Verifying a Secret-Ballot Election with Cryptography

Ben Adida
PhD Thesis Defense

Thesis Committee
Ronald L. Rivest, Srini Devadas, Shafi Goldwasser

22 June 2006
Ostraka
(sea shells)

http://darkwing.uoregon.edu/~klio/im/gr/ath/Athen%20-%20Ostraka.jpg
1892 - Australian Ballot

DEMOCRATIC

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.

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.

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

1893

Majorities

848

221

101

198

24
The Breakfast Vote

Carl the Coercer
“Eggs&Bacon Lobby”

Valerie the Voter

Croissant

Eggs & Bacon
Carl the Coercer
“Eggs&Bacon Lobby”

Valerie the Voter
Voting Interface
Croissant
The Ballot Handoff

Valerie the Voter
The Cost of Secrecy

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
Chain of Custody

Vendor

Polling Location

Valerie

Voting Machine

Ballot Box Collection

Results

1

/*
 * source
 * code
 */

if (...)

2

3

4

5

6
“Secret ballots and transparency in government are mutually exclusive concepts.”

Lynn Landes - Nov. 2005

eVoting in Switzerland
95% of Geneva citizens vote by mail (and now Internet)

http://votebymailproject.org
The Secret Ballot Matters

Secret Ballot implemented in Chile in 1958.

“the secrecy of the ballot [...] has first-order implications for resource allocation, political outcomes, and social efficiency.”

[BalandRobinson 2004]
Secrecy vs. Audit-ability?

“Cryptography solves problems that seem contradictory. There’s such a thing as ‘just the right level’ of contradiction.”

Ronald L. Rivest (paraphrased)
End-to-End Verification

Vendor

Polling Location

Voting Machine

Bulletin Board

Results

Valerie

Receipt

/*
 * source
 * code
 */

if (....

[1]

[2]
A Bulletin Board?

Valerie: Croissant

Vanessa: Croissant

Victor: Eggs&Bacon

Tally
Croissant: 2
Eggs&Bacon: 1
An Encrypted Bulletin Board!

Bulletin Board

Valerie:
Vanessa:
Victor:

Ballot Casting Assurance
Universal Verifiability

Tally
Croissant: 2
Eggs&Bacon: 1
Crypto Voting Schemes

Results

Registration Database

Tally

decryption

anonymization

Encryption

Encrypted Votes

Valerie

Vanessa

Victor
Contributions

Valerie
Vanessa
Victor

Registration Database

Encrypted Votes

[AR2006]

[ANa2006, ANb2006]

[AW2006]

decryption

anonymization

Tally

Results
This Talk

★ Introduction to Crypto Voting
★ Scratch & Vote
★ Public Mixing
Ryan Ballot

“Onion”
Onion Decryption

Onion = Enc_{pk_1}(r_1; Enc_{pk_2}(r_2; Enc_{pk_3}(r_3)))

<table>
<thead>
<tr>
<th>Croissant</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Eggs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

r_1

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

r_2

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

r_3

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Eggs

Croissant

None

8c3859x0dfsw
Ryan Ballot: Verification

Internet / Phone

Valerie the Voter

Bulletin Board

<table>
<thead>
<tr>
<th>Valerie</th>
<th>Vanessa</th>
<th>Victor</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Croissant
Eggs
None

Ed the Election Official
What can we improve?

* Pre-voting auditing
  - administrators involved for Ryan ballot
  - individual voter verification unlikely

* Post-voting auditing
  - administrators are highly involved
Homomorphic Counters

# US eligible voters < $2^{28}$ (28 bits)
Paillier Plaintext = 1024 bits

- $2^{56}$: 0001 0000 0000 → Vote for Croissant
- $2^{28}$: 0000 0001 0000 → Vote for Eggs&Bacon
- $2^0$: 0000 0000 0001 → Vote for None
Scratch & Vote Ballot

Scratch Surface

2D barcode

$\mathsf{Enc}_{pk}(2^{28}; r_2)$

$\mathsf{Enc}_{pk}(2^0; r_3)$

$\mathsf{Enc}_{pk}(2^{56}; r_1)$

$\mathsf{Enc}_{pk}(2^{28}; r_2)$

$\mathsf{Enc}_{pk}(2^0; r_3)$

$\mathsf{Enc}_{pk}(2^{28}; r_2)$

$\mathsf{Enc}_{pk}(2^0; r_3)$

Scratch Surface

2D barcode

$\mathsf{Enc}_{pk}(2^{56}; r_1)$
Pre-Voting Verification

Vote

Valerie the Voter

Audit
Post-Voting Verification

Internet / Phone

Valerie the Voter

Bulletin Board

Valerie
Vanessa
Victor
Tally

Homomorphic Addition

Single Decryption

Croissant: 2
Eggs & Bacon: 1
Issues Under the Rug

* Voter/Official Collusion
  - NIZK on bboard
* Casting a Ballot
  - Pre/Double Tear
* More than one race?
  - Chaum ballot
* Ballot Printers know the candidate orders
  - Working on that!

http://www.rickandlynne.com/rick/go/gallery/image_full/504/
This Talk

* Introduction to Crypto Voting
* Scratch & Vote
* Public Mixing
El Gamal Reencrytion

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

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

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

\[ \text{Reenc}_{pk}(c; r') = c \cdot \text{Enc}_{pk}(1, r') \]
\[ = (g^{r+r'}, m \cdot y^{r+r'}) \]
Reencryption Mixnet

Each mix server shuffles and reencrypts inputs.
Proving the Mix

$c'_i = \text{Reenc}(c_{\pi(i)}, r'_i)$

$\text{ZKPoK} \left[\pi, \{r'_i\}\right]$
what if we could replace the private mixnet with a public program?
So What?

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

\[ P \]

- **public program**
  anyone can run it

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

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

That’s great, but can it really be done?

[BG+2001, GK2005]
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

\[
\text{Enc}_{pk}(m) \otimes \text{Enc}_{pk}(0) = \text{Enc}_{pk}(0)
\]
\[
\text{Enc}_{pk}(m) \otimes \text{Enc}_{pk}(1) = \text{Enc}_{pk}(m)
\]

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

Clearly Useful for PIR and OT [BGN2005].
In fact, it’s more powerful still.
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 matrix multiplication by an encrypted permutation matrix = Mixing!
Public Mixing

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

Private

Public

\[ \begin{array}{cccc}
c_1 \\
c_2 \\
\vdots \\
c_n
\end{array} \otimes \begin{bmatrix}
0 & \ldots & 1 \\
\vdots & \ddots & \vdots \\
1 & \ldots & 0
\end{bmatrix} = \begin{array}{cccc}
c'_1 \\
c'_2 \\
\vdots \\
c'_n
\end{array} \]
A Taste of the Proofs

* “Deterministic Mixing” functionality
  - permutation-indistinguishable by a hybrid argument on semantic security.

* Proof of Correct Obfuscation
  - simulator creates its own mixing matrix
  - semantic security, thus adversary cannot distinguish
Why Did We Succeed?

- [BG+2001, GK2005] tell us generic obfuscation is hard.
- Functionality defined on the plaintexts; we’re only dealing with ciphertexts
  - “covers of encryption”

We don’t know that this is really a permutation matrix!
We must **prove** correct functionality.
Proving the Matrix

is

an encrypted permutation matrix?

* Straight-forward proof:

- Use Proof of Partial Knowledge [CDS94] to show that each element is either 0 or 1.
- Homomorphically compute the row and column sums and prove that they’re all equal to 1.
- $n^2$ proofs. Uggh.
Proving the Matrix (better)

\[
\begin{bmatrix}
\vdots & \cdots & \vdots \\
\vdots & \ddots & \vdots \\
\vdots & \cdots & \vdots \\
\end{bmatrix}
\otimes
\begin{bmatrix}
\mathbf{r}_1 \\
\vdots \\
\mathbf{r}_n \\
\end{bmatrix} =
\begin{bmatrix}
\mathbf{c}_1 \\
\vdots \\
\mathbf{c}_n \\
\end{bmatrix}
\]

* Proof by Random Vector Challenge
* Well-known techniques, $O(n)$.
* $n^2$ computation, $O(n)$ proof.
Mixing more than once?

Not with BGN bilinear map...
Only one multiplication.
Distributed Generation

Use a **Mixnet** to shuffle the matrix rows

Prove each one using Random Vector Test

Remember, this is still **before** the inputs to mix are available.
“Encapsulated” Mixing

* Capture the actions of the various mixers.
* Prove that everything went well.
* “Replay” them on the encrypted votes when they’re available.
Generalized Paillier

\[ Enc_{pk}(m) = g^{m} r^{n} \mod n^{2}, m \in \mathbb{Z}_{n} \]

\[ Enc_{pk,2}(m) = h^{m} r^{n^{2}} \mod n^{3}, m \in \mathbb{Z}_{n^{2}} \]

\[ Enc_{pk,2}(Enc_{pk}(m)) = h^{g^{m} r^{n}} r^{n^{2}} \mod n^{3} \]

\[ c = Enc_{pk}(m) \]

\[ [Enc_{pk,2}(0)]^{c} = Enc_{pk,2}(0) \]

\[ [Enc_{pk,2}(Enc_{pk}(0))]^{c} = Enc_{pk,2}(c) \]
GP Homomorphisms

\[
\begin{align*}
0 \cdot m &= 0 \\
0 \cdot m &= 0 + m = m
\end{align*}
\]
**GP Public Mixing**

- Full-length plaintexts
- Faster computation (modexp vs. BM)
- But ... longer proofs (double discrete log)
- Composable via multiple layering?
Contributions

* Education
  - Introduction to Crypto Voting
  - Mixnet Review
  - Ballot Casting Assurance [ANa2006]

* Practice
  - Scratch & Vote [AR2006]

* Theory
  - Public Mixing [AW2005]
  - Assisted Human Interactive Proofs [ANb2006]
The Promise of Crypto Voting

1. Secrecy **AND** Audit-ability
2. End-to-end Verification
What’s Holding This Up?

* Education
  - remote voting is dangerous
  - crypto is integral, so “trust your cryptographer?”

* Recovery
  - if you know what went wrong, then you have to fix it.
  - Future Research: recovery-centric schemes
So what next?

New voting laws should encourage research and pilot deployments of direct voter verifiable voting techniques.

VVPAT only is a missed opportunity.
Thanks!!

Ron
Shafi, Srini
Andy, David, Douglas, Susan, David
Steven, Seth, Rafael, Chris, Ran, Guy
Hal, Danny, Eric, Ralph
Zak, Ken, Pete
Rita, Mom, Dad, Claire, Juliette
Questions?