ESCAPE

RaCAF ANR-15-CE40-0016-01 project

http://www.lirmm.fr/~ashen/racaf/

Permanents

B. Durand, PR UM2
G. Lafitte, MC UM2
A. Romashchenko, CR CNRS
A. Shen, DR CNRS

Others:

R. Ishkuvatov (2019–2020)
F. Givors (2020)

LIRMM

What is randomness?

- Philosophy: why do we believe that

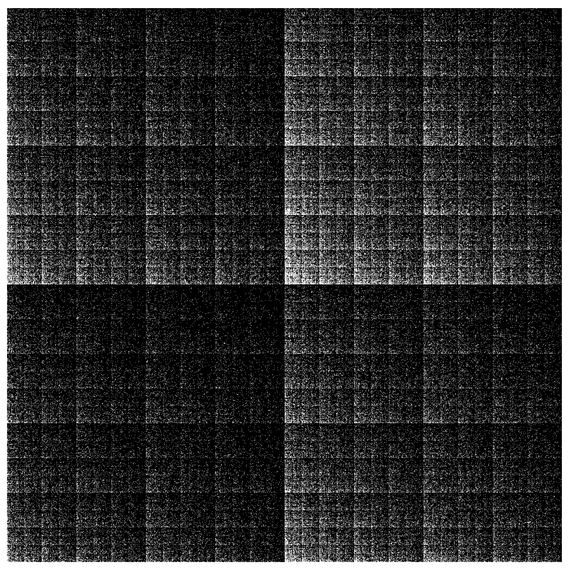
  0010101111101010010111

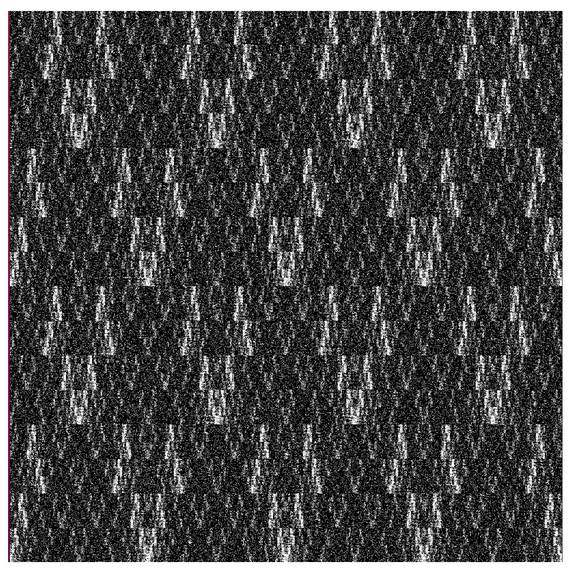
  may produced by a fair coin, but do not believe that

  0101010101010101010101

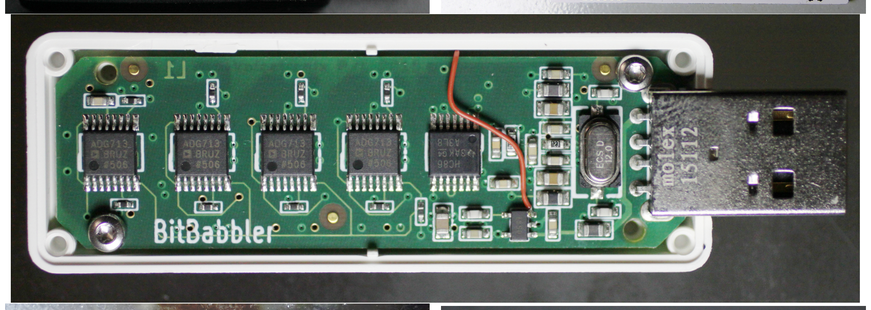
- Mathematics: how can we define formally the notion of a random sequence (finite or infinite): Mises, Church, Kolmogorov, Levin, Martin-Löf, Chaitin, Schnorr, etc.
- Practice: we need random bits for cryptography, randomized algorithms, games, lotteries, etc. How can we reliably generate them? How can we test the generators?

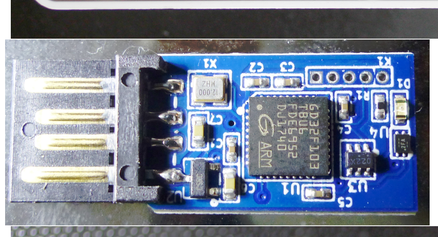
Not all generators are equal

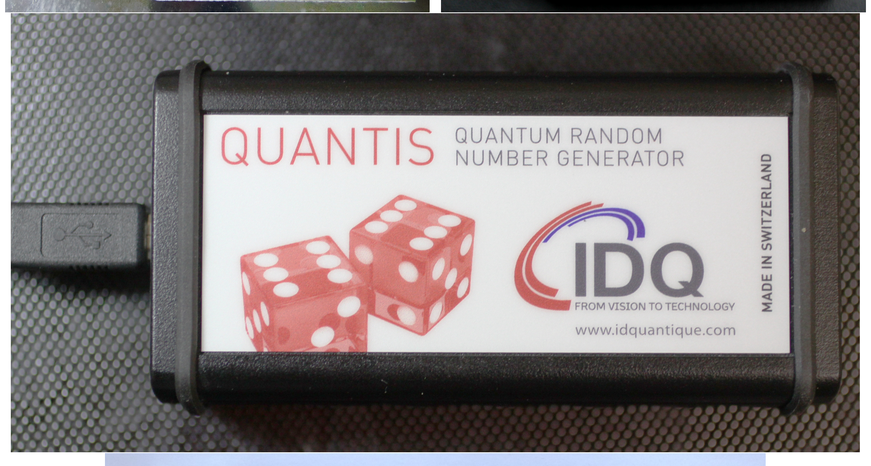


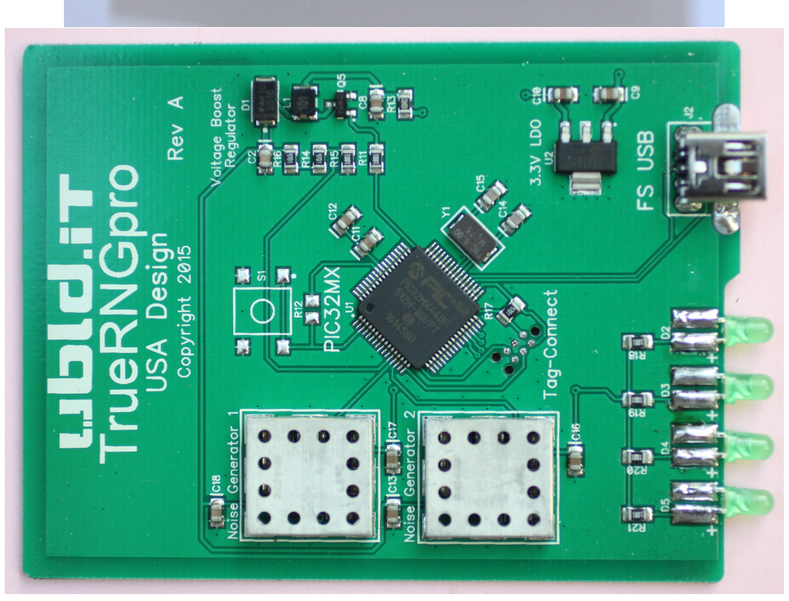


Random bit generators

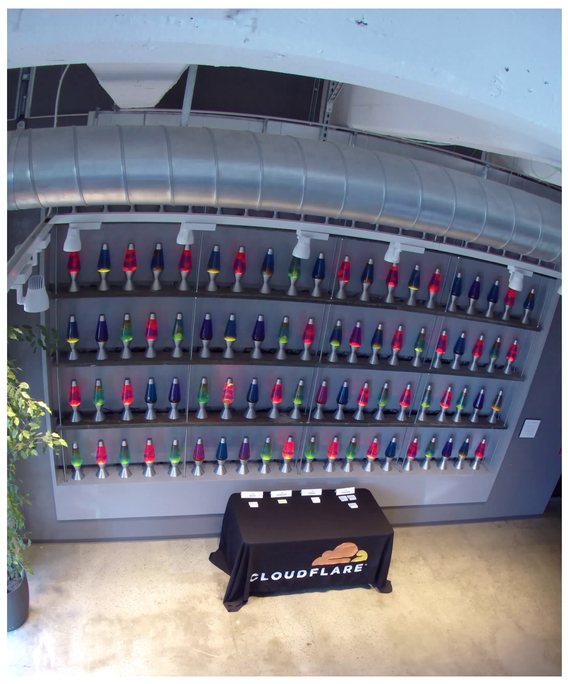




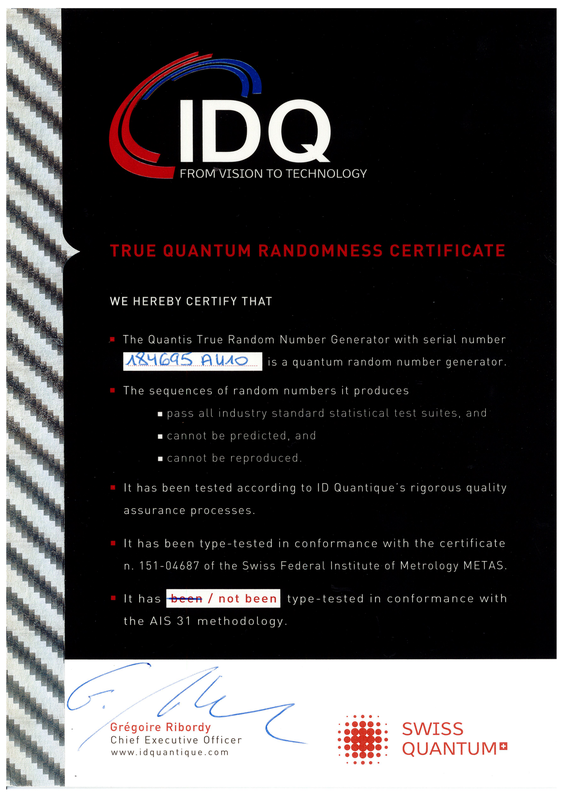




DIY approach



Certificates?




```
Entropy = 7.999997 bits per byte.

Optimum compression would reduce the size
of this 102400000 byte file by 0 percent.

Chi square distribution for 102400000
samples is 484.39, and randomly
would exceed this value less
than 0.01 percent of the times.

Arithmetic mean value of data bytes
is 127.5025 (127.5 = random).
Monte Carlo value for Pi is 3.141912310
(error 0.01 percent).
Serial correlation coefficient is 0.000126
(totally uncorrelated = 0.0).
```

Project goals

- Use theoretical background to study the state of the art for
  - hardware ("non-deterministic") random bit generators
  - tests suites for testing randomness
  - standards for generators and tests
  - tools for "randomness extraction" (conditioning)
- Finding deficiencies and flaws in the existing techniques, tools, standards
- Corrections of the flaws found
- Trying new kinds of tests and randomness extraction methods
- Recommendations for making a hardware RNG

Université Montpellier
cnrs
Agence Nationale de la Recherche
ANR