RANDOMNESS FROM CHAOTIC SYSYTEMS: BUOYANCY DRIVEN FLUID FLOW

ENTROPY LAMP SYSTEM

Cryptographic Random Number Generator Based on Buoyancy Driven Fluid Flow

The Entropy Lamp System is a Cryptographically Secure Random Number Generator (CSPRNG) developed at METU IVMER. Its unpredictability comes from the chaotic movements of entropy particles inside the liquid of the flask. This chaotic movement is driven by the temperature difference between the bottom and the top of the flask, which causes a density change within the liquid.

Entropy From Particles in Chaotic Fluid Flow

Entropy Lamp particles rotate and move chaotically. RGB color information from pixels in live frames inside the chaotic flow are captured and distilled to an alphabet size of 256 to produce raw data

Conditioned with SHA256 & SHAKE256

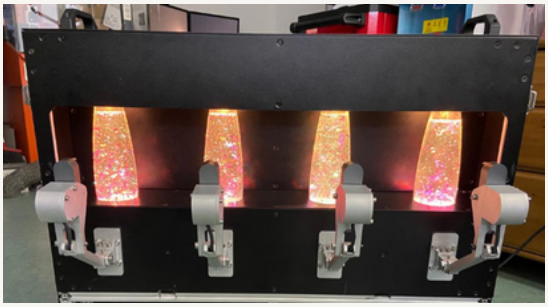
Raw data is inserted into SHA256 to break raw data biases and later inserted into SHAKE256 to increase the output size without reducing the security metrics.

Health Tests

Raw data from the entropy source is continuously monitored by RCT and APT health tests based on NIST SP 800-90B.

Applications

- Secure key generation
- Gaming / Lottery Industries
- Scientific Simulations



Key Features

01
Entropy From the Captured RGB Pixels in a Chaotic Fluid Flow and Distillation

02
50 kg Portable System

03
Continous Health Tests for Monitoring the Random Number Generator

04
SHA256 and SHAKE256 Conditioning

05
Up to 117 Mbit/s of Conditioned Output Speed

06
User Friendly Interaction at Terminal Level

Specifications

PARAMETERS	SPECIFICATIONS
ENTROPY SOURCE AND TESTS	
Physical process	RGB color informations of entropy particles and distillation
Min-entropy (SP 800-90B)	7.17 bits/byte · non-IID (Passed all permutation tests-Fails Chi-Square tests)
NIST SP800-22 Rev. 1a Test Battery	All passed
CONDITIONING	
Hash Function	SHA256
XOF	SHAKE256
Output data rate	117 Mbit/s ± 5%
HARDWARE AND INTERFACE	
SBC	Tinkerboard 2S x4
Supported OS	Linux
Web Camera	Logitech BRIO 4K x4
PHYSICAL CHARACTERISTICS	
Operating temperature	+65 °C (Flask Center Temperature)
Dimensions· Weight	202,5×805×455 mm³ · 50 kg
Heater Lamps x4	35 W/ 230V / 350 – 400 lm / 2800 K – 3000 K
Power	220 V/ 0.73 A / 160.6 W

METU · IVMER

Middle East Technical University, Research Park, 06800, Çankaya, Ankara, Türkiye

ivmer@metu.edu.tr