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

Progress on Six Pillars

RSE implementation	🟩	Statistical analysis and simulations	🟨
Audit software implementations	🟩	*Trustworthy public randomness*	🟨
Cryptographic models (UCF)	🟧	Vote selling game theoretic analysis	🟧
🟥 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.

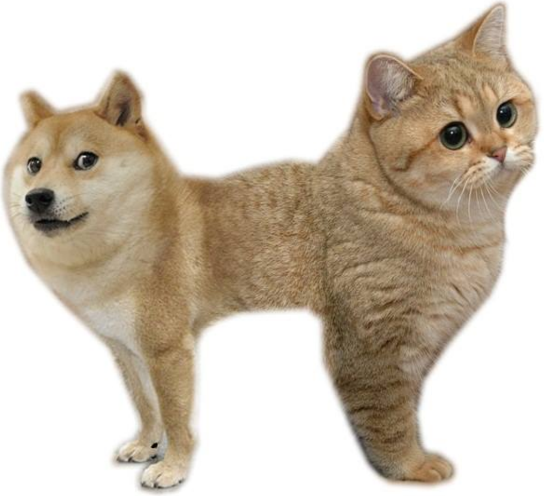
Bits that are done

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.

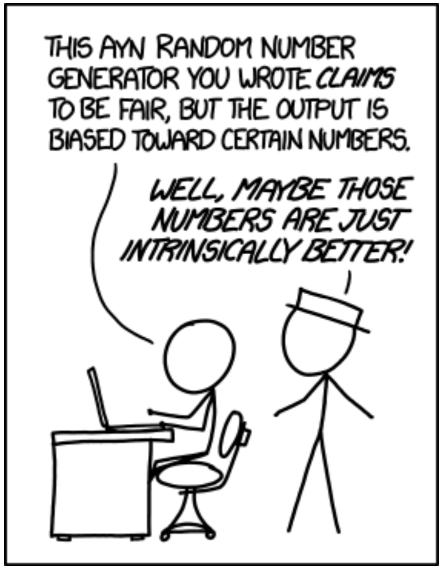
- Mathematical and adversarial models
- Entropy estimation
- Extractor algorithms development

Challenging bits

Our entropy sources are not independent.

They have correlation and even self-correlation.

- How do we estimate entropy and build extractors?


THIS AYN RANDOM NUMBER GENERATOR YOU WROTE *CLAIMS* TO BE FAIR, BUT THE OUTPUT IS BIASED TOWARD CERTAIN NUMBERS.
WELL, MAYBE THOSE NUMBERS ARE JUST INTRINSICALLY BETTER!

(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!