Public Verifiable Randomness Beacon
for Random Sample Elections

Christopher D. Nguyen, David Chaum,
Alan T. Sherman, Aggelos Kiayias

CRYPTO 2014 Rump Session
August 19, 2014
Random Sample Elections (RSE)
http://rs-elections.com/

Participants

David Chaum  Pedro A.D. de Rezende  Maciej Kosarzecki  Pance Ribarski  Brian Sutin
Deborah Hurley  Markus Duermuth  Christopher Nguyen  Mark Ryan  Douglas Wikström
Richard Carback  James Honaker  Hannu Nurmi  Peter Schwabe  Lirong Xia
Jeremy Clark  Aggelos Kiayias  Christof Paar  Alan Sherman  Filip Zagórski
Michael Clarkson  Maciej Kosarzecki  David Parkes  Emin Gün Sirer  Bingsheng Zhang

Progress on Six Pillars

<table>
<thead>
<tr>
<th>RSE implementation</th>
<th>Statistical analysis and simulations</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Progress" /></td>
<td><img src="#" alt="Progress" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit software implementations</th>
<th>Trustworthy public randomness</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Progress" /></td>
<td><img src="#" alt="Progress" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cryptographic models (UCF)</th>
<th>Vote selling game theoretic analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Progress" /></td>
<td><img src="#" alt="Progress" /></td>
</tr>
</tbody>
</table>

0% 25% 50% 75% 100%
Goal and Motivation

Provide a source of bits that are

- uniformly distributed
- forward unpredictable
- end-to-end auditable

Why trust the beacon? Why not check it yourself?

Applies to any system/protocol requiring trustworthy public random bits. (e.g., random challenges)

In RSE, random sample selection and audit challenges. Requires randomness from entropy sources of varying quality, latency, and throughput.

Fine Print: Not appropriate for secret values. (e.g., crypto keys)
Bits that are done

Identified candidate entropy sources:
  ○ Financial data (stocks)
  ○ Scientific data (weather)
  ○ Information archives (web archives)

*Note: Incorporation of different sources allows us to meet varying requirements on quality, latency, and throughput.*

Built scrapers for US stocks and weather. Web archive scraper under development.

Have a voter-palatable explanation of how we use this randomness in Random Sample Elections.
Bits that are done

Identified candidate entropy sources:

- Financial data (stocks)
- Scientific data (weather)
- Information archives (web archives)

Note: Incorporation of different sources allows us to meet varying requirements on quality, latency, and throughput.

Facebook is a lot like ancient Egypt: people writing on walls; worshipping cats.

(Source: Unknown)
Bits in progress

- Prototype → Production
  - Expand beacon from stocks to other entropy sources.
  - Rework data formats to handle multiple sources and provide better linking between random bits and the source data.

- Mathematical and adversarial models
- Entropy estimation
- Extractor algorithms development
Challenging bits

Our entropy sources are not independent. They have correlation and even self-correlation.

- How do we estimate entropy and build extractors?

(Source: xkcd.com)
Challenging bits

Our entropy sources are not independent. They have correlation and even self-correlation.

- How do we estimate entropy and build extractors?

The extractor and verifiers may disagree.

- Entropy quantity vs. measurement consistency
- Measurement synchronization.
  - Ex: website changes while the extractor and verifiers are archiving it.
- How do we reconcile these inconsistencies?
We welcome you to join!

For information about the RSE project contact
David Chaum <david@chaum.com> or
Deborah Hurley <dhurley@well.com>

Possible major scholarships for BS, MS, and PhD students via UMBC:
   NSF Scholarship for Service (SFS)
   UMBC Cyber Scholars
Contact Alan Sherman <sherman@umbc.edu>

Also accepting new customers to use our entropy!