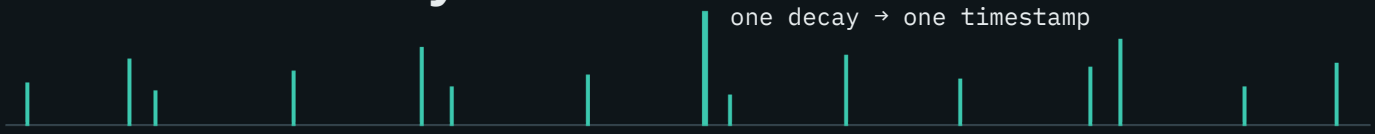
RANDOMNESS FROM RADIOACTIVE DECAY

KUTADGU

Quantum Random Number Generator Based on Radioactive Decay



Patent Number: TR 2022 015702 B

KUTADGU is a, patented, USB-interfaced random number generator developed at METU IVMER. Its entropy comes from the arrival times of alpha particles from a small harmless americium-241 source, which are time-stamped by a picosecond-level resolution time-to-digital converter and conditioned with SHAKE256 inside an FPGA.

Entropy From Decay Timing

Each alpha particle that strikes the silicon detector makes a pulse. A comparator turns it into an edge that a TDC-GPX2 timestamps with ≈10 ps RMS precision.

Conditioned with SHAKE-256

An IGLOO2 FPGA feeds the timestamps into a SHAKE256 sponge (FIPS 202), reseeded continuously from the source. Output leaves over USB at up to 19.2 Mbit/s.

On-Chip Health Tests

Raw data from the entropy source is continuously monitored by RCT and APT on-chip health tests based on NIST SP 800-90B. The source yields a min-entropy of 7.86 bits per byte for every 1 MB of data, achieving a 97% success rate on NIST IID tests.

Applications and features

One bus-powered USB board: no external supply, no custom driver, no network.

- Secure key generation
- Plug and play: no setup, no custom driver
- Portable: runs from a laptop's USB port



Key Features

01
Entropy from the arrival times of alpha decays

02
Picosecond-level time stamps from a TDC-GPX2

03
Tuned threshold that separates decay pulses from noise

04
SHAKE256 conditioning in FPGA logic, continuously reseeded

05
Up to 19.2 Mbit/s of conditioned random output

06
Plain USB: bus-powered, virtual COM ports, Python capture tools

Specifications

PARAMETERS	SPECIFICATIONS
ENTROPY SOURCE AND TESTS	
Physical process	Arrival times of americium-241 alpha decays
Min-entropy (SP 800-90B)	7.86 bits per byte with a %97 success rate on IID tests
NIST SP800-22 Rev. 1a Test Battery	All passed
TIMESTAMPING AND CONDITIONING	
Time-to-digital converter	TDC-GPX2, high-resolution mode
Single-shot precision	≈10 ps RMS
Conditioning	SHAKE256
Output data rate	19.2 Mbit/s ± 5%
HARDWARE AND INTERFACE	
FPGA	Microchip IGLOO2 M2GL005
Host interface	USB 2.0 via FTDI FT4232H (virtual COM ports), bus-powered
Supported OS	Windows, Linux, macOS: any OS with an FTDI VCP driver; no custom driver[3]
PHYSICAL CHARACTERISTICS	
Operating temperature	+0 °C to +50 °C ambient, non-condensing
Storage temperature	−20 °C to +70 °C, non-condensing (board)
Dimensions · Weight	97 × 33 × 20 mm · 33 grams
Power (W)	USB bus-powered (1.25W)
Radioactive source	Am-241 (≈33kBq)

METU · IVMER

Middle East Technical University, Research Center, 06800, Ankara, Türkiye

ivmer@metu.edu.tr