What's All the Fuss About Randomness?

October 21, 2020

General David Petraeus, commander of the U.S. Central Command, performs the coin toss before Super Bowl XLIII between the Arizona Cardinals and the Pittsburgh Steelers on Feb. 1, 2009, at Raymond James Stadium in Tampa.

Photographer: Jamie Squire/Getty Images

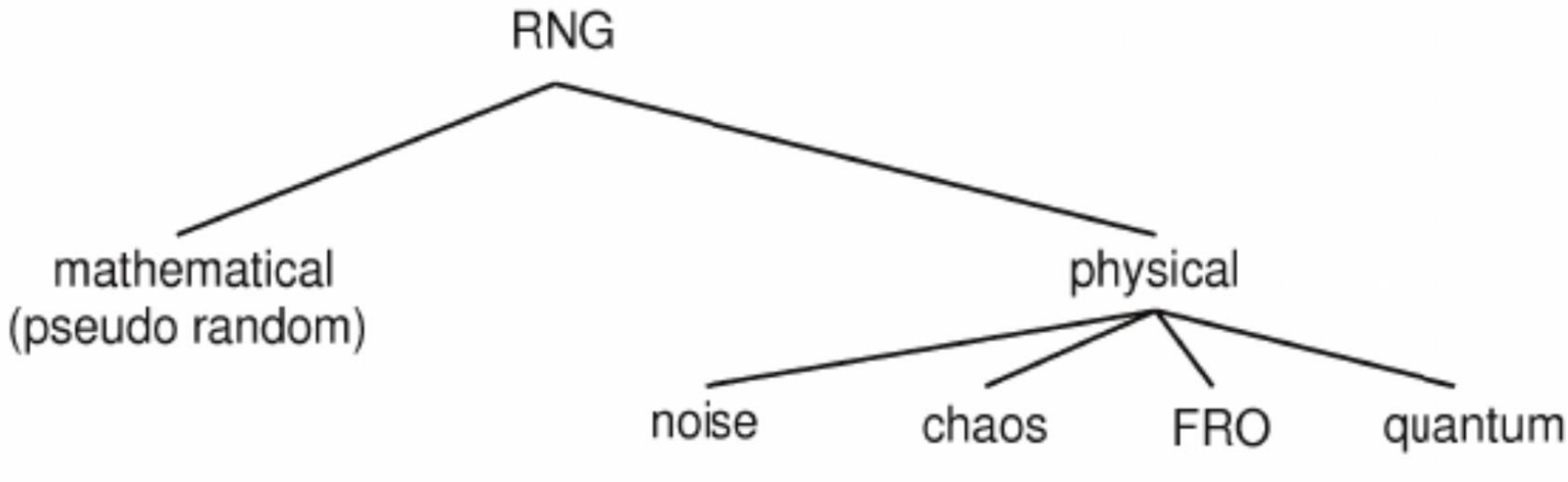
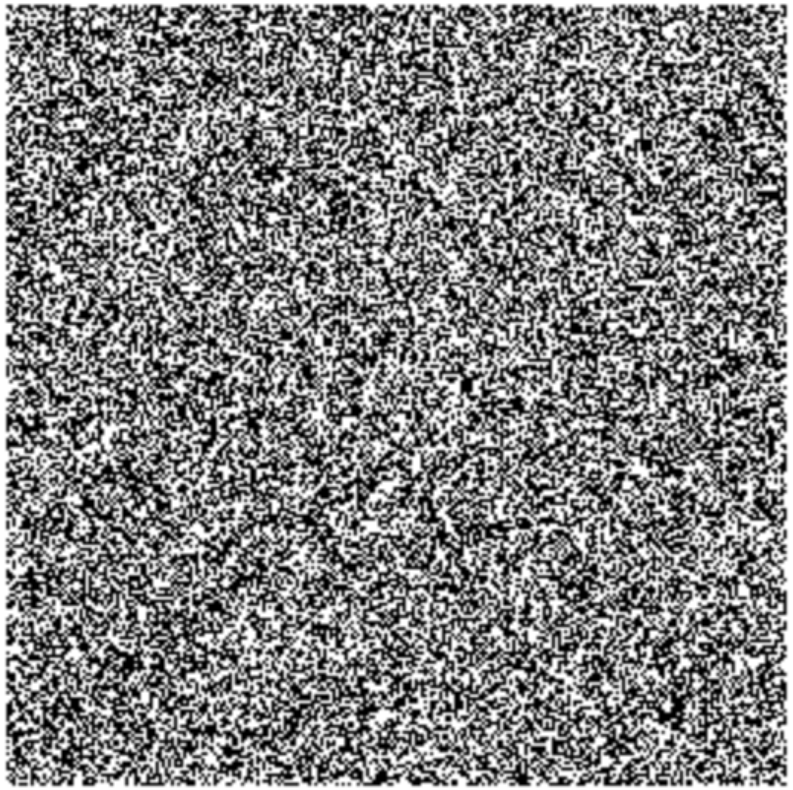
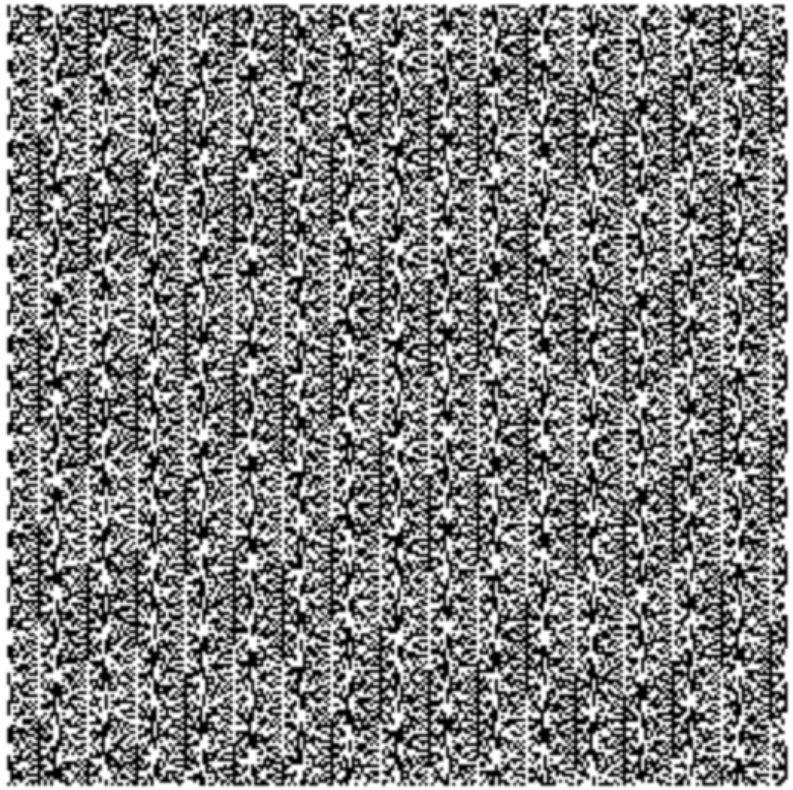


Figure 1: Classification of random number generators.

Visualization of Entropy



RANDOM.ORG



PHP rand() on Microsoft Windows

TRNG

-Uses an unpredictable physical means to generate numbers(like atmospheric noise)

VS

PRNG

- Uses methematical and deterministic algorithms(completely computer-generated)

“Nein Nines”

Matt Blaze's

EXHAUSTIVE SEARCH

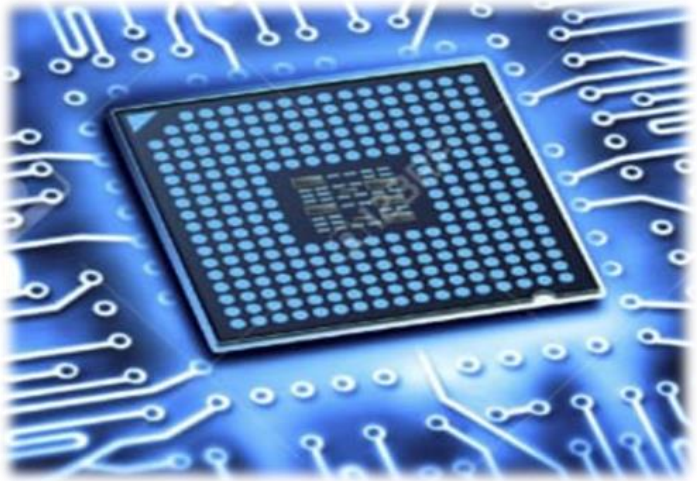
Science, Security, Curiosity

A Cryptologic Mystery

Did a broken random number generator in Cuba help expose a Russian espionage network?

Random Number Evolution

Classic Computer Mathematical Entropy



Centralized Bio-Mechanical Entropy using Lavarand at ***Cloudflare***

Centralized / Decentralized Bio-mechanical Entropy with visual analog source

Scientists Across the Globe Are Hunting for Pure Randomness

By Michael Dhar October 06, 2018

True Random Numbers Since 1998!

RANDOM.ORG

What's this fuss about *true* randomness?

Perhaps you have wondered how predictable machines like computers can generate randomness. In reality, most random numbers used in computer programs are *pseudo-random*, which means they are generated in a predictable fashion using a mathematical formula. This is fine for many purposes, but it may not be random in the way you expect if you're used to dice rolls and lottery drawings.

RANDOM.ORG offers *true* random numbers to anyone on the Internet. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. People use RANDOM.ORG for holding drawings, lotteries and sweepstakes, to drive online games, for scientific applications and for art and music. The service has existed since 1998 and was built by Dr Mads Haahr of the School of Computer Science and Statistics at Trinity College, Dublin in Ireland. Today, RANDOM.ORG is operated by Randomness and Integrity Services Ltd.

True Random Number Generator

Min: 1

Max: 100

Generate

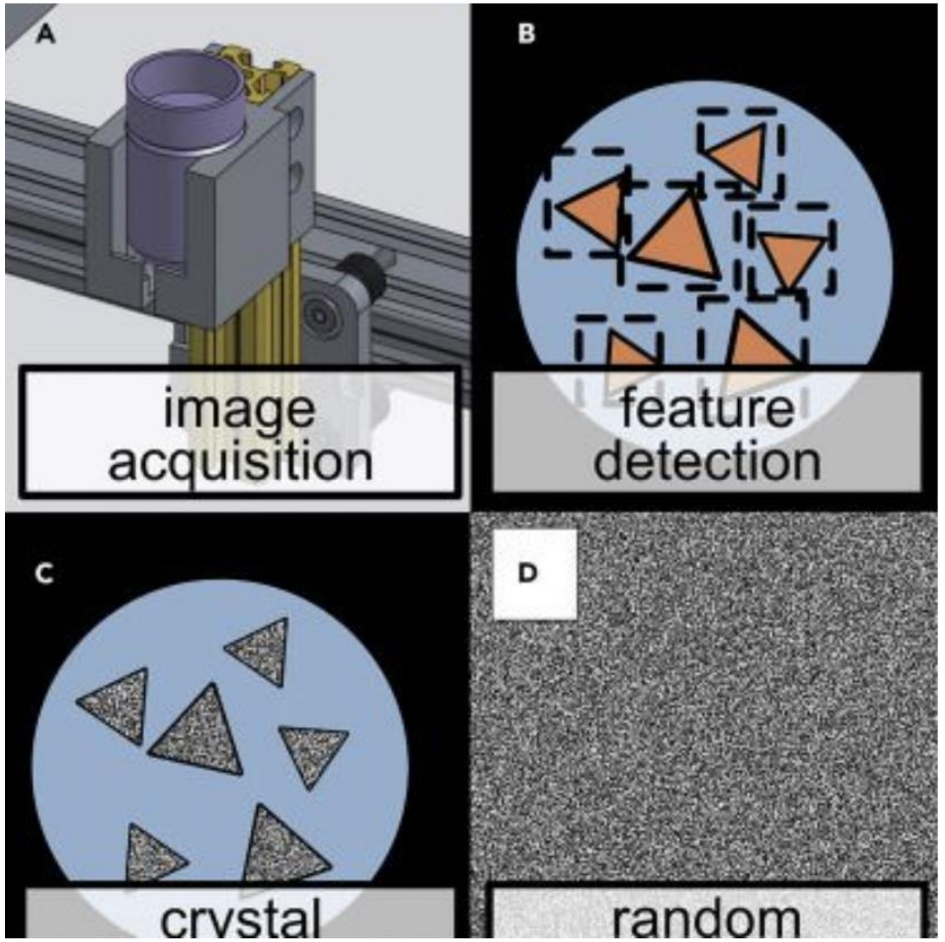
Result:

Powered by RANDOM.ORG

Mad Scientists and Crystal Formations

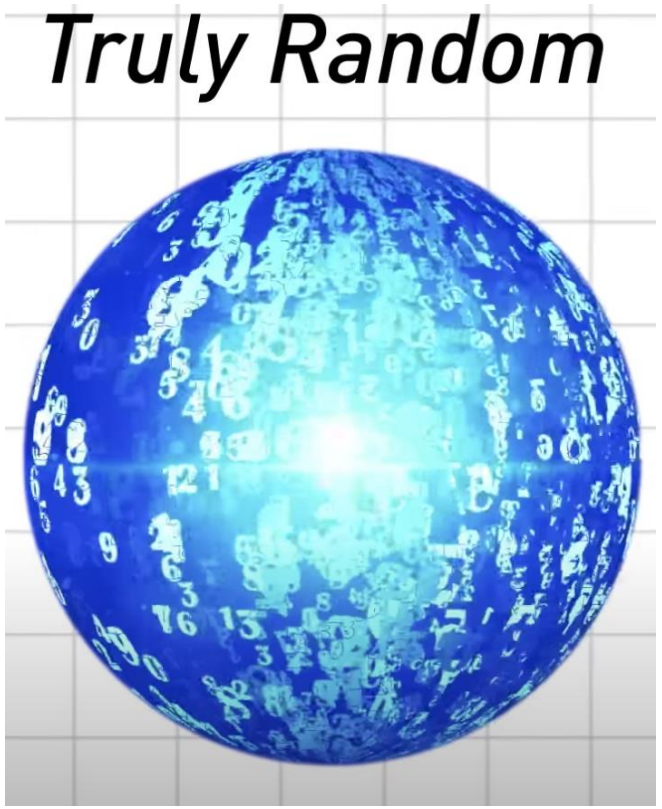
Computers, Meet Entropy

Automated Randomness



UNIVERSITY OF GLASGOW

Environmental Randomness

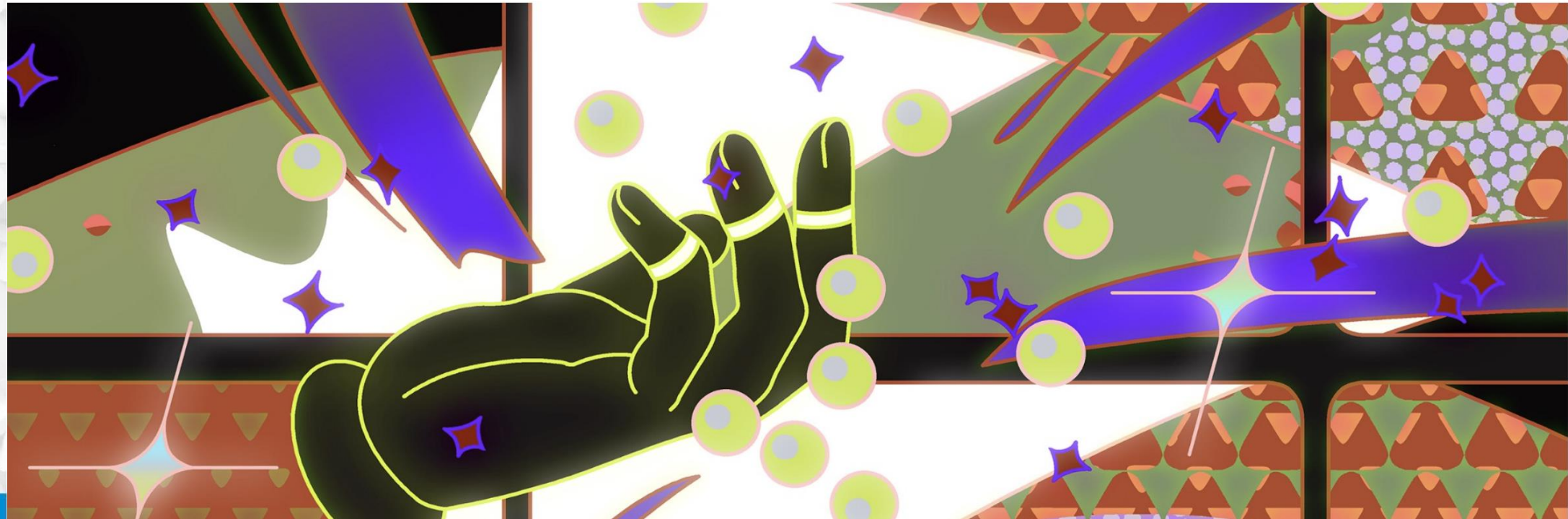


Random Resources

The League of Entropy Is Making Randomness Truly Random

Creating reliably random numbers isn't as easy as you think, but a new alliance of organizations and individuals is decentralizing randomness for more equitable and trustworthy applications

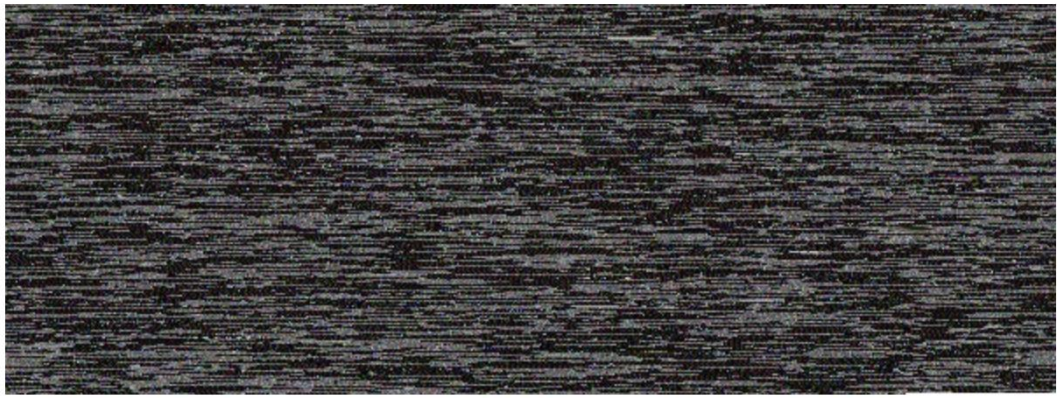
Rina Diane Caballar Aug 7, 2019 · 7 min read ★



Random Tweets?

Getting random Tweets

Twitter allows anyone to retrieve a small **random** sample of all public statuses being published in **real-time** using the *GET statuses/sample API*.



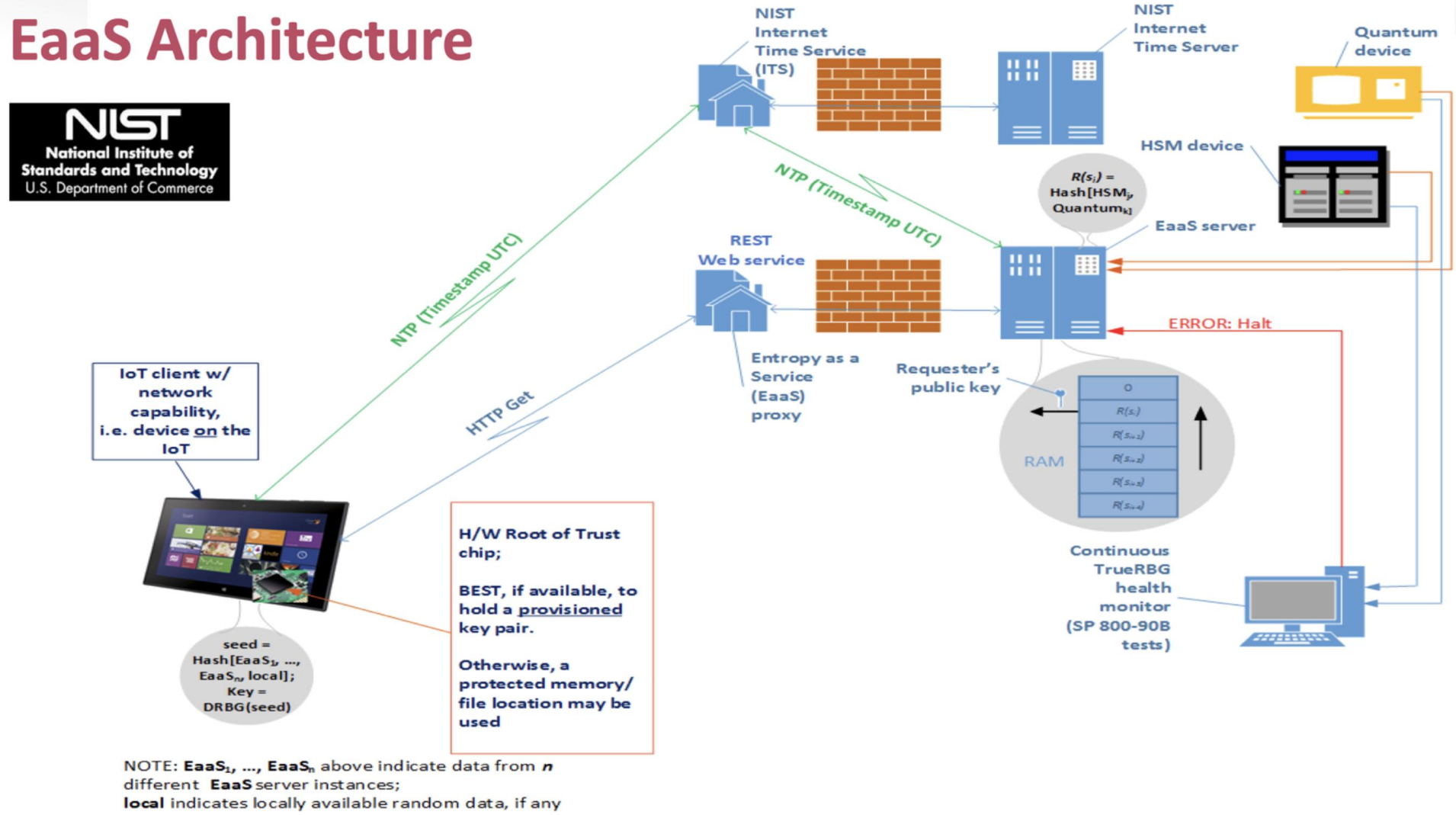
Twitter noise (concatenated UTF-8 encoded tweets)

Sampling 500KB of raw tweet data, entropy is around 6.5519 bits per byte (true random would reach 8) and the arithmetic mean value is 135.65 (random would be around 127.5). This is not perfect random but we're getting there!

⚠️ **The purpose of this article is to illustrate a joke & recreational RNG. Not something to be taken seriously.**

***tl;dr*: Do not use this for sensitive cryptographic operations.**

EaaS Architecture



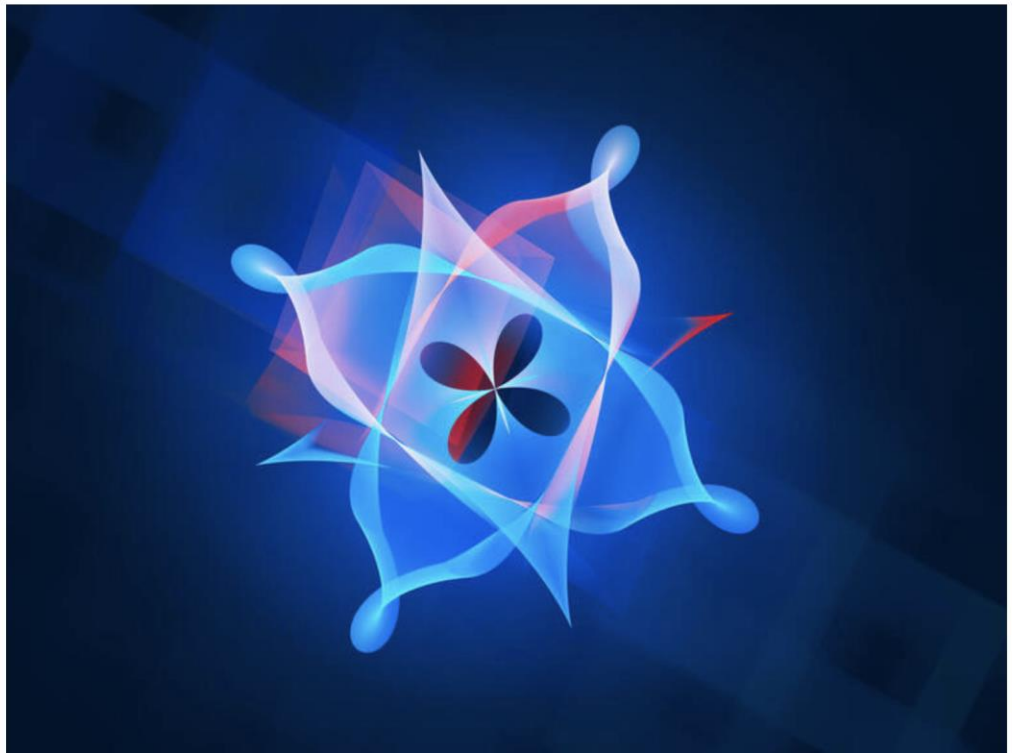
A. Vassilev and R. Staples. "Entropy-as-a-Service: Unlocking the Full Potential of Cryptography". *IEEE Computer*. September 2016.

Random Collaborations

IBM and Cambridge Quantum Computing announce random number generator service

by **Veronica Combs** in **Cloud**
on September 17, 2020, 10:01 AM PST

This cloud-based quantum computing service includes verification and is now available to members of the IBM Q Network.



Random Numbers in Your Pocket!

Latest News

LATEST NEWS PRESS RELEASES

ID Quantique and SK Telecom announce the world's first 5G smartphone equipped with a Quantum Random Number Generator (QRNG) chipset

ID Quantique announces that its newest Quantum Random Number Generator (QRNG) chip has been integrated in the new 5G smartphone 'Galaxy A Quantum'.

DISCOVER MORE

Investing in Randomness

Institute for Quantum Computing

IQC is a scientific research institute harnessing the quantum laws of nature to develop powerful new technologies.

Australian National University

DEPARTMENT OF QUANTUM SCIENCE
Research School of Physics
ANU College of Science

TRNG can Improve PRNG!

The Problem of Weak Entropy

	Our TLS Scan		Our SSH Scans	
Number of live hosts	12,828,613	(100.00%)	10,216,363	(100.00%)
... using repeated keys	7,770,232	(60.50%)	6,642,222	(65.00%)
... using vulnerable repeated keys	714,243	(5.57%)	981,166	(9.60%)
... using default certificates or default keys	670,391	(5.23%)		
... using low-entropy repeated keys	43,852	(0.34%)		
... using RSA keys we could factor	64,081	(0.50%)	2,459	(0.03%)
... using DSA keys we could compromise			105,728	(1.03%)
... using Debian weak keys	4,147	(0.03%)	53,141	(0.52%)
... using 512-bit RSA keys	123,038	(0.96%)	8,459	(0.08%)
... identified as a vulnerable device model	985,031	(7.68%)	1,070,522	(10.48%)
... model using low-entropy repeated keys	314,640	(2.45%)		

Improving Encryption with True Randomness

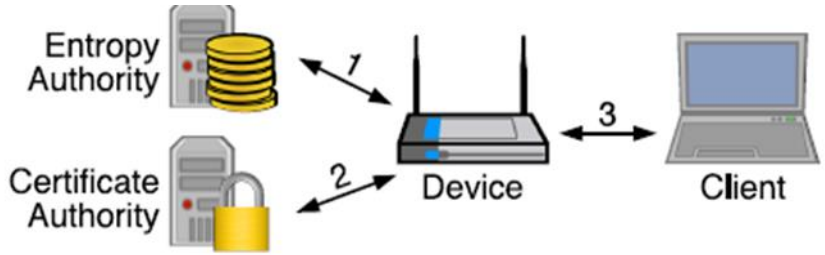
Ensuring High-Quality Randomness in Cryptographic Key Generation

Henry Corrigan-Gibbs*
Stanford University
henrycg@stanford.edu

Wendy Mu
Stanford University
wmu@cs.stanford.edu

Dan Boneh
Stanford University
dabo@cs.stanford.edu

Bryan Ford
Yale University
bryan.ford@yale.edu



Question and Answer Session

Real Random. LLC
802 E. Whiting St.
Tampa, FL 33602

doug@realrandom.co

Doug Hill – Founder
https://www.linkedin.com/in/doug-hill-2aabb318/