c_n & \rightarrow \begin{bmatrix} 1 & \ldots & 0 \end{bmatrix}
\end{align*}
\]
Public Mixing

Private

\[ \pi \rightarrow \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix} \{r_i\} \]

Public

\[ \begin{gathered} c_1 \quad c_2 \quad \cdots \quad c_n \\ \end{gathered} \quad \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix} =\begin{gathered} c'_1 \quad c'_2 \quad \cdots \quad c'_n \\ \end{gathered} \]
Public Mixing

\[ \pi \rightarrow \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix} \{r_i\} \]

\[ \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \otimes \begin{bmatrix} 0 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 0 \end{bmatrix} = \begin{bmatrix} c'_1 \\ c'_2 \\ \vdots \\ c'_n \end{bmatrix} \]
Anonymous Tallying

Homomorphic

- Encrypted Identified Ballots
- Encrypted Tally
- Decrypted Tally

Mixnet

- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
- Decrypted De-Identified Ballots
- Decrypted Tally
Anonymous Tallying

Homomorphic

Encrypted Identified Ballots → Encrypted Tally → Decrypted Tally

Mixnet

Encrypted Identified Ballots → Encrypted De-Identified Ballots → Decrypted De-Identified Ballots → Decrypted Tally

(Public Mixing)
Anonymous Tallying

Homomorphic

Encrypted Identified Ballots → Encrypted Tally → Decrypted Tally

Mixnet

Encrypted Identified Ballots → Encrypted De-Identified Ballots → Decrypted De-Identified Ballots → Decrypted Tally

/Public Mixing/
Anonymous Tallying

Homomorphic

- Encrypted Identified Ballots
- Encrypted Tally
- Decrypted Tally

Mixnet

- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
- Decrypted De-Identified Ballots
- Decrypted Tally

(Public Mixing)

- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
Anonymous Tallying

Homomorphic

- Encrypted Identified Ballots
- Encrypted Tally
- Decrypted Tally

Mixnet

- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
- Decrypted De-Identified Ballots
- Decrypted Tally

(Public Mixing)

- Encrypted Identified Ballots
- Encrypted De-Identified Ballots
- Decrypted De-Identified Ballots
- Decrypted Tally

Private
Public
Incoercibility

Alice

Adrienne

Encryption

Encrypted Votes
Incoercibility
Incoercibility

- How do votes get to the bulletin board in the first place?
Incoercibility

- How do votes get to the bulletin board in the first place?
- Alice can't perform the encryption herself, or she would be able to sell her vote.
Incoercibility

• How do votes get to the bulletin board in the first place?

• Alice can’t perform the encryption herself, or she would be able to sell her vote.

• How can Alice be certain that the encryption was performed correctly, yet still not be able to sell her vote?
Receipt-Freeness

[BT94]
Receipt-Freeness

- A Voting Machine prepares the encrypted ballot for Alice.
- The Machine provides Alice with a ZK proof that her vote was correctly encrypted.

[BT94]
Receipt-Freeness

- A Voting Machine prepares the encrypted ballot for Alice.
- The Machine provides Alice with a ZK proof that her vote was correctly encrypted.

[BT94]
Receipt-Freeness

- A Voting Machine prepares the encrypted ballot for Alice.
- The Machine provides Alice with a ZK proof that her vote was correctly encrypted.
- Requirement: private voting booth where crucial elements of this proof occur.

[BT94]
MarkPledge

[Neff2004]
MarkPledge

• Challenge Ticket

[Neff2004]
MarkPledge

- Challenge Ticket
- Fill out ballot normally

Alice

[Neff2004]
MarkPledge

- Challenge Ticket
- Fill out ballot normally
- Get a printed receipt and Screen Confirmation Code

Alice

[Rice: dhjq]

Receipt

[ab54]

[Neff2004]
MarkPledge

- Challenge Ticket
- Fill out ballot normally
- Get a printed receipt and Screen Confirmation Code
- Scan Challenge Ticket

[Neff2004]
MarkPledge

- Challenge Ticket
- Fill out ballot normally
- Get a printed receipt and Screen Confirmation Code
- Scan Challenge Ticket
- Receive complete receipt

[Neff2004]
MarkPledge

- Challenge Ticket
- Fill out ballot normally
- Get a printed receipt and Screen Confirmation Code
- Scan Challenge Ticket
- Receive complete receipt
- Verify that codes match

[Neff2004]
MarkPledge (II)

<table>
<thead>
<tr>
<th>Receipt Ticket: ab54</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinton: 34c7</td>
</tr>
<tr>
<td>Rice: dhjq</td>
</tr>
<tr>
<td>None: 8489</td>
</tr>
</tbody>
</table>

- Receipt contains encrypted ballot that can be checked against bulletin board by voter or a helper.
- Codes are random: Alice cannot convince anyone that dhjq was the “real” code.

[Neff2004]
Questions?