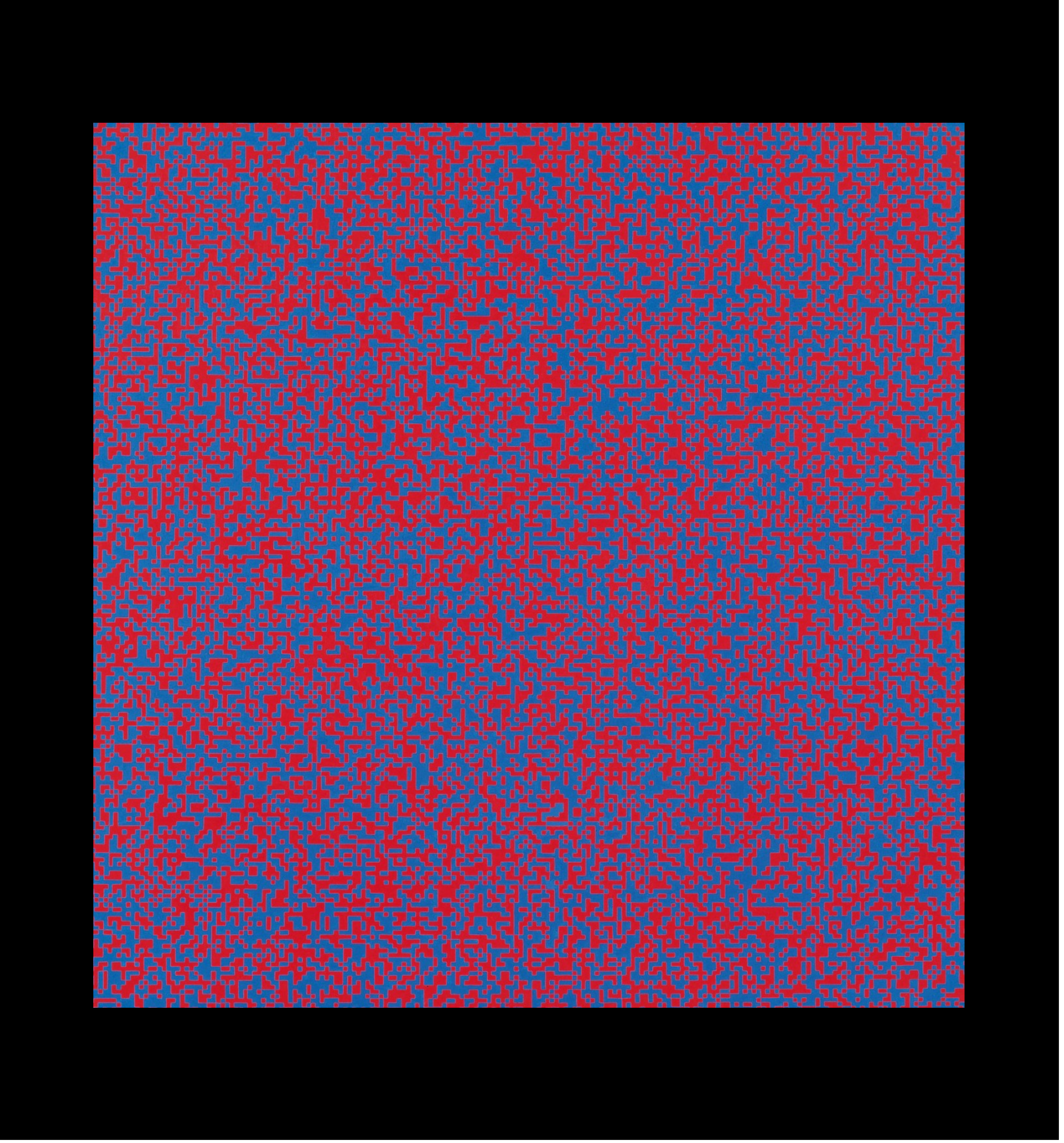


François Morellet
*Random Distribution of 40,000 Squares using the Odd and Even Numbers of a Telephone Directory* 1960

# In-Silico generation of random bit streams

RANDOM POWER

## the value of unpredictability

Massimo Caccia
Università dell'Insubria & Random Power s.r.l.
massimo.caccia@randompower.eu

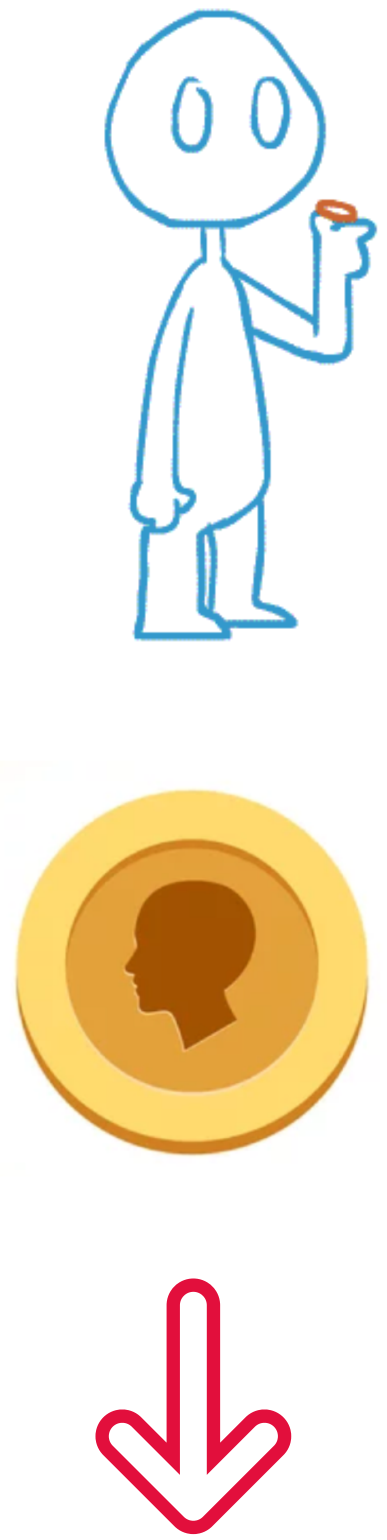
**AIDAInnova Training Course on Quantum tech**
**CERN, January 22nd 2025**

# what we do:

# what we do:

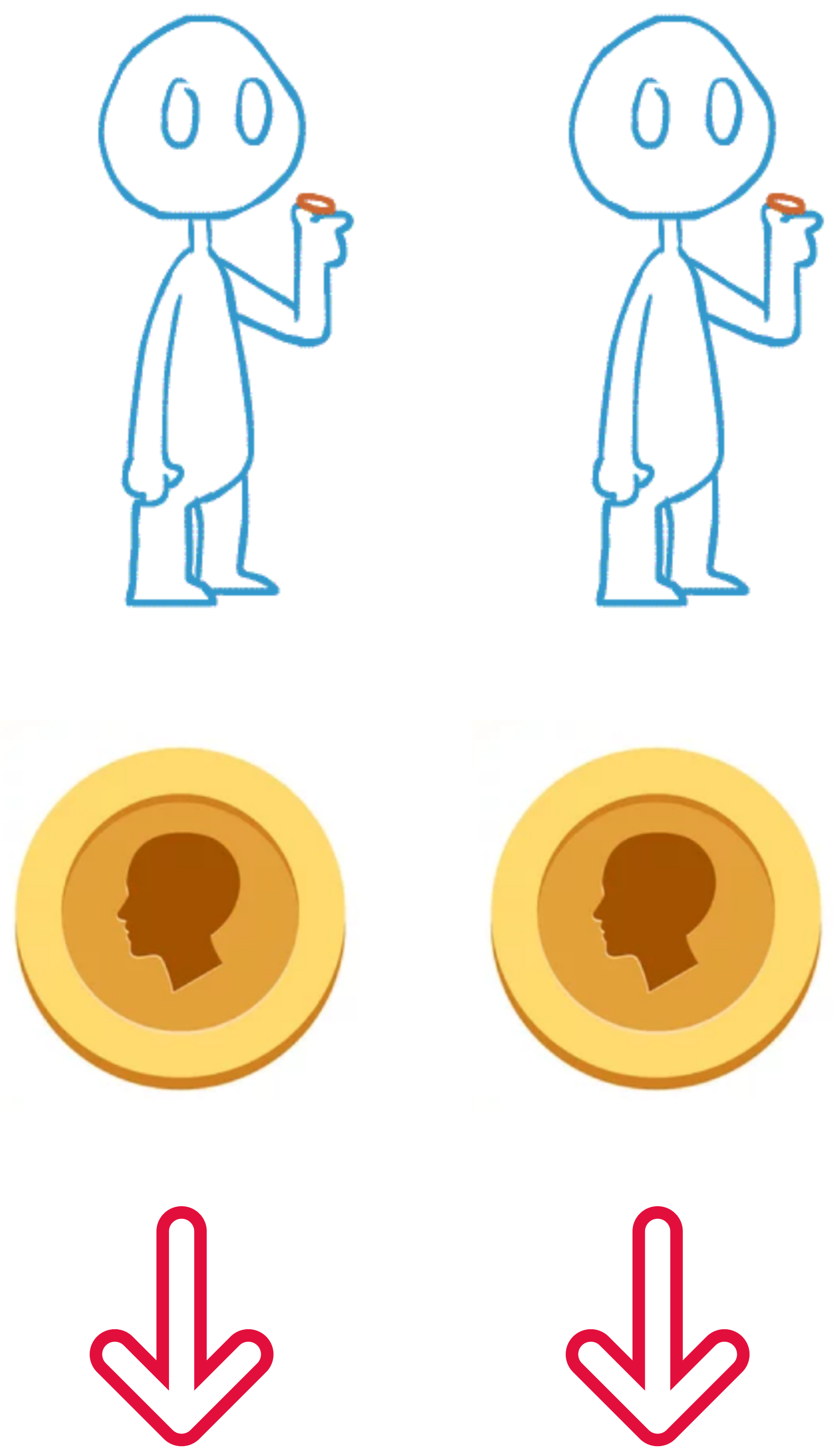
# what we do:

# what we do:



1

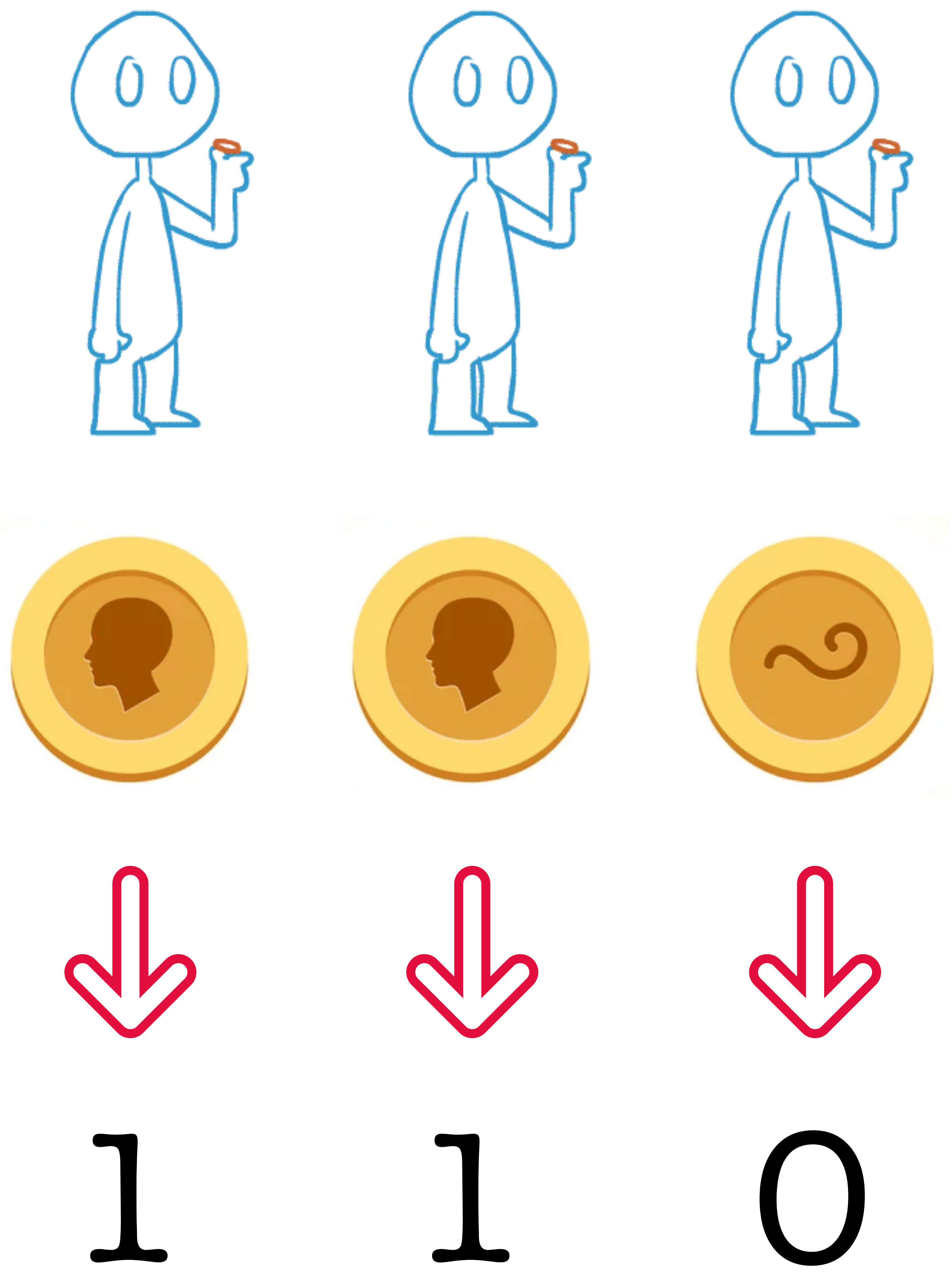
# what we do:



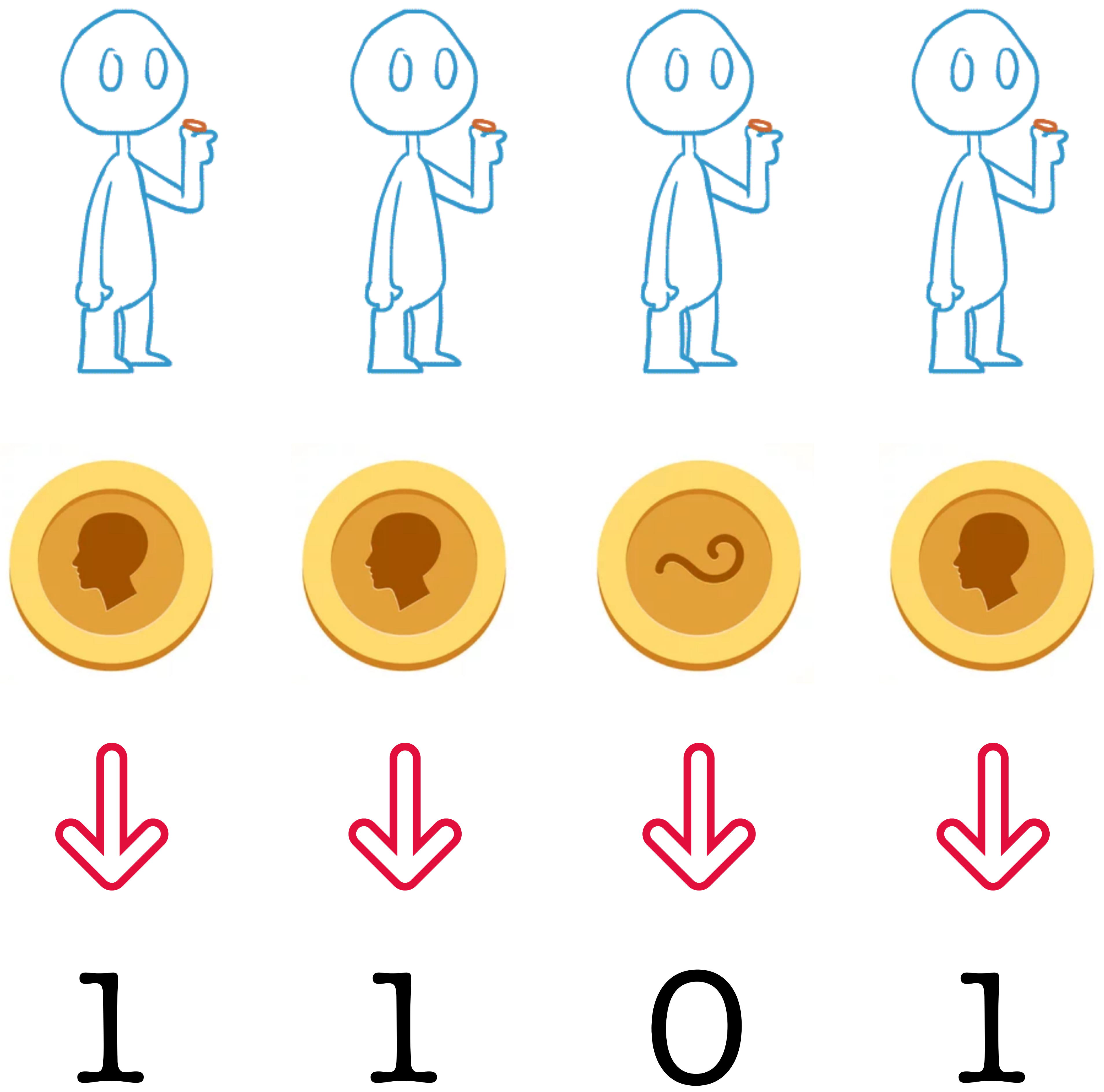
1 1

FALLING WALLS VENTURE

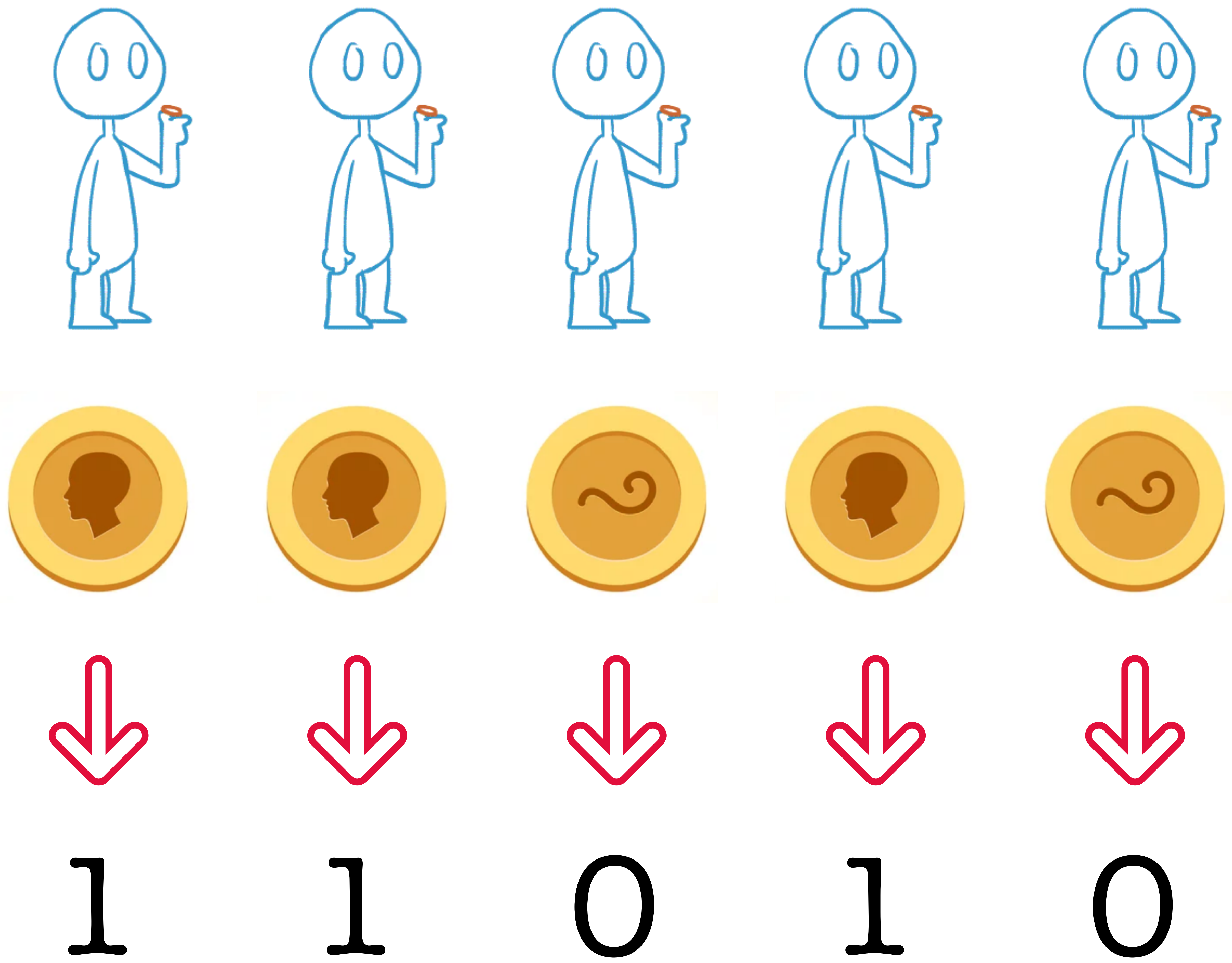
# what we do:



## what we do:

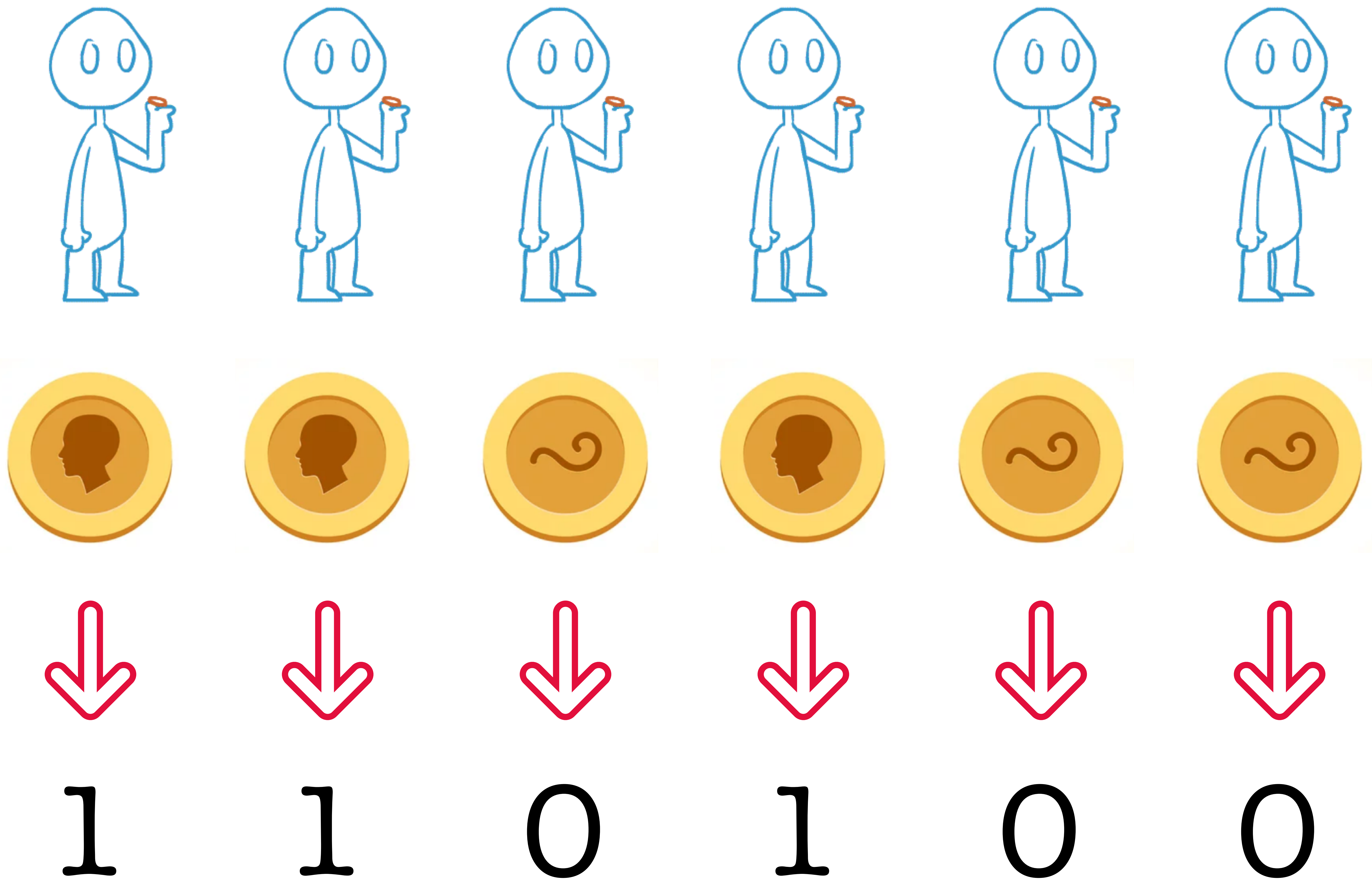


w h a t w e d o :

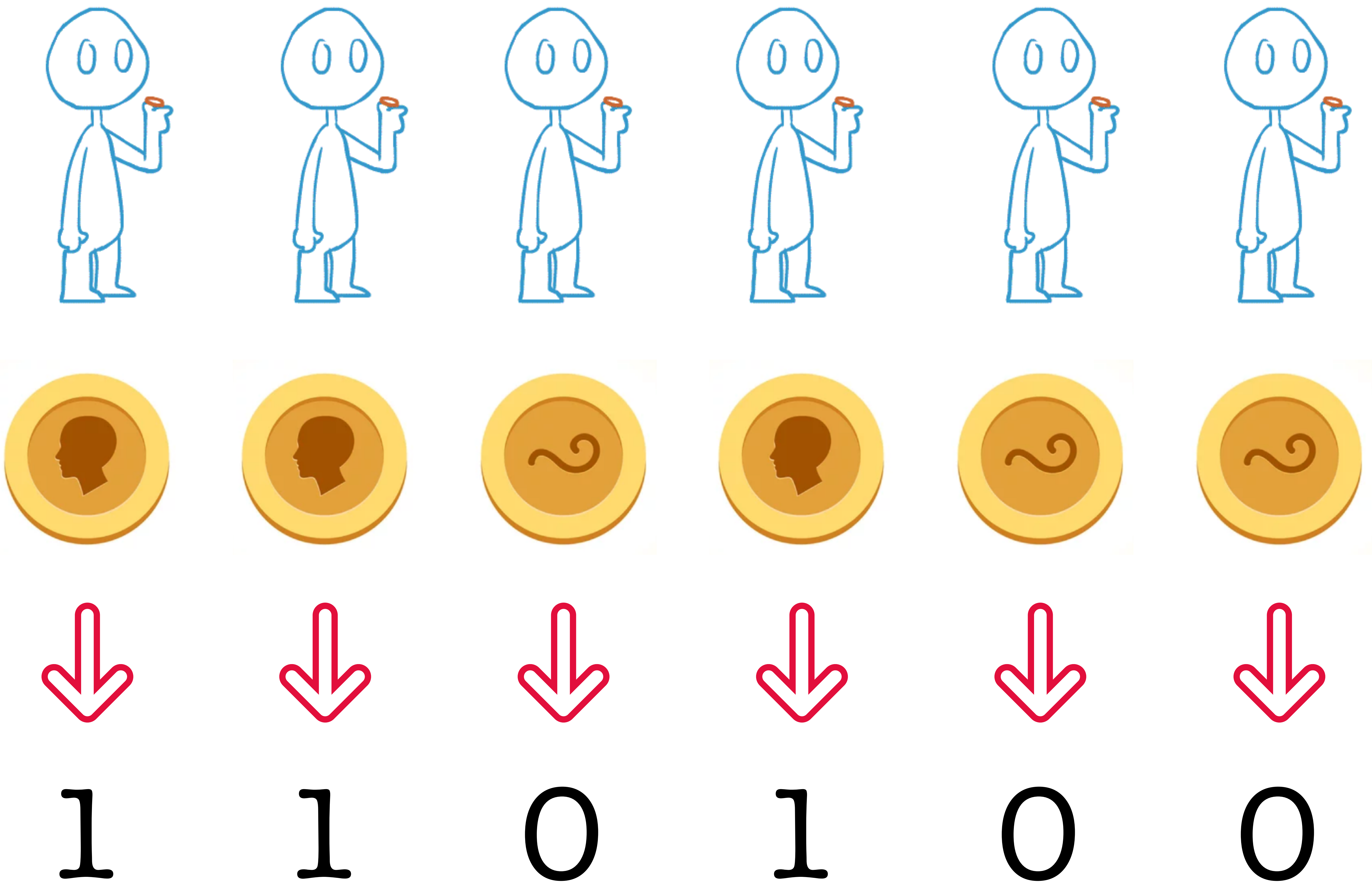


FALLING WALLS VENTURE

## what we do:



## what we do:




RANDOM POWER

**Random Power is developing a platform of Silicon based, patent protected, "QUANTUM coin flippers", generating virtually endless streams of random bits**

# w h a t   f o r :

**Unpredictability to preserve the predictability of our clockwork world**

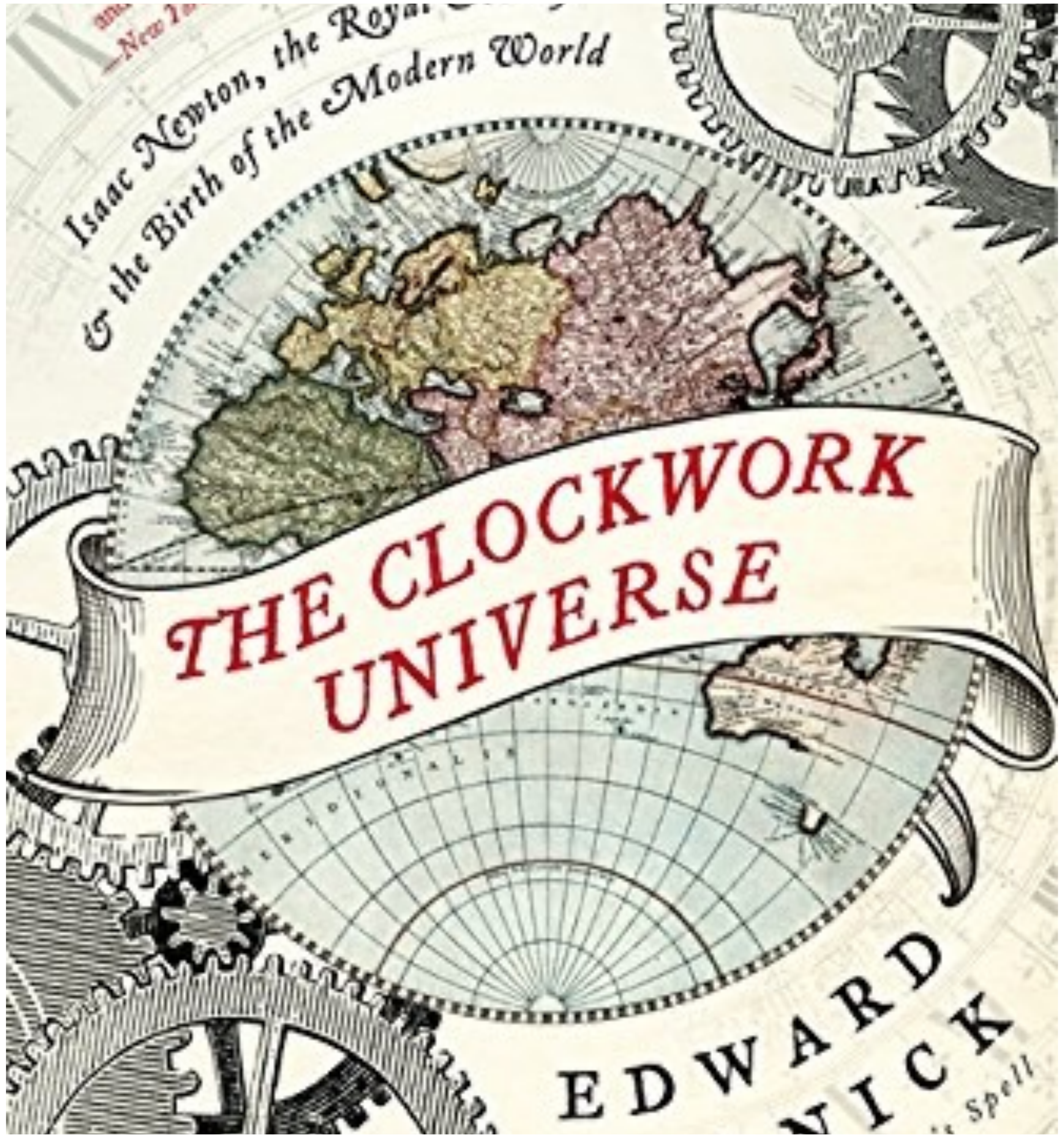
- There is definitely a hype about Random bit streams, not only for cryptograhy & authentication but also for gaming, virtual reality, Monte Carlo simulations , Privacy Preservation Procedures and Identity management

to learn more, watch this BBC report:

**The search for the random numbers that run our lives**

6 July 2024

Share




The Clockwork Universe
Isaac Newto, Royal Society, and the Birth of the Modern Worldl
by Edward Dolnick - 2011 Harper Collins

# the problem:



**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

- **1951, John Von Neumann** [J. Res. Nat. Bur. Stand. Appl. Math. Series 3, 36-38 (1951)]

**Various Techniques Used in Connection With Random Digits**

**Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.**

# the problem:



**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

# the problem:

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

## a 2013 NSA scandal unveiled by the NYT:

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition

The New York Times — U.S.

Search All NYTimes.com — Go

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

POLITICS | EDUCATION | TEXAS

### Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break. Related Article »

Excerpt from 2013 Intelligence Budget Request | Bullrun Briefing Sheet

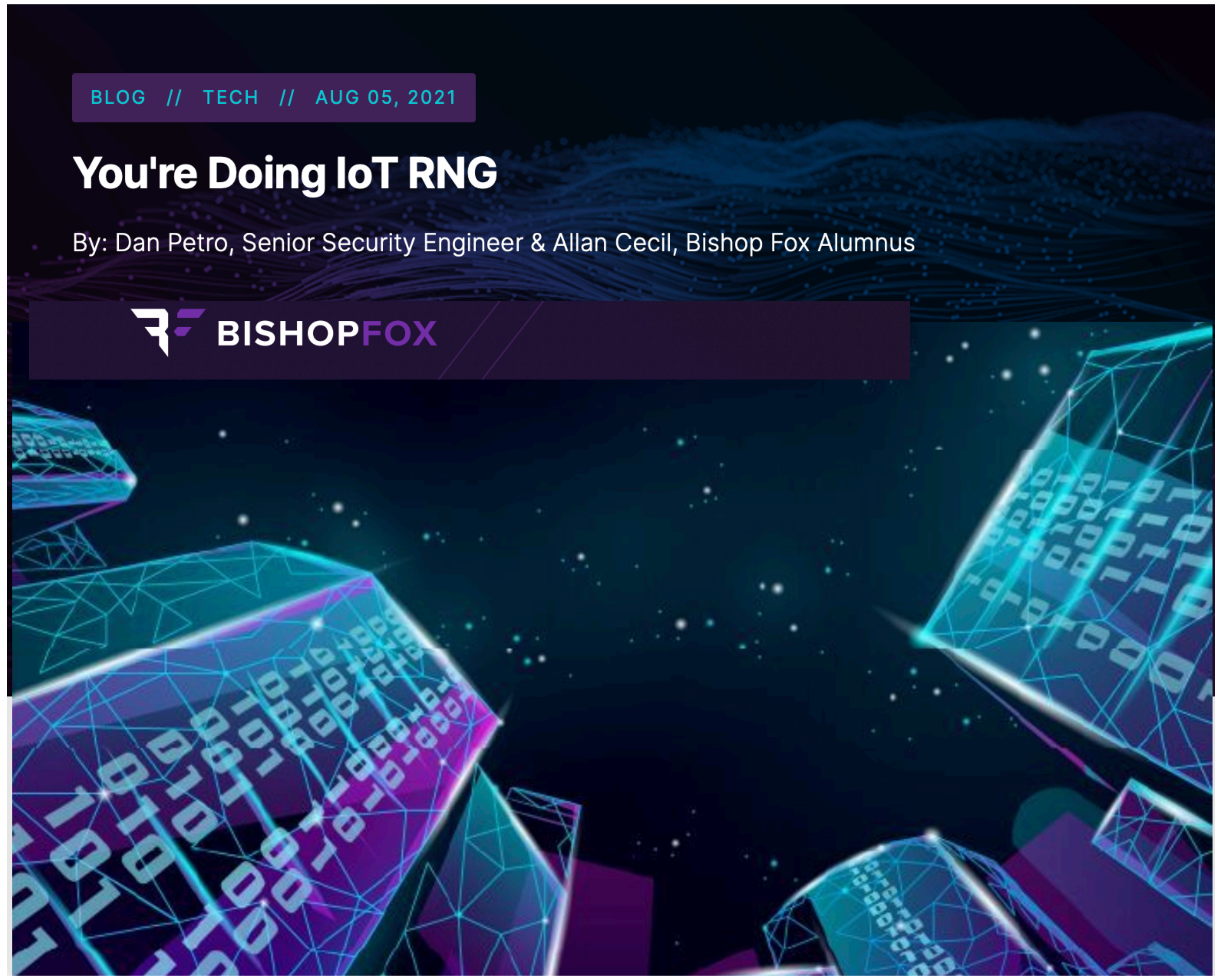
This excerpt from the N.S.A.'s 2013 budget request outlines the ways in which the agency circumvents the encryption protection of everyday Internet communications. The Sigint Enabling Project involves industry relationships, clandestine changes to commercial software to weaken encryption, and lobbying for encryption standards it can crack.

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

# the problem:

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

[a 2021 finding on weakness in Randomness generation for IoT:]




Share

There's a crack in the foundation of Internet of Things (IoT) security, one that affects **35 billion devices worldwide**. Basically, every IoT device with a hardware random number generator (RNG) contains a serious vulnerability whereby it fails to properly generate random numbers, which undermines security for any upstream use.

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

[a 2023 article on FORBES:]

**Challenges Of Zero-Knowledge Proof Technology For Compliance**

**Alexander Ray** Forbes Councils Member

**Forbes Business Council** COUNCIL POST | Membership (fee-based)

**Problem 2: Vulnerability To Random Number Generator Attacks**

**Generating REAL, certified and *robust* randomness is far from being trivial, both using algorithmic solutions and exploiting unpredictable natural phenomena based on classical physics**

a 2020 paper by the U.S. Census Bureau:

## Randomness Concerns When Deploying Differential Privacy

Simson L. Garfinkel
US Census Bureau
Suitland, MD
*simson.l.garfinkel@census.gov*

Philip Leclerc
US Census Bureau
Suitland, MD
*philip.leclerc@census.gov*

true data. Thus, while the data for the Decennial Census can be stored in a few tens of gigabytes, protecting its output statistics will require the DAS to use roughly 90TB of random data.

a 2023 article on FORBES:

**Challenges Of Zero-Knowledge Proof Technology For Compliance**

**Alexander Ray** Forbes Councils Member
**Forbes Business Council** COUNCIL POST | Membership (fee-based)

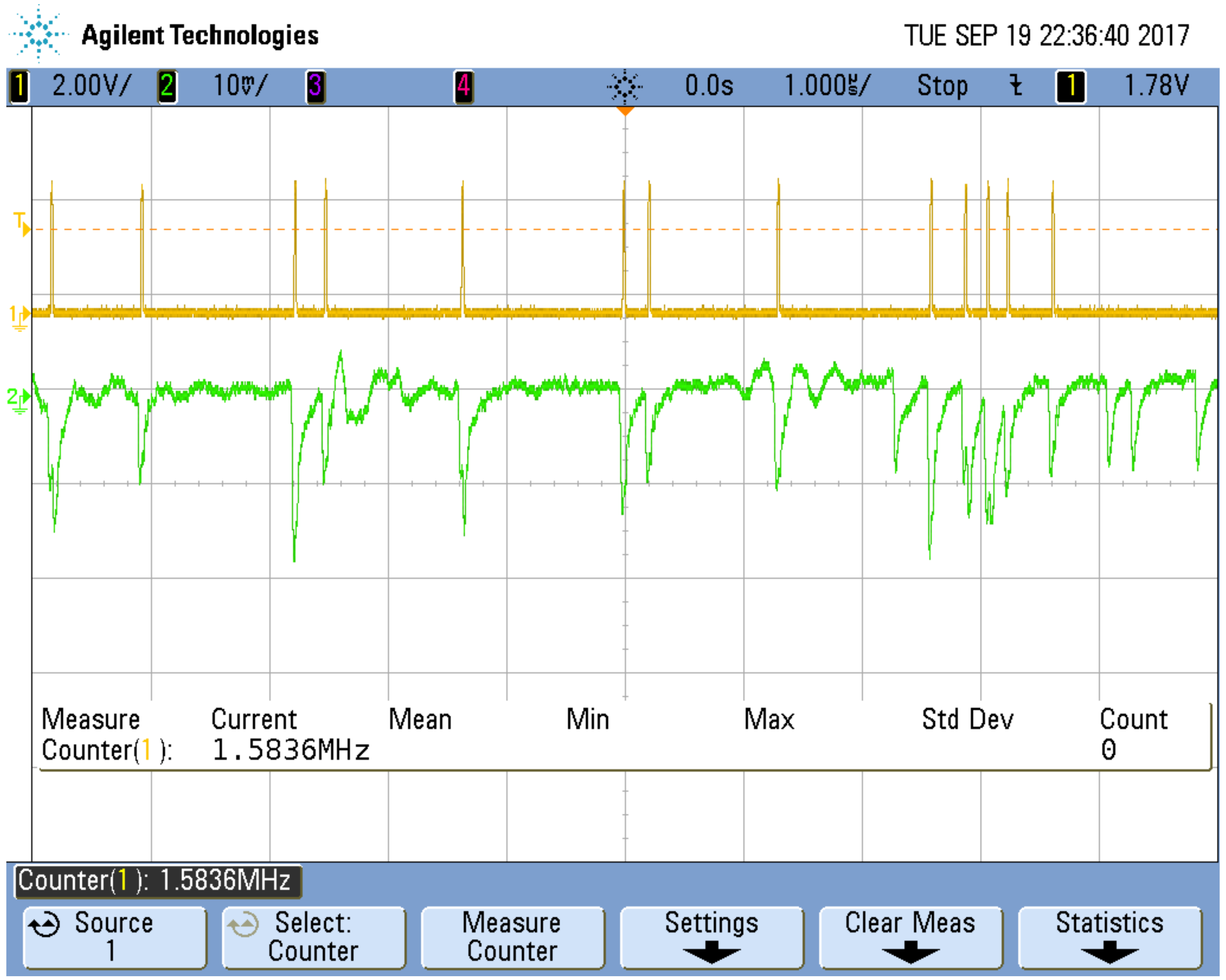
**Problem 2: Vulnerability To Random Number Generator Attacks**

# RANDOM NUMBER GENERATION BY OBSERVING UNPREDICTABLE QUANTUM PHENOMENA

where unpredictability is secured by the very same laws of Nature.

# RANDOM NUMBER GENERATION BY OBSERVING UNPREDICTABLE QUANTUM PHENOMENA

where unpredictability is secured by the very same laws of Nature.



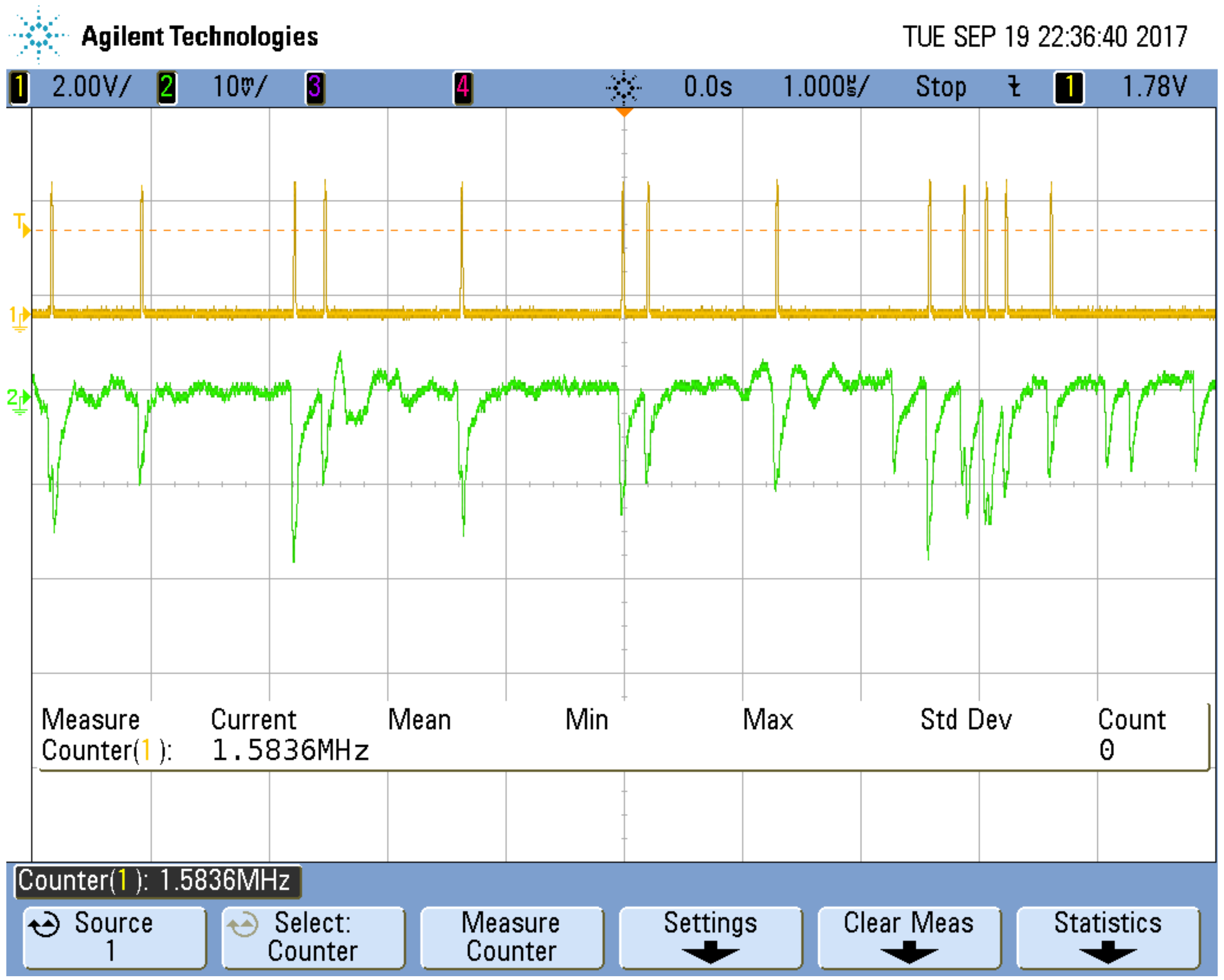
# RANDOM NUMBER GENERATION BY OBSERVING UNPREDICTABLE QUANTUM PHENOMENA

where unpredictability is secured by the very same laws of Nature.

✱ **The very first example**: exploiting the **unpredictability of Radioactive Decays**

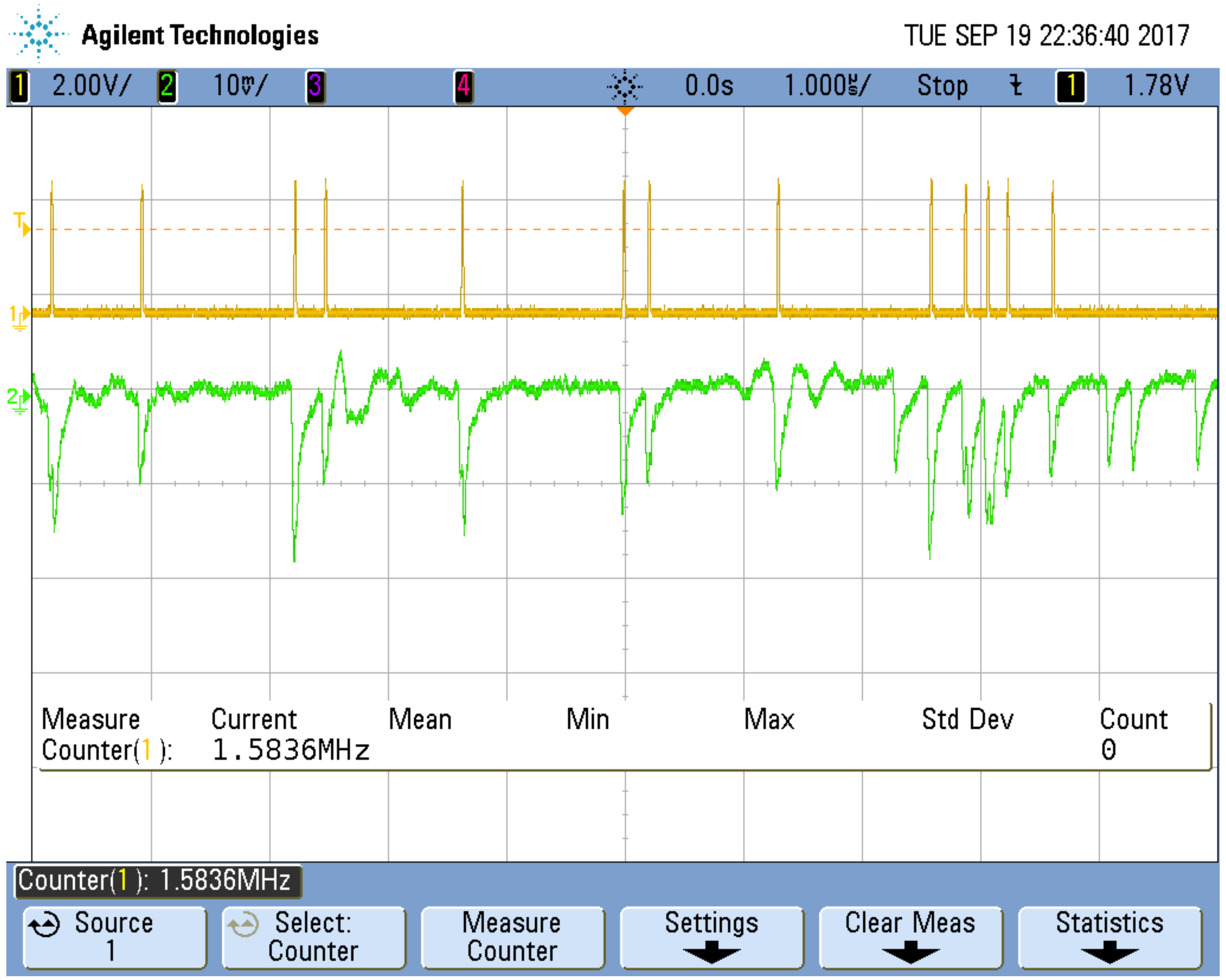
the sequence of detected decays can be used to generate random bits with different recipes:

- check the parity of the number of pulses in a time window
- pre-define the time window in a way that is equally like to have or not to have a single pulse



# RANDOM NUMBER GENERATION BY OBSERVING UNPREDICTABLE QUANTUM PHENOMENA

where unpredictability is secured by the very same laws of Nature.




RANDOM POWER

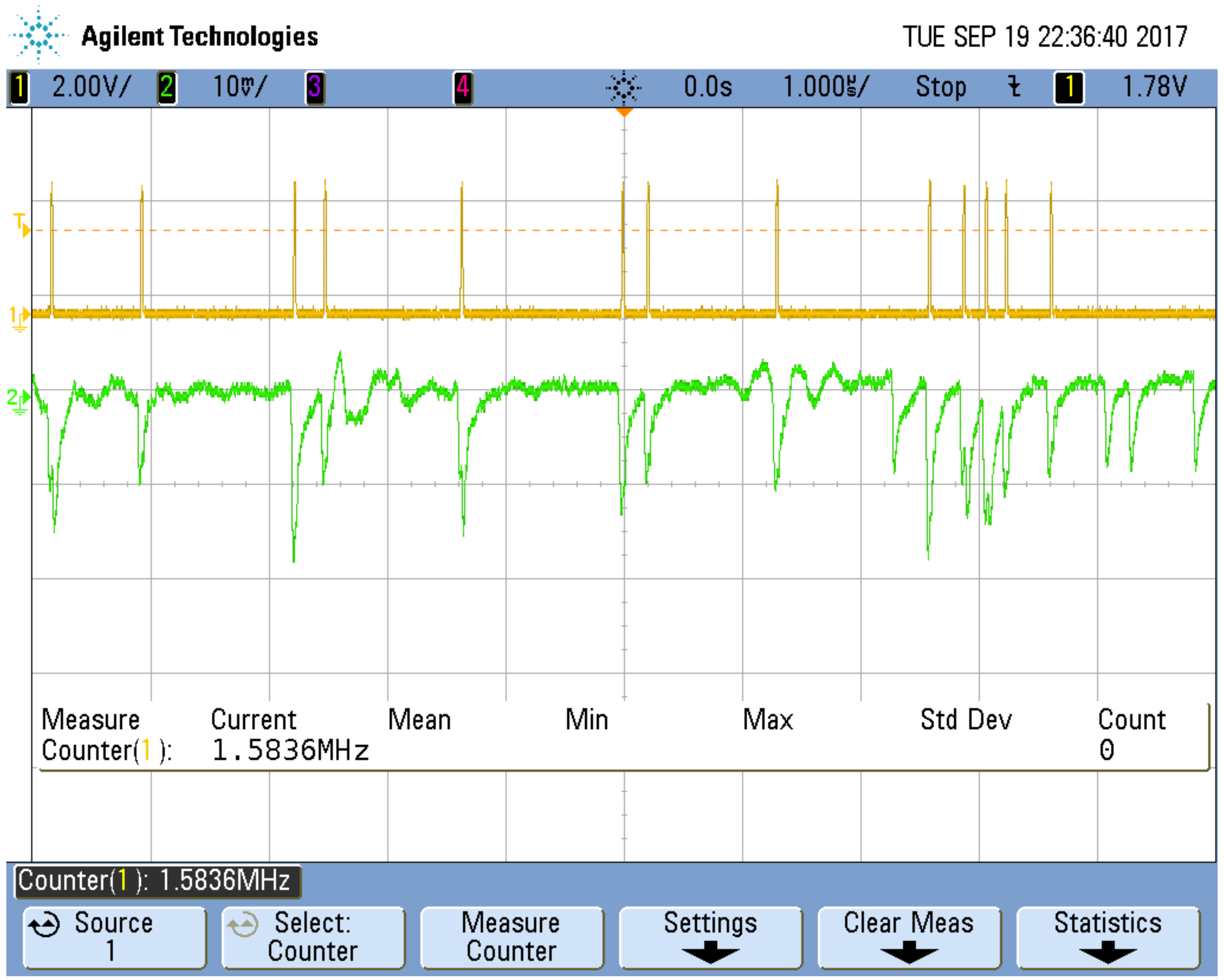
# RANDOM NUMBER GENERATION BY OBSERVING UNPREDICTABLE QUANTUM PHENOMENA

where unpredictability is secured by the very same laws of Nature.

Inspired by Forrest Gump, we say:

✱ **RADIOACTIVE IS AS RADIOACTIVE DOES**

**The idea behind RANDOM POWER is to replace a radioactive source with something safer, more handy, cost effective, simple, robust, providing sequences of pulses mimicking radioactive decays.**



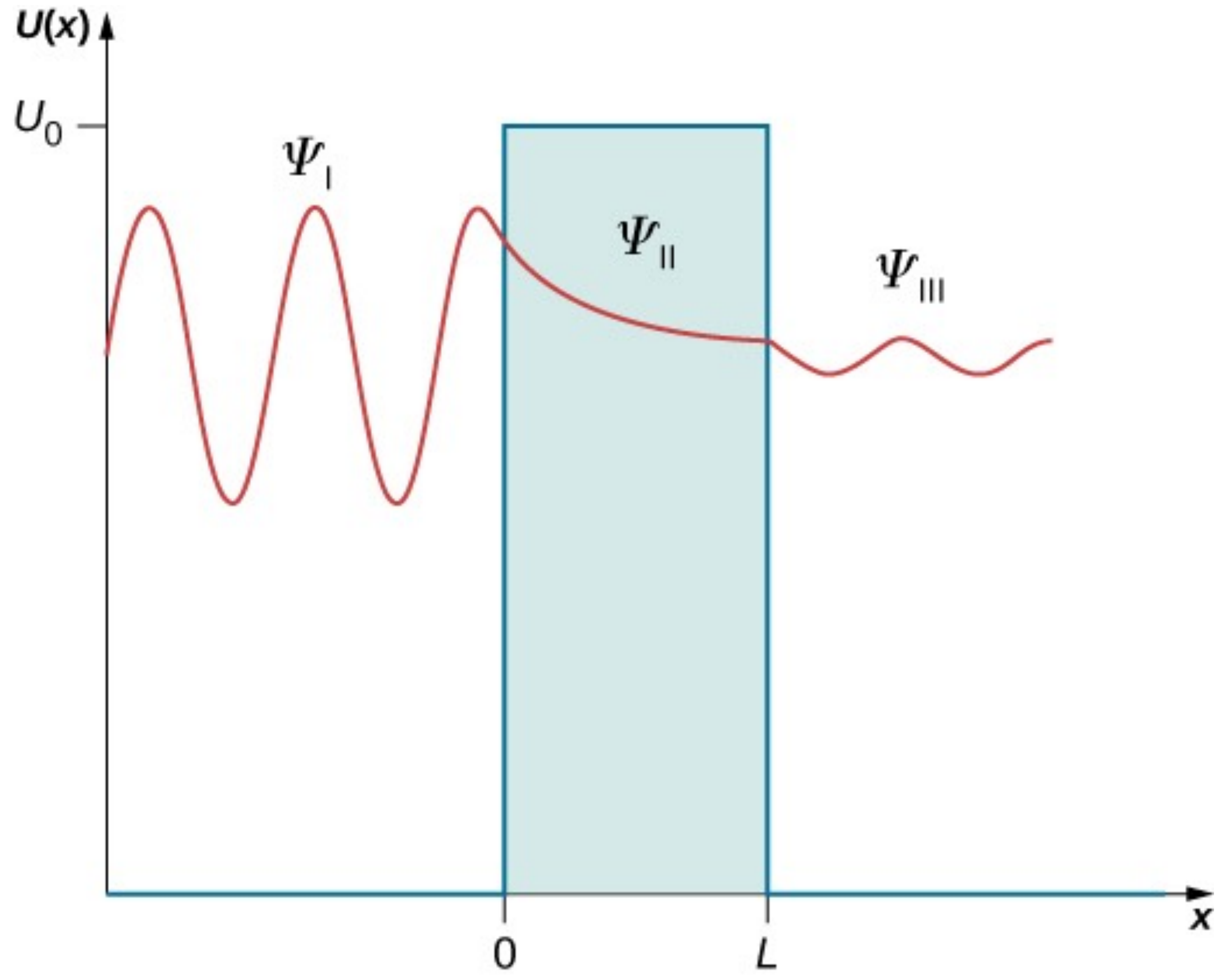
# A THREE STEP DANCE:

# A THREE STEP DANCE:

The name of the game is **QUANTUM TUNNELING:**

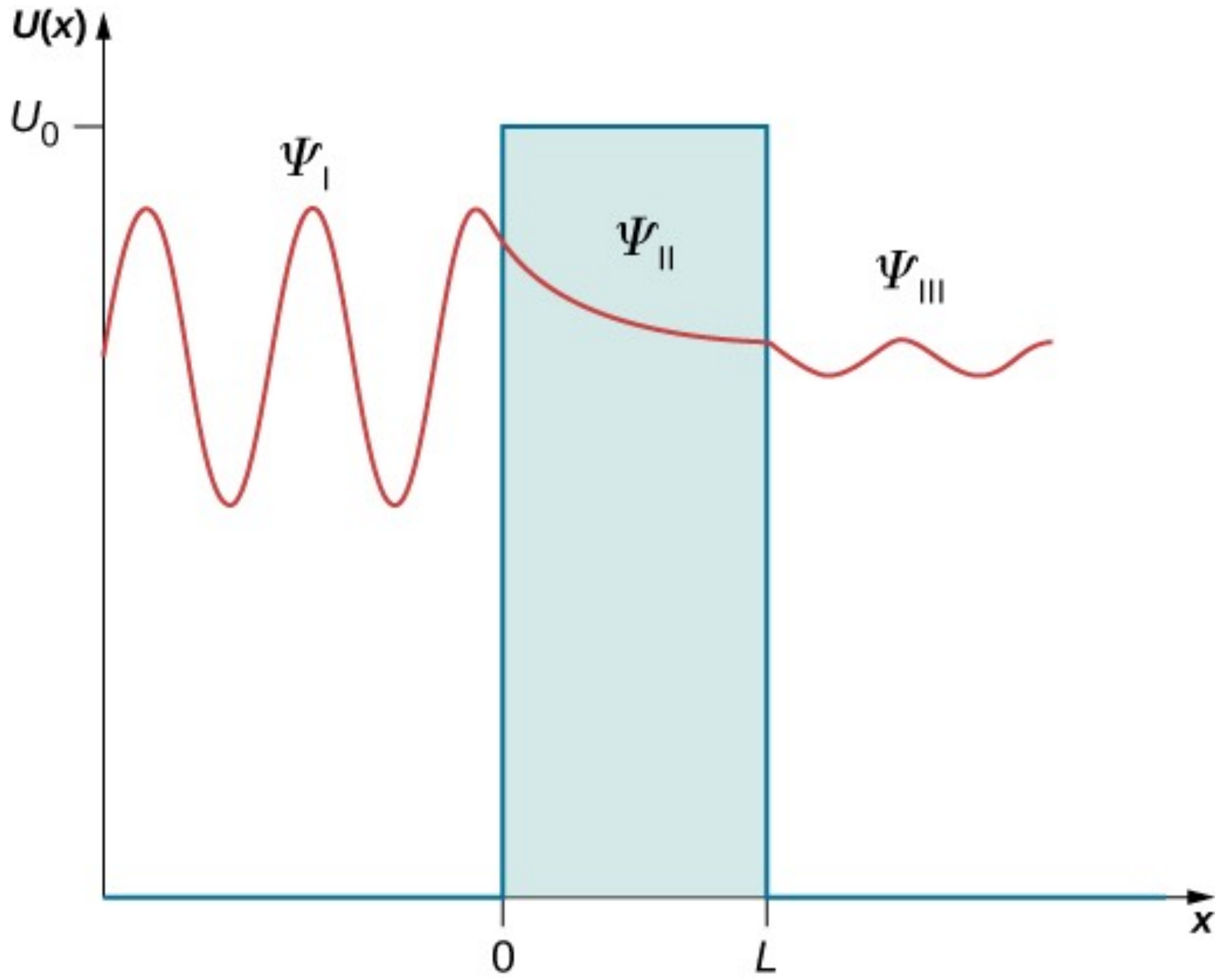
* **Electrons** and quantum entities in general are not like a  but they rather appear as a 

when they bounce against a [potential] barrier, they can occasionally go through in an unpredictable way.



# A THREE STEP DANCE:

The name of the game is **QUANTUM TUNNELING:**




* **Electrons** and quantum entities in general are not like a  but they rather appear as a 

when they bounce against a [potential] barrier, they can occasionally go through in an unpredictable way.

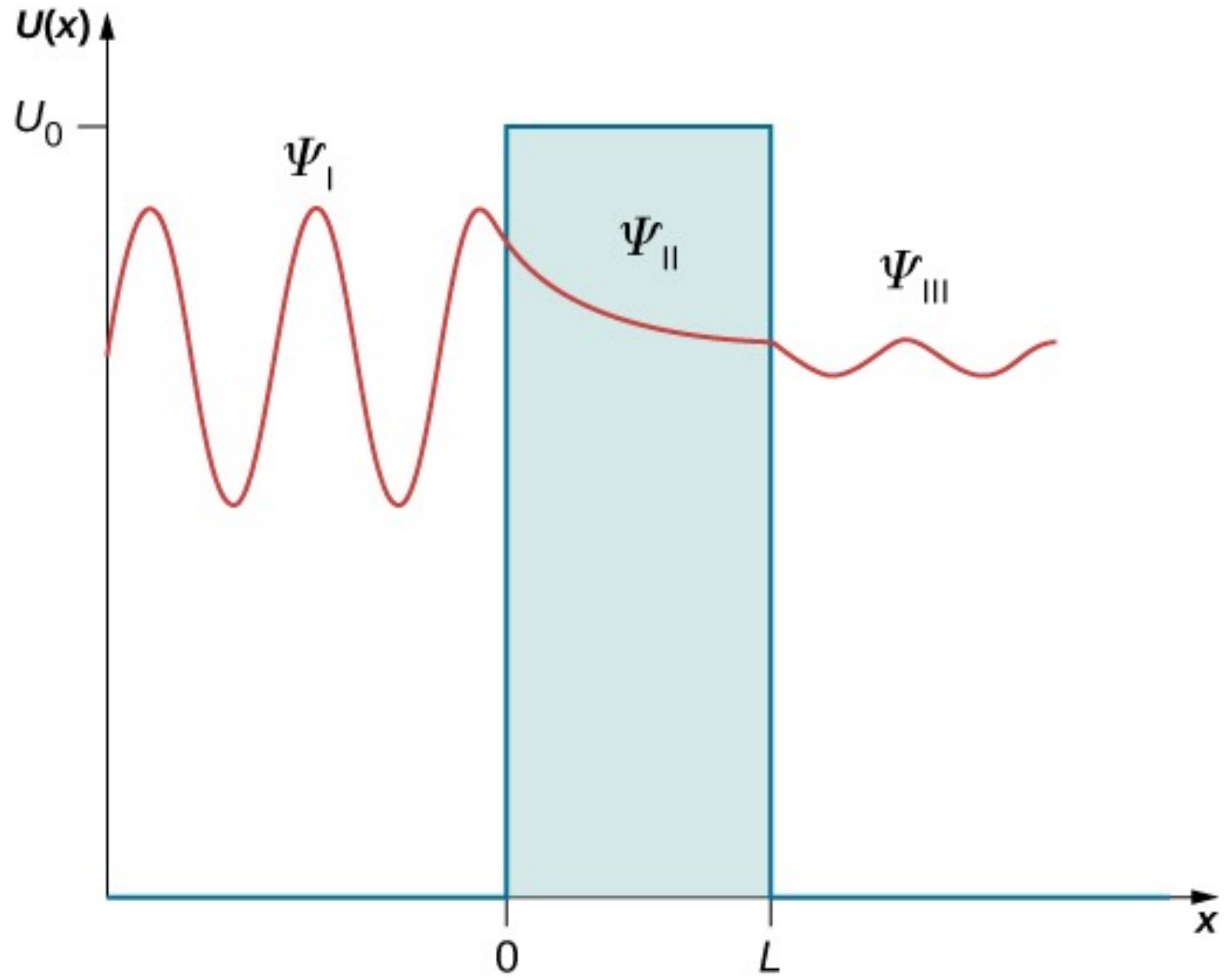
* When this is happening, the “ghost” electron enters a region of high electric field, generating a **current pulse** by impact ionisation

# A THREE STEP DANCE:

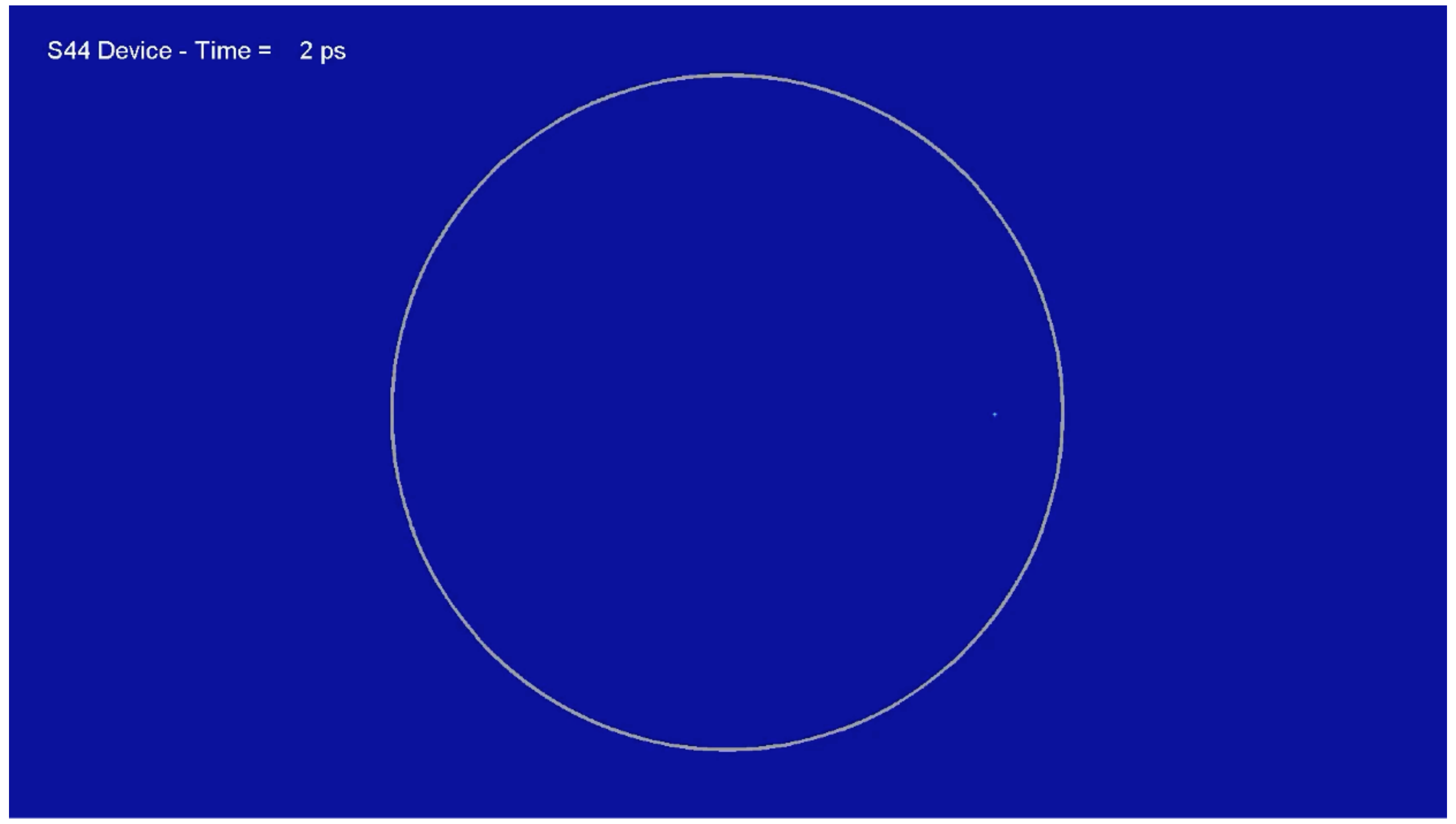
The name of the game is **QUANTUM TUNNELING:**

- **Electrons** and quantum entities in general are not like a  but they rather appear as a 

when they bounce against a [potential] barrier, they can occasionally go through in an unpredictable way.




- When this is happening, the "ghost" electron enters a region of high electric field, generating a **current pulse** by impact ionisation



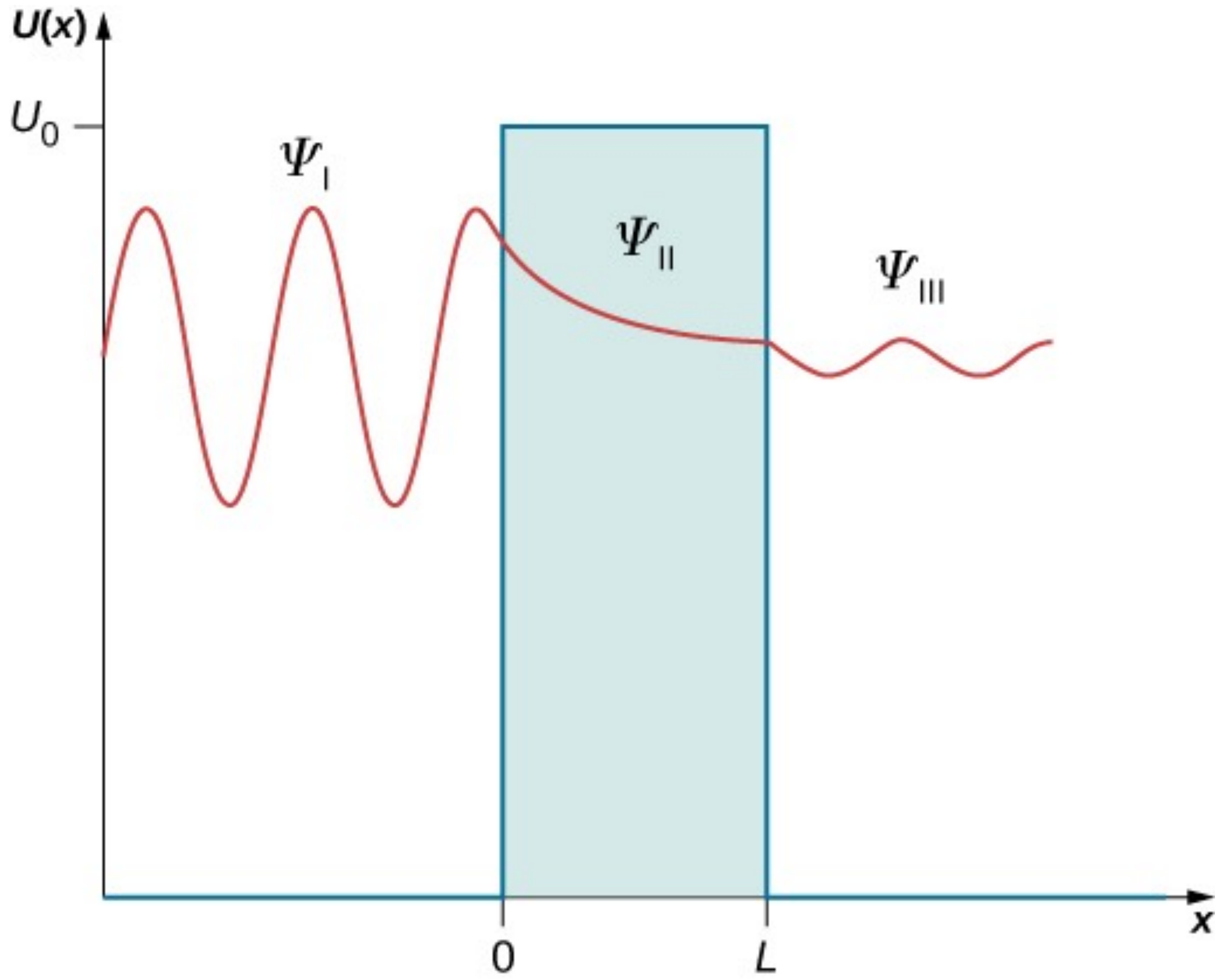
# A THREE STEP DANCE:

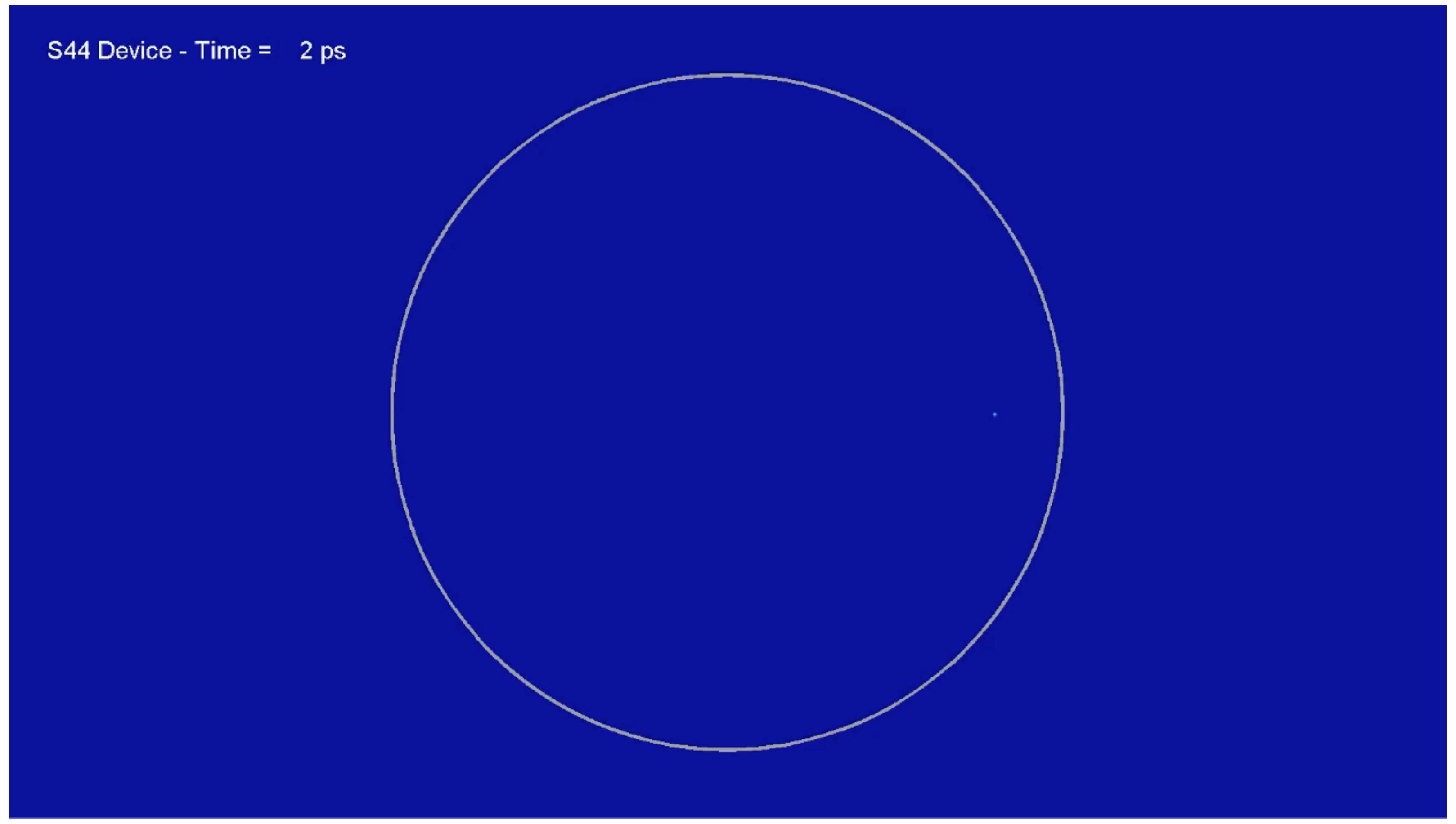
The name of the game is **QUANTUM TUNNELING:**

- **Electrons** and quantum entities in general are not like a  but they rather appear as a 

when they bounce against a [potential] barrier, they can occasionally go through in an unpredictable way.

- When this is happening, the “ghost” electron enters a region of high electric field, generating a **current pulse** by impact ionisation



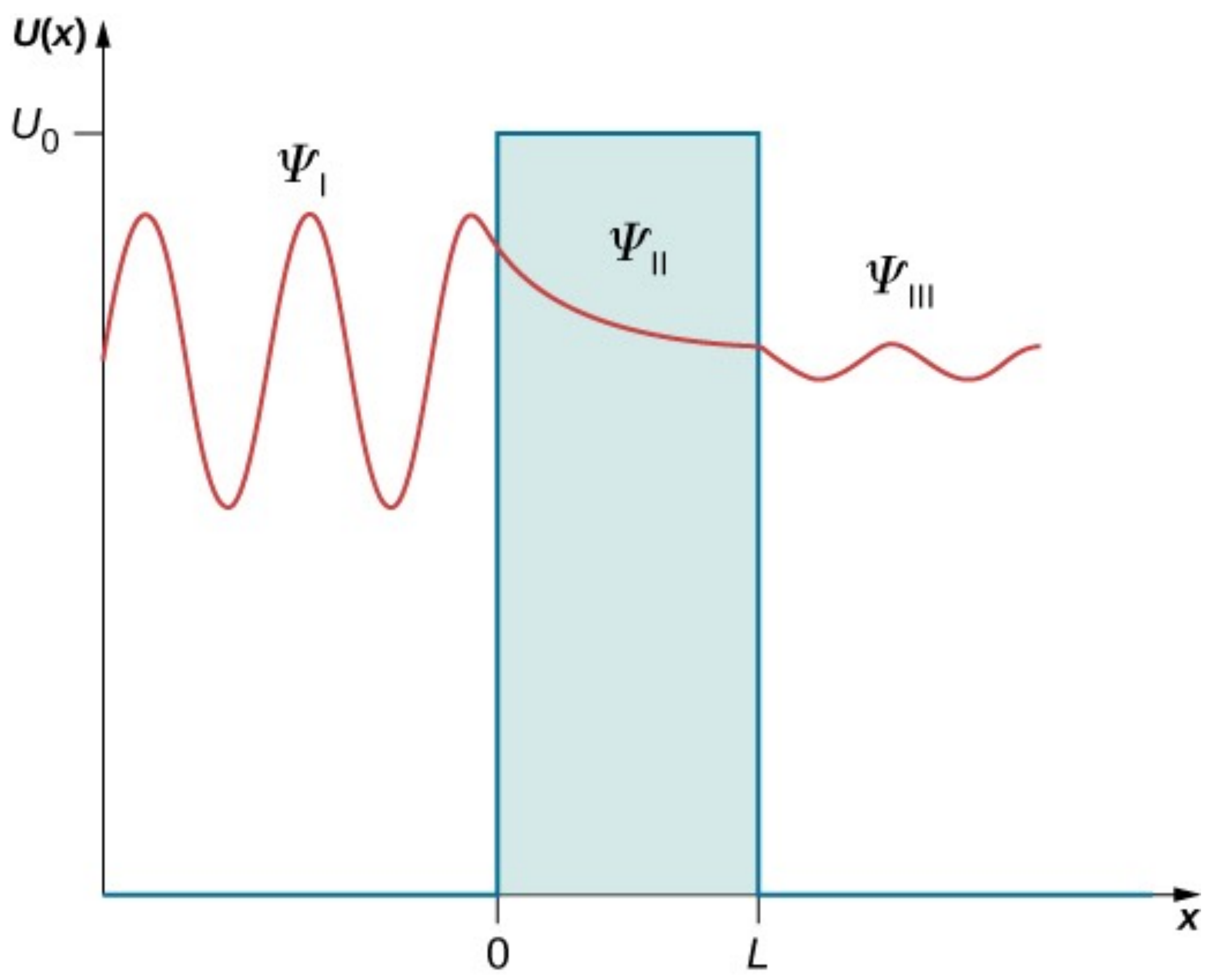

Courtesy of Ivan Rech, Politecnico di Milano
[50 µm cell size]

# A THREE STEP DANCE:

The name of the game is **QUANTUM TUNNELING:**

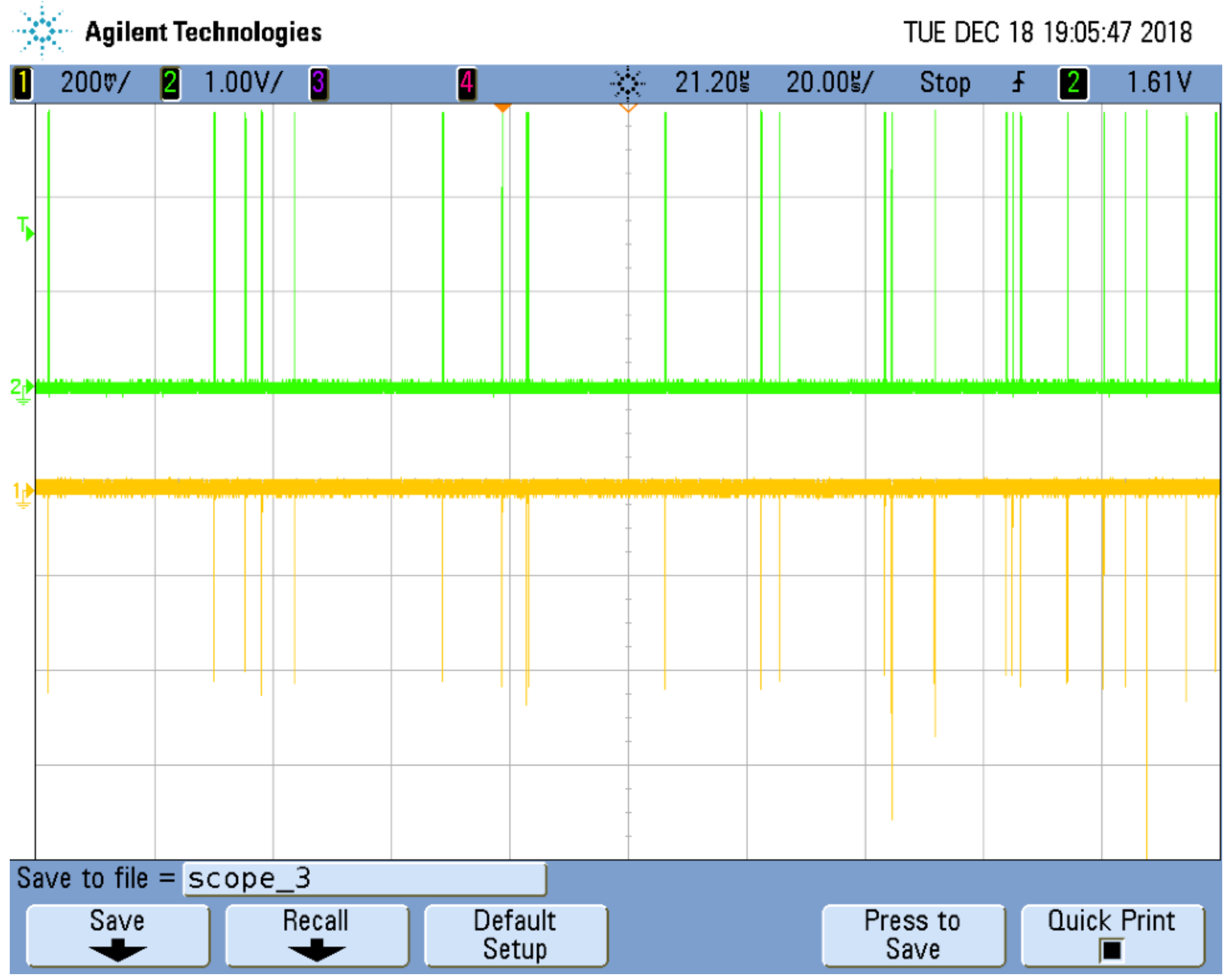
- **Electrons** and quantum entities in general are not like a  but they rather appear as a  :

when they bounce against a [potential] barrier, they can occasionally go through in an unpredictable way.




- When this is happening, the “ghost” electron enters a region of high electric field, generating a **current pulse** by impact ionisation

- By **time stamping** the pulses the analysing the time series, we turn unpredictable occurrence of the pulses into **bits**




**and we embody the principle in a platform of Silicon-based devices**

# This is the PATENTED essence of RANDOM POWER

- Italian Patent granted in Sept. 2020
- EU patent granted in 2022
- Japanese patent granted in 2024
- in the examination phase in China, Korea and U.S. (since April 2021)

Ministero dello Sviluppo Economico
Direzione generale per la tutela della proprietà industriale
Ufficio Italiano Brevetti e Marchi

**ATTESTATO DI BREVETTO PER INVENZIONE INDUSTRIALE**

Il presente brevetto viene concesso per l'invenzione oggetto della domanda:

**N. 102018000009064**

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) **EP 3 861 431 B8**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
**Corrected version no 1 (W1 B1)**
**Corrections, see**
**Bibliography INID code(s) 73**

(48) Corrigendum issued on:
**16.11.2022 Bulletin 2022/46**

(45) Date of publication and mention of the grant of the patent:
**05.10.2022 Bulletin 2022/40**

(21) Application number: **…9611.7**

(22) Date of filing: **01.10.2…**

(51) International Patent Classification (IPC):
***G06F 7/58*** (2006.01) ***H04L 9/08*** (2006.01)

(52) Cooperative Patent Classification (CPC):
**H04L 9/0852; G06F 7/588;** Y04S 40/20

(86) International application number:
**PCT/IB2019/058340**

(87) International publication number:
**WO 2020/070641 (09.04.2020 Gazette 2020/15)**

特　許　証
(CERTIFICATE OF PATENT)

特許第７５６８２９７号
(PATENT NUMBER)

| | |
|---|---|
| 発明の名称 (TITLE OF THE INVENTION) | ランダムビットシーケンスを生成するための装置及び方法 |
| 特許権者 (PATENTEE) | イタリア２０１２９ミラノ、ヴィア・マセドニオ・メローニ４０<br>国籍・地域　イタリア共和国<br>ランダム・パワー・ソチエタ・ア・レスポンサビリタ・リミタータ・イン・フォルマ・アップレヴィアータ・ラップ！・ソチエタ・ア・レス　（その他別紙記載） |
| 発明者 (INVENTOR) | マッシモ・ルイージ・マリア・カッチア |

# This is the PATENTED essence of

# RANDOM POWER

where the key issues are:

- **endogenous in-silico seeding of the pulses**
- self-amplification of the seeds in excess of a factor 1 000 000, making pulse tagging robust
- **bit extraction through a non parametric local analysis of the time series of pulses**
- no influence of temperature on the randomness of the occurrences
- **no need of post-processing to correct left-over bias**
- maximum bit/occurrence rate = 40% [2 random bits every 5 pulses]
- **current rate at the 5-10 Mbps rate for every mm$^2$ of Silicon sensor**
- potential to embed the generator into an ASIC [Application Specific Integrated Circuit]

# a few notes:

**a. Our principle is actually a lesson from the past. This effect was known since the early days of the Silicon technology development:**

PHYSICAL REVIEW VOLUME 94, NUMBER 4 MAY 15, 1954

1

### Avalanche Breakdown in Silicon

K. G. McKay
*Bell Telephone Laboratories, Murray Hill, New Jersey*
(Received December 23, 1953)

JOURNAL OF APPLIED PHYSICS VOLUME 35, NUMBER 5 MAY 1964

2

### Model for the Electrical Behavior of a Microplasma*

Roland H. Haitz†
*Shockley Laboratory, Clevite Corporation Semiconductor Division, Palo Alto, California*
(Received 5 November 1963)

The complex current fluctuations observed in connection with microplasma breakdown can be explained by a simple model containing two constants: extrapolated breakdown voltage $V_b$ and series resistance $R_s$; and two continuous probability functions: turnoff probability per unit time $p_{10}(I)$ as a function of pulse current $I$ and turn-on probability per unit time $p_{01}$. Experimental methods allowing an accurate measurement of these four quantities are described. The new concept of an extrapolated breakdown voltage $V_b$ is discussed based on two independent measurements: one of secondary multiplication and the other of instantaneous current, both as a function of voltage. Within the experimental accuracy of 20 mV both methods extrapolated to one and the same breakdown voltage. The turnoff probability $p_{10}(I)$ is determined by a new combination of experimental techniques to cover the current range from 5 to 70 $\mu$A with a variation of 11 decades for $p_{10}(I)$. The observation of a narrow turnoff interval is explained quantitatively.

F APPLIED PHYSICS VOLUME 36, NUMBER 10 OCTOBER 1965

3

### Mechanisms Contributing to the Noise Pulse Rate of Avalanche Diodes*

Roland H. Haitz†
*Shockley Research Laboratory, Semiconductor Division of Clevite Corporation,‡ Palo Alto, California*
(Received 16 November 1964)

**1. INTRODUCTION**

MOST reverse biased $p$–$n$ junctions in silicon have their avalanche breakdown caused by microplasma effects. Microplasmas are small regions within the junction,[1] where a local disturbance of the electrical field is believed to reduce the breakdown voltage to a value below the breakdown voltage of the surrounding uniform junction.[2–5] As voltage is increased from low values microplasma breakdown is generally characterized by random "on–off" current fluctuations so long as currents remain below a critical value (40 to 120 $\mu$A).[6–8]

from paper 2

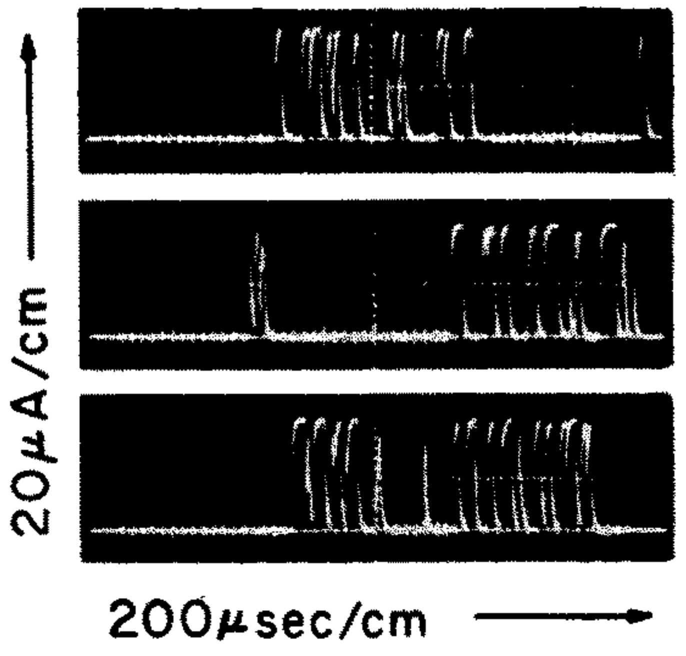



Fig. 5. Avalanche current as a function of time at low temperatures. The group character of the avalanche pulses is obvious.

from paper 3

**The phenomenology is by now quite well known** [even if large uncertainties are still there, requiring somehow a "cook & look" approach]

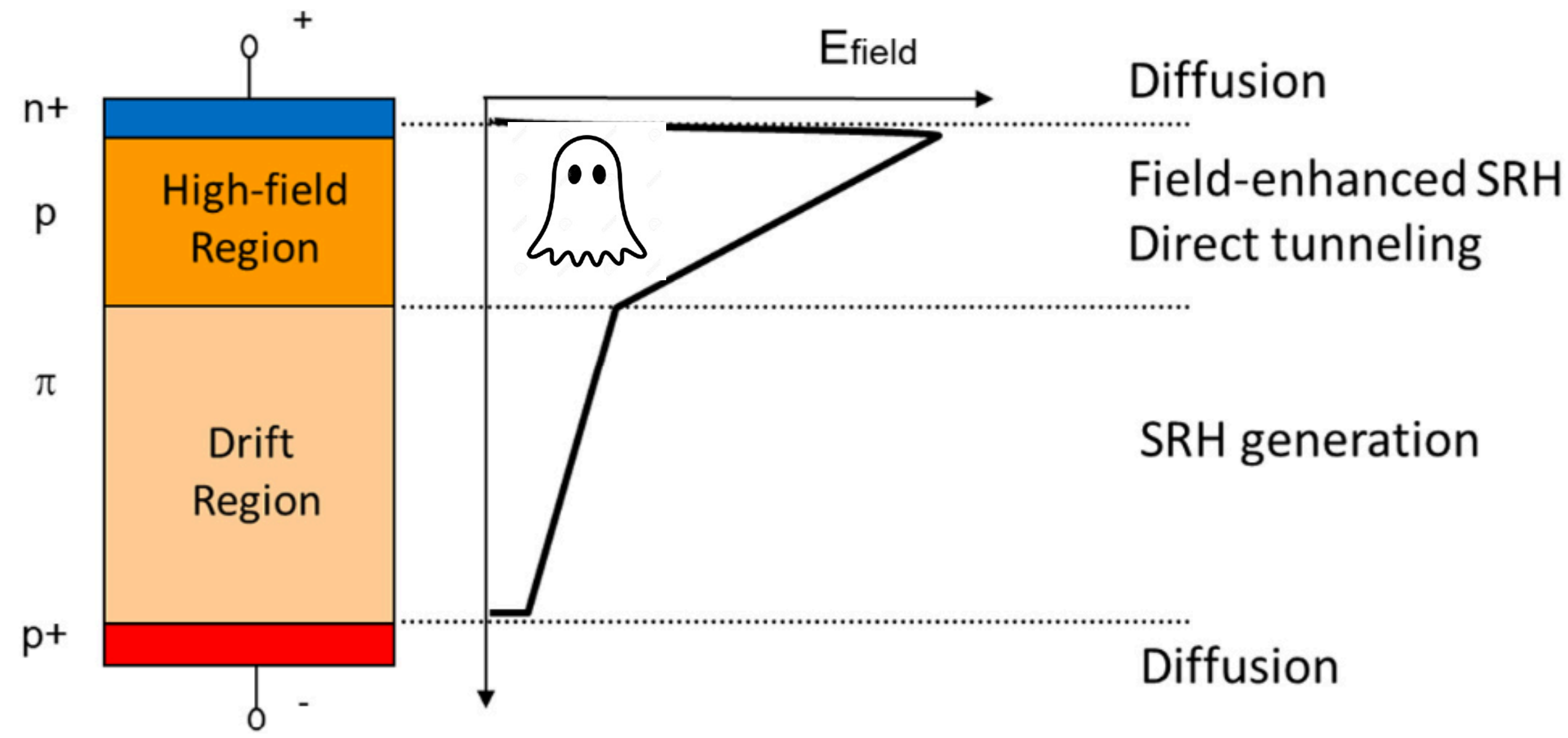



**Fig. 8.** Representation of the different sources of primary dark events and their location in the SPAD structure.

after A. Gola, C. Piemonte, NIM A926 (2019) 2-15

**Key issues:**

- ✳ **the Pulse Rate is O(1 KHz)/cell, 50 μm pitch (it may be higher for SPAD arrays in CMOS technology)**
- ✳ provided the nature of the "Dark Pulses", we have a significant dependence on Temperature
- ✳ forget-me-not: the Over-voltage is affecting the triggering probability

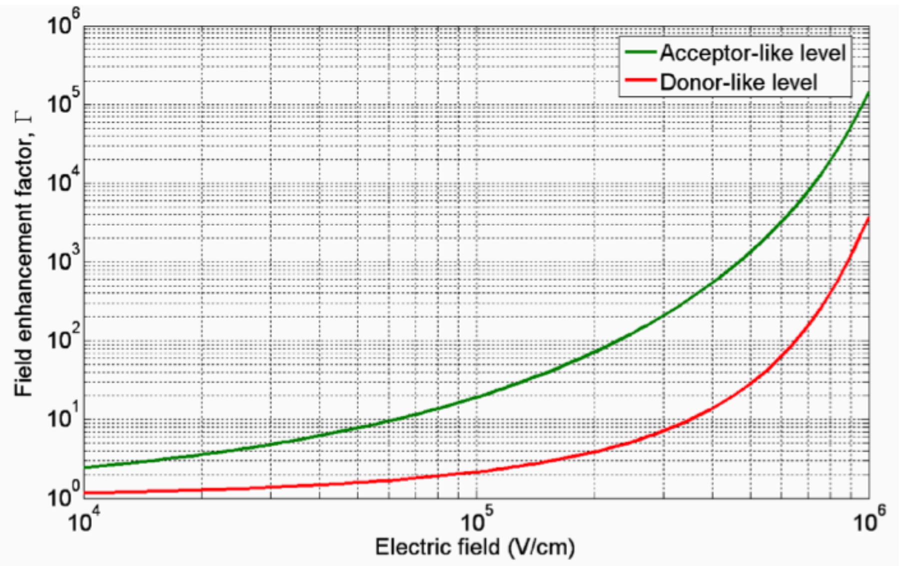
**Thermal generation of carriers by states in the bang-gap** (Shockley-Read-Hall statistics), where trapping and de-trapping is increased by the high electric field in the junction. The **Generation rate** can be written as:

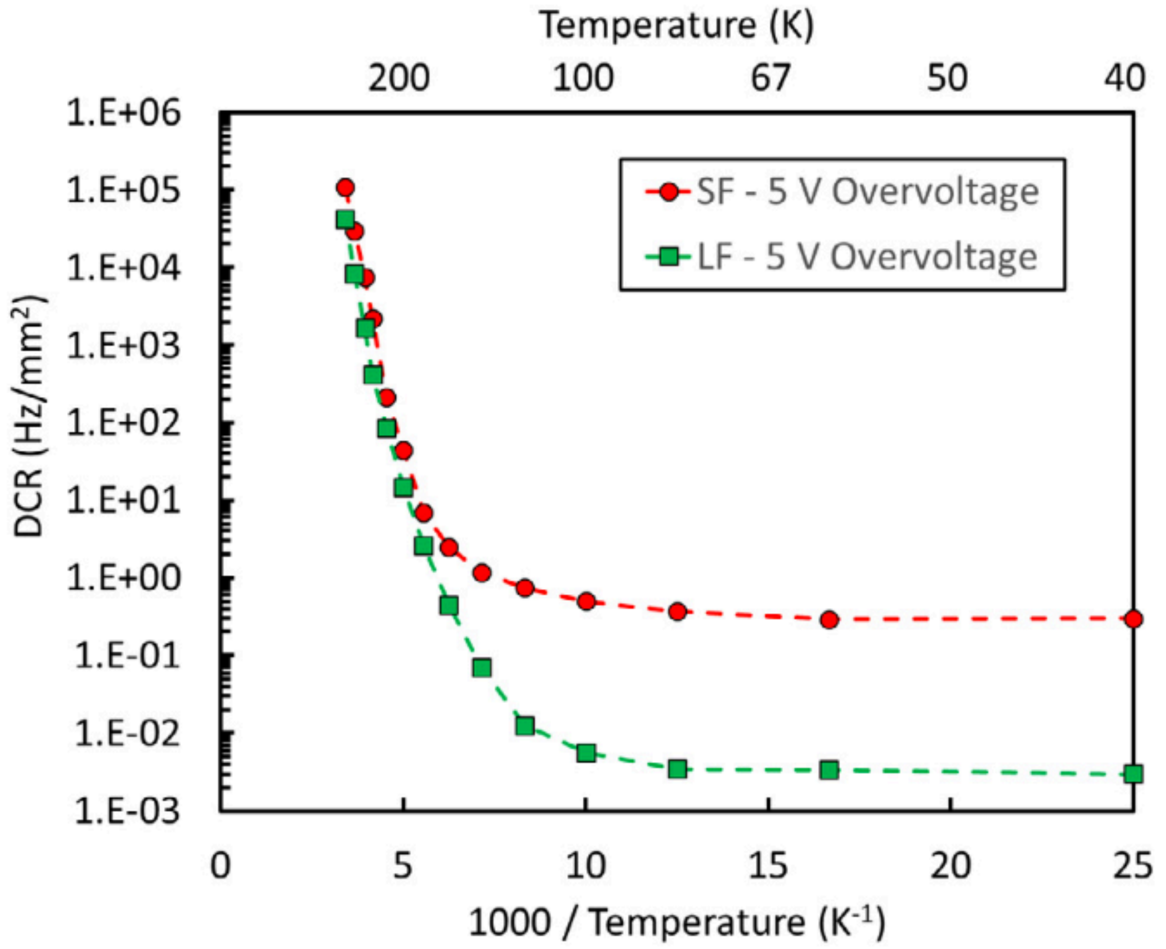
$$G = \frac{n_i}{2 \cdot \cosh\left(\frac{E_0 - E_t}{kT}\right)} N_t \sigma v_{th} = \frac{n_i}{\tau_{g0}}$$

$E_0$ = Fermi level
$E_t$ = trapping level
$n_i$ = intrinsic carrier concentration
$N_t$ = trapping concentration
$\sigma$ = trapping cross section
$v_{th}$ = thermal velocity

$$G = \frac{(1+\Gamma)\, n_i}{\tau_{g0}}$$

$\Gamma$ "boost" by the field

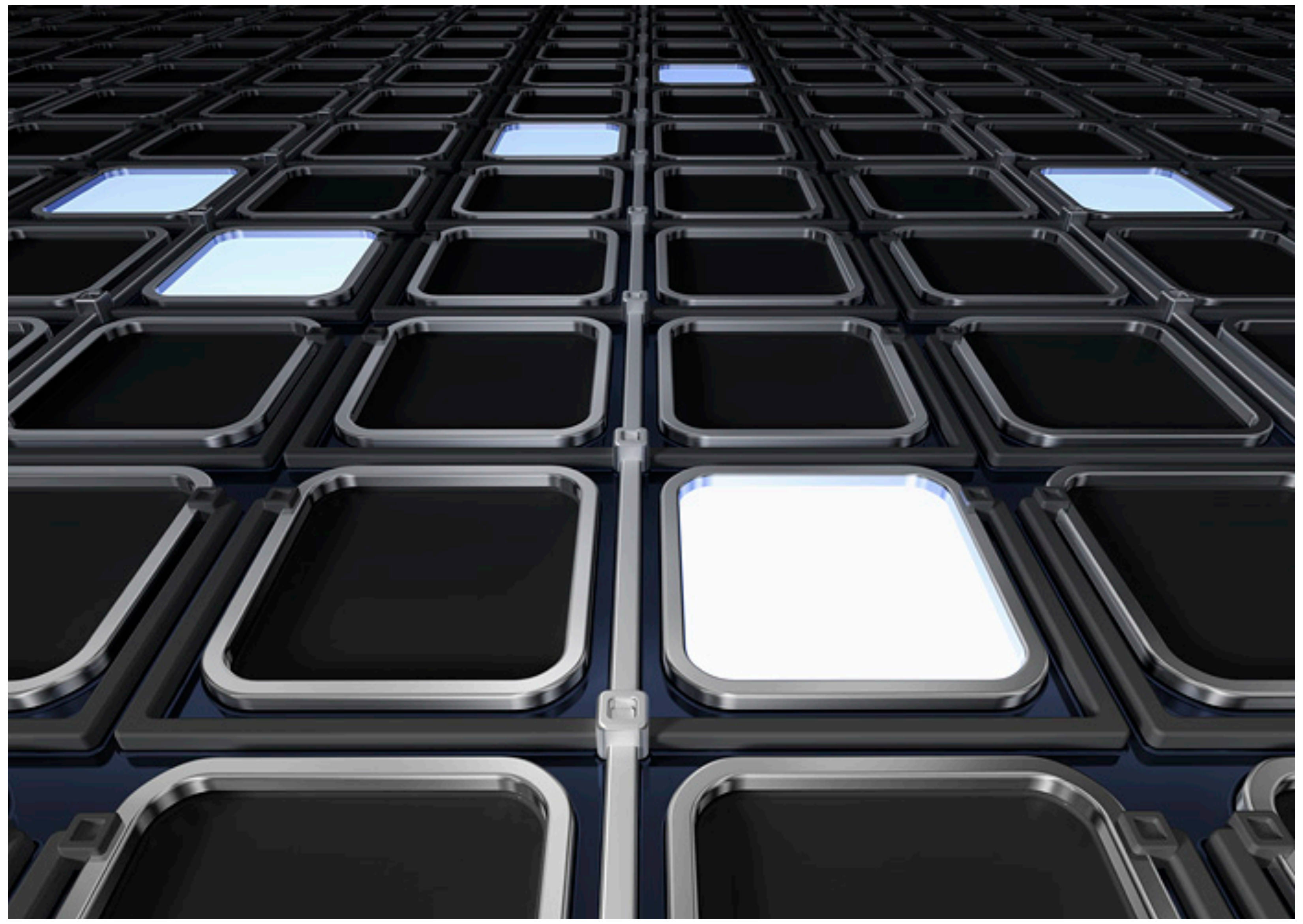



F. Acerbi, et al., IEEE Trans. Electron Devices 64 (2) (2017) 521-526.

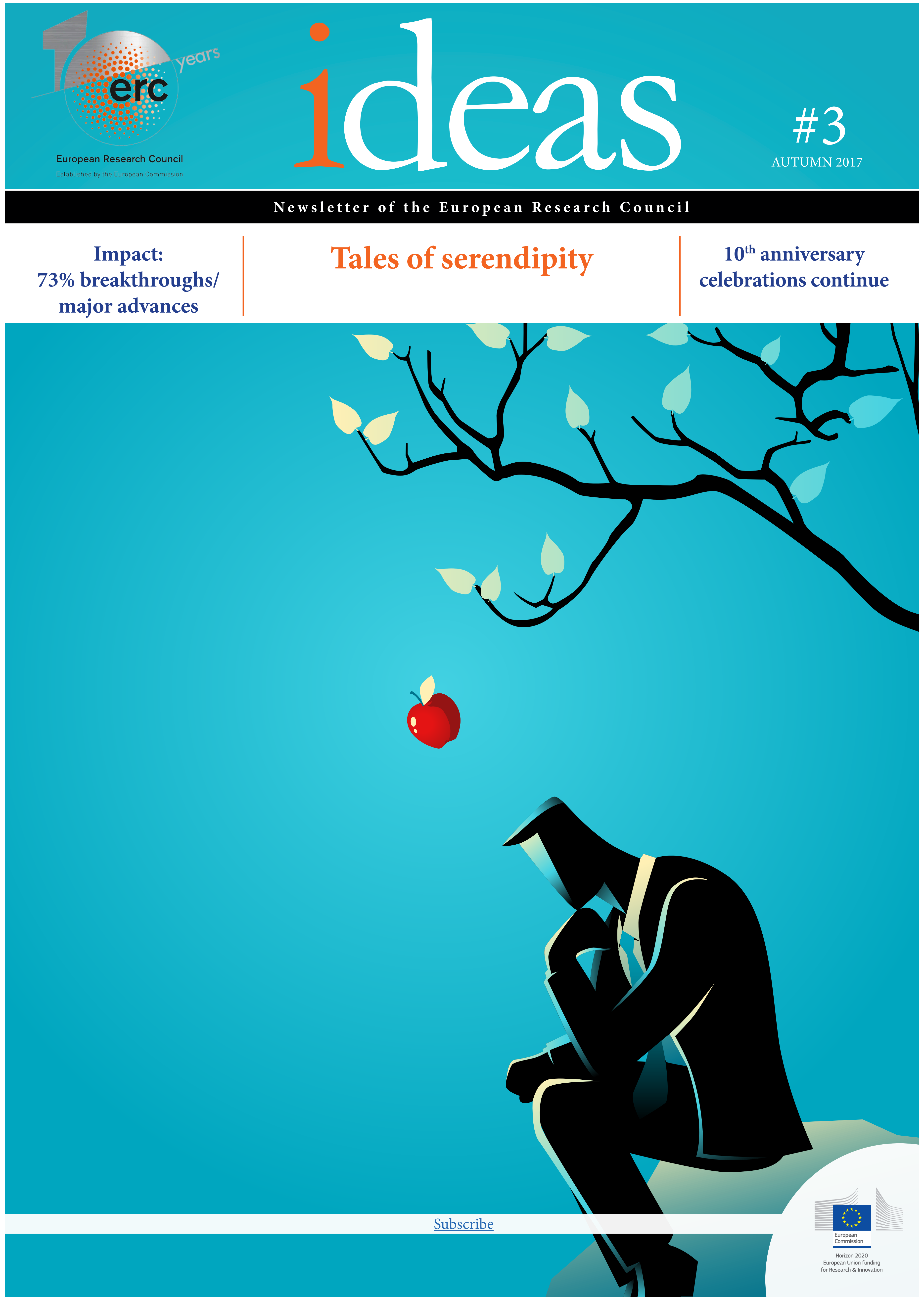
# ▷ a few notes:

**b. The idea flashed as a genuine act of serendipity, while studying the properties of Dark Counts in Silicon Photomultipliers (SiPM)**



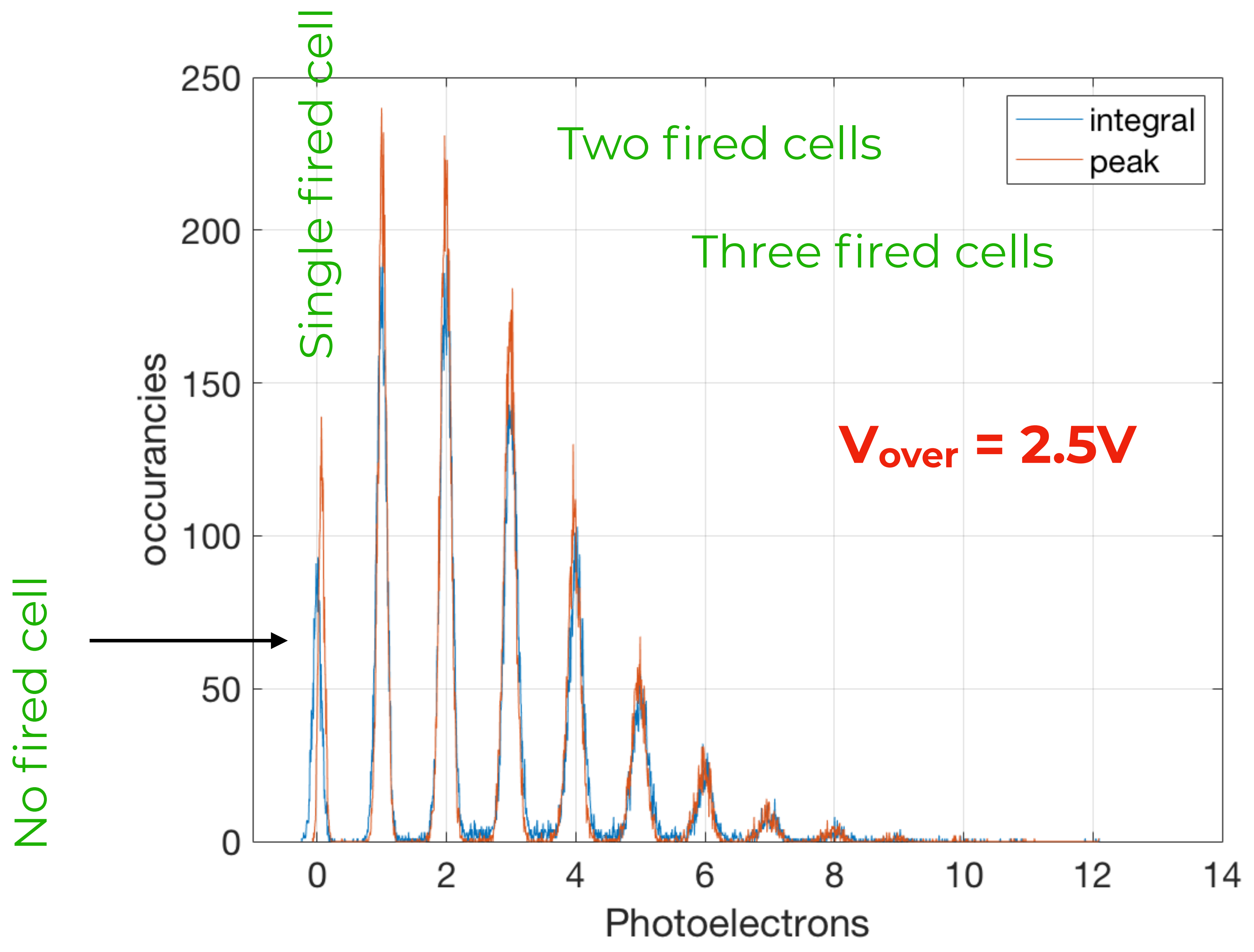
- SiPM may be seen as a collection of binary cells, p-n junctions operated beyond the breakdown voltage [SPAD], fired when a photon in absorbed

**[in principle, a NATIVE DIGITAL DEVICE]**

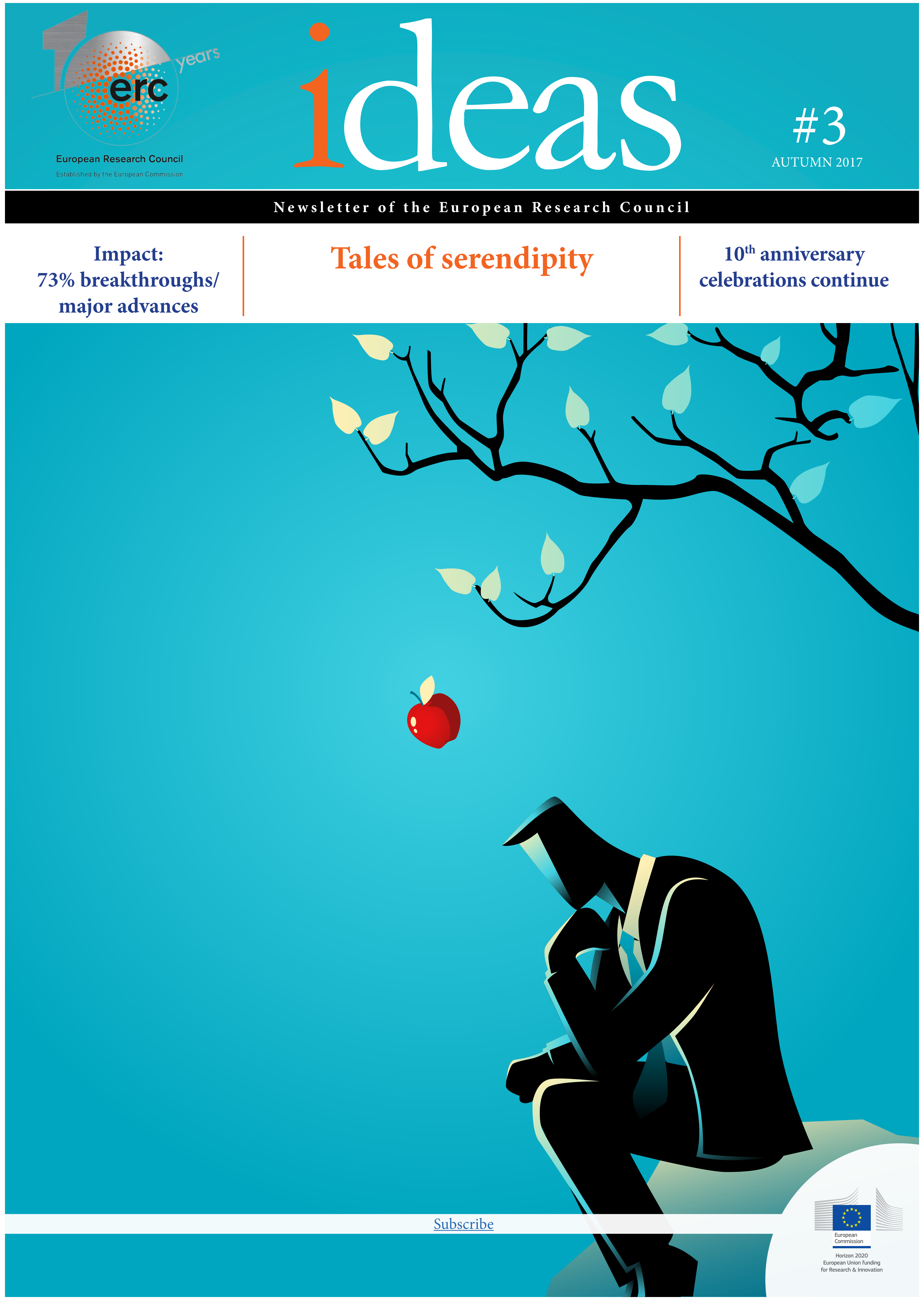


# a few notes:

**b. The idea flashed as a genuine act of serendipity, while studying the properties of Dark Counts in Silicon Photomultipliers (SiPM)**

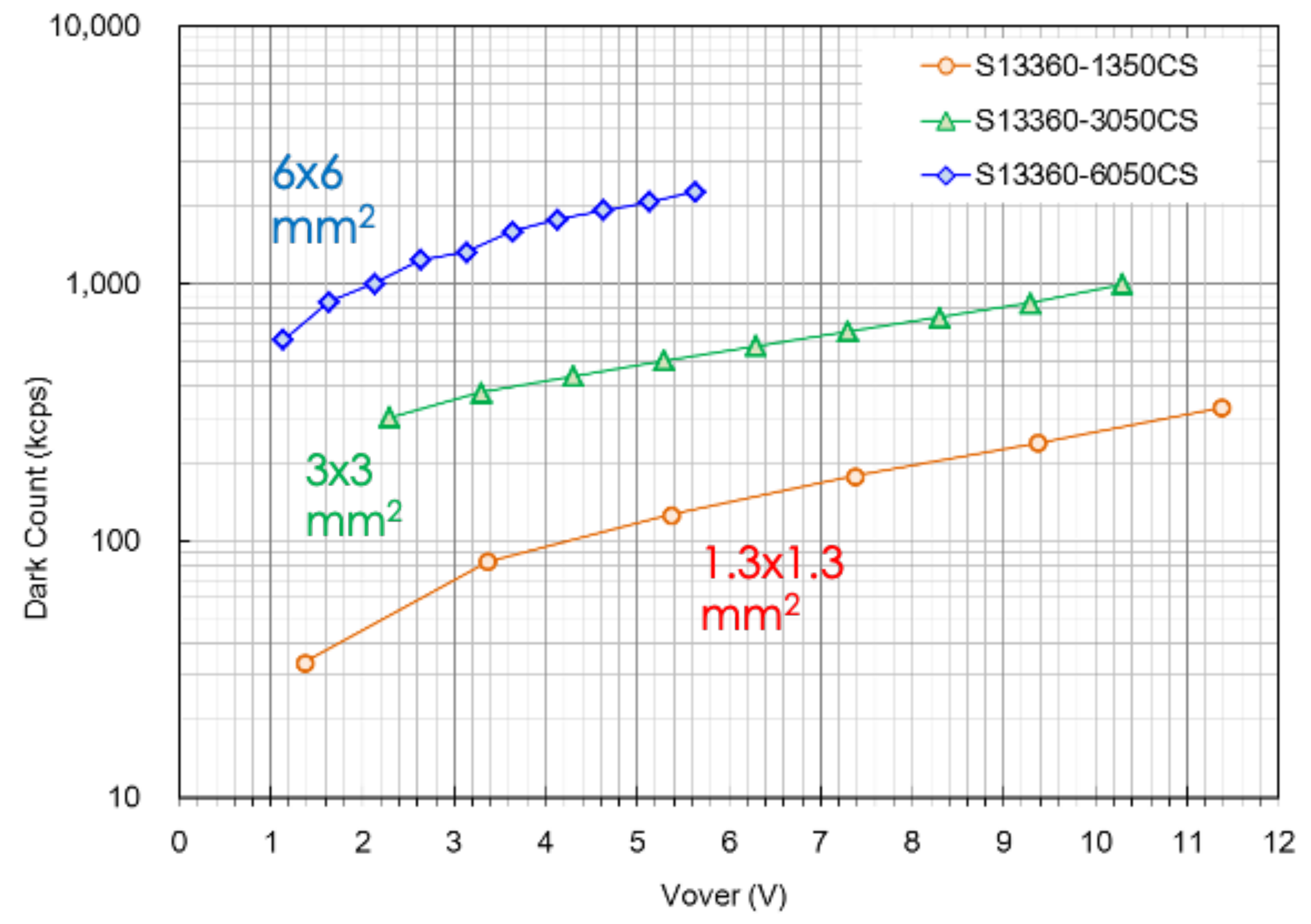



- histogram of the response to a high statistics of low intensity light pulses

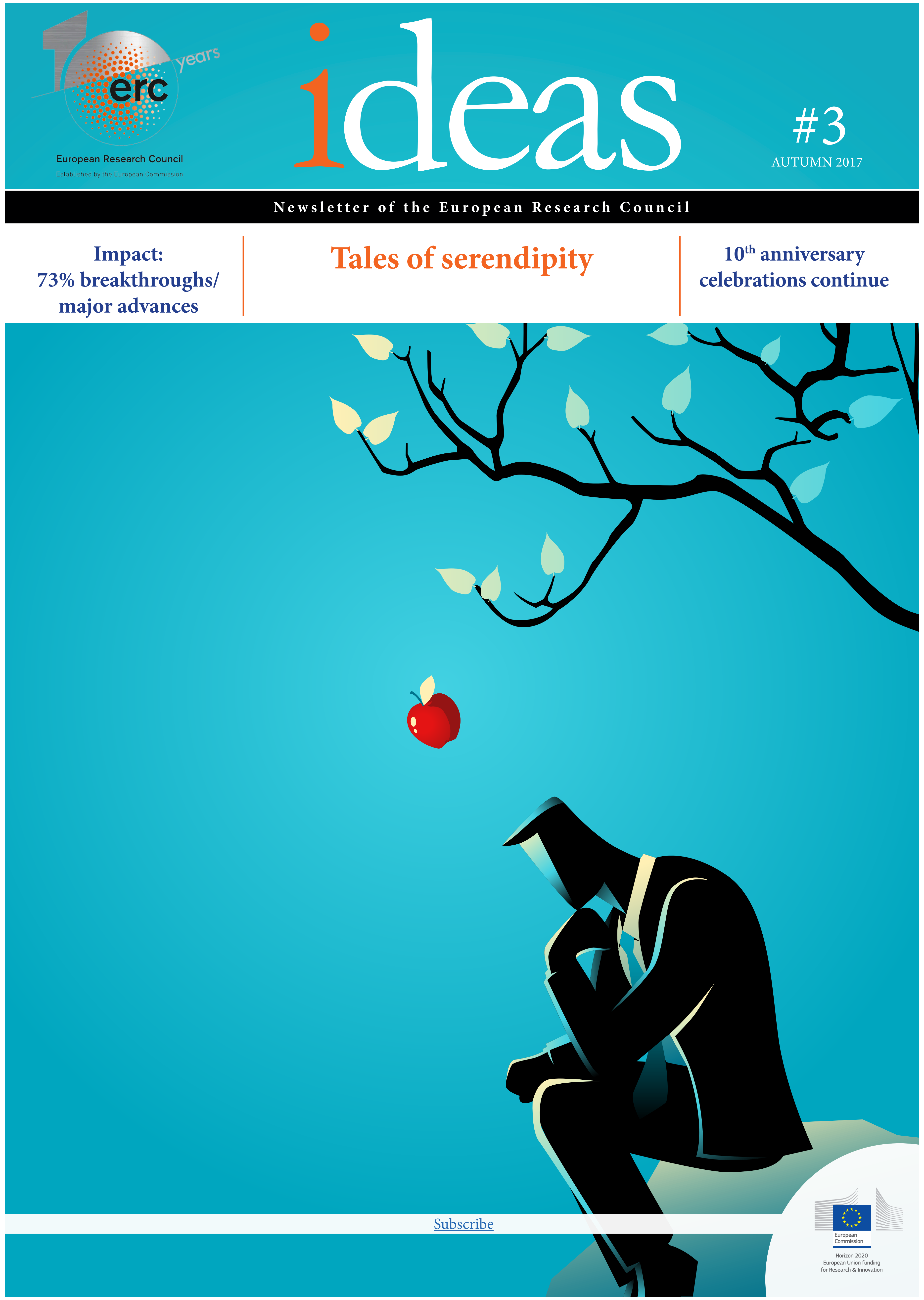


# a few notes:

**b. The idea flashed as a genuine act of serendipity, while studying the properties of Dark Counts in Silicon Photomultipliers (SiPM)**




Dependence of the Dark Count Rate on the Overvoltage (wrt Breakdown) in different HAMAMATSU SiPM



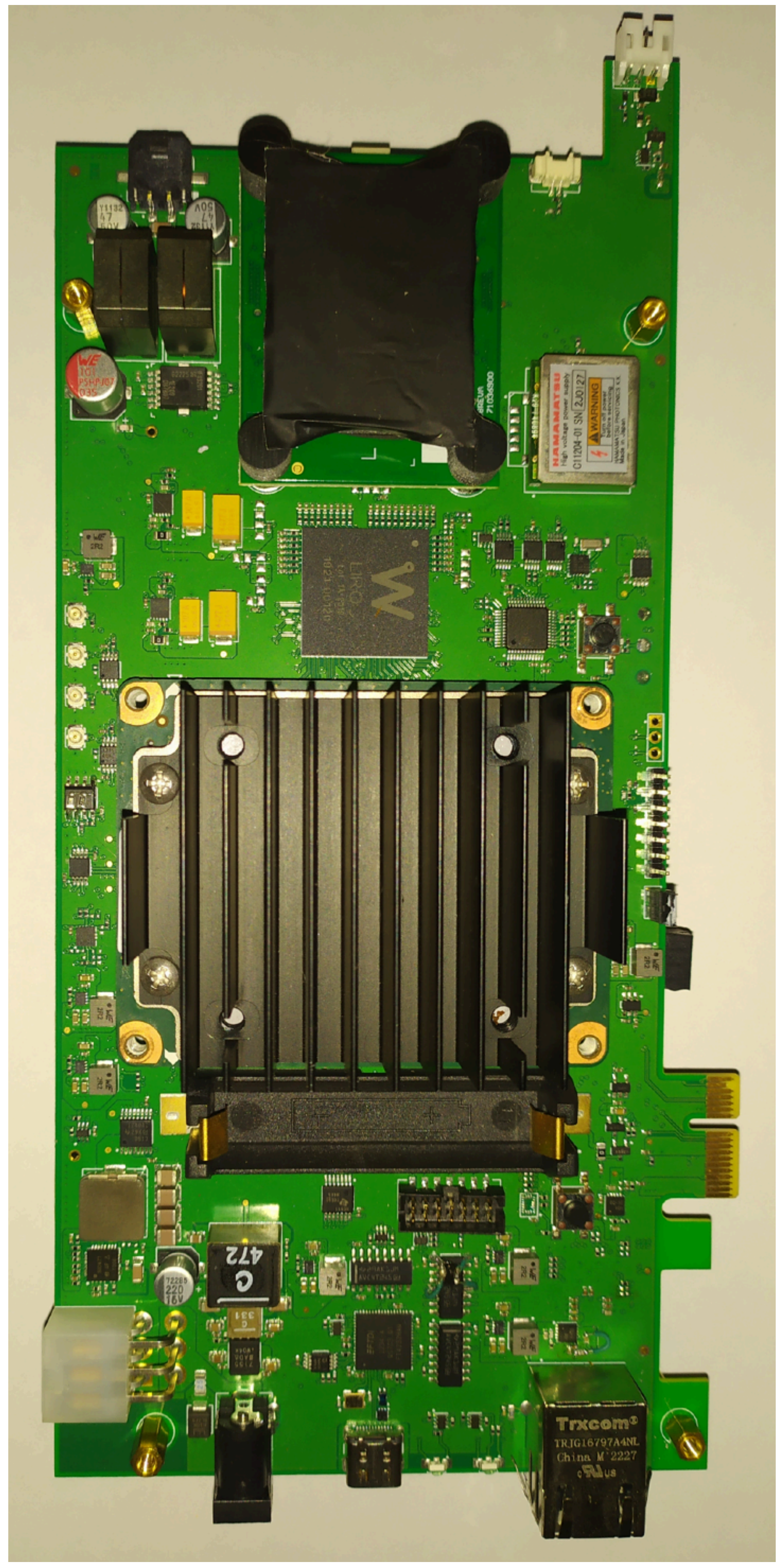
## Three elements of the platform have been developed and will be **ready for the market by Q1 2025:**

8 cm


3.5 cm

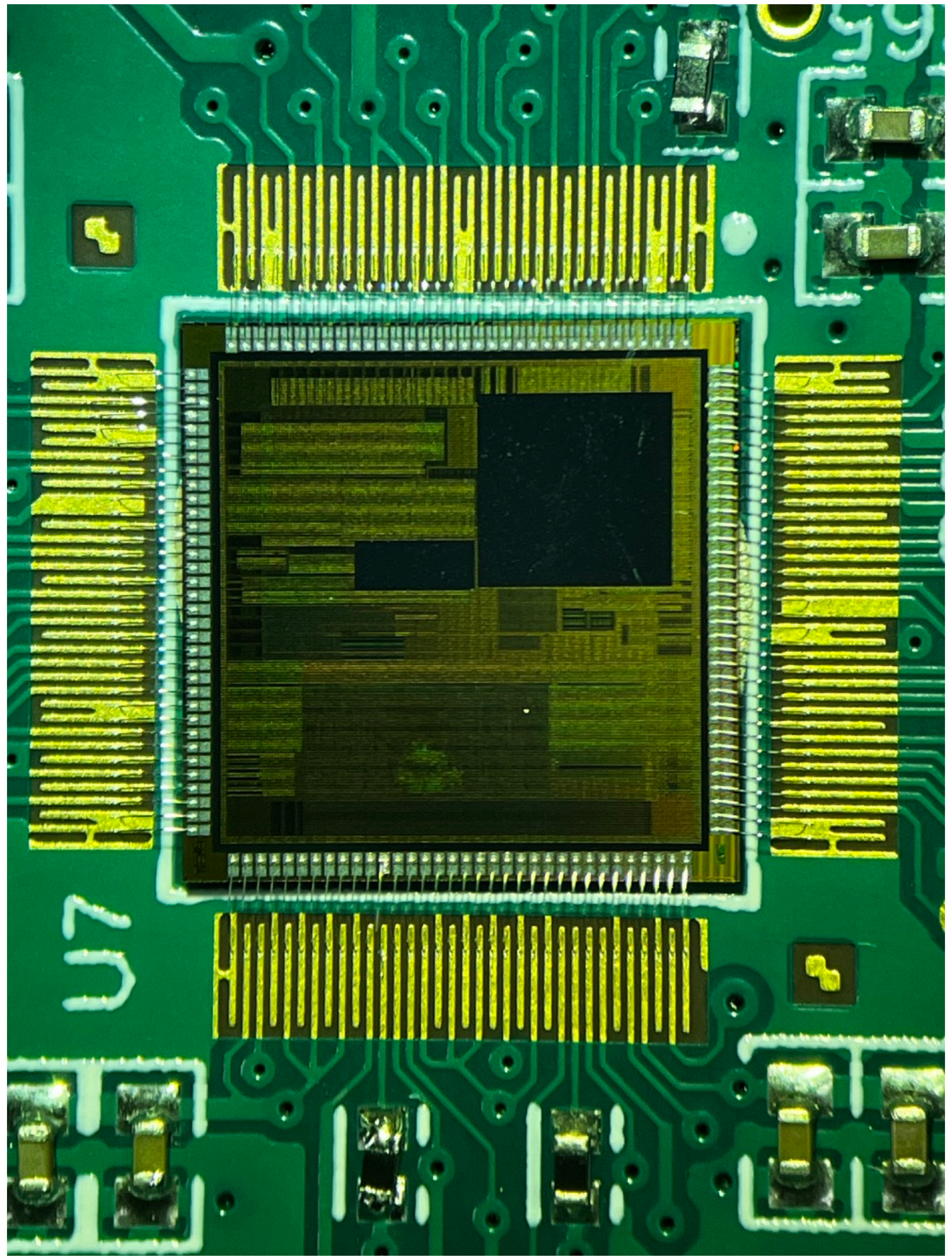
A **single generator board**, for **qualification and the educational market**

31 cm



11 cm

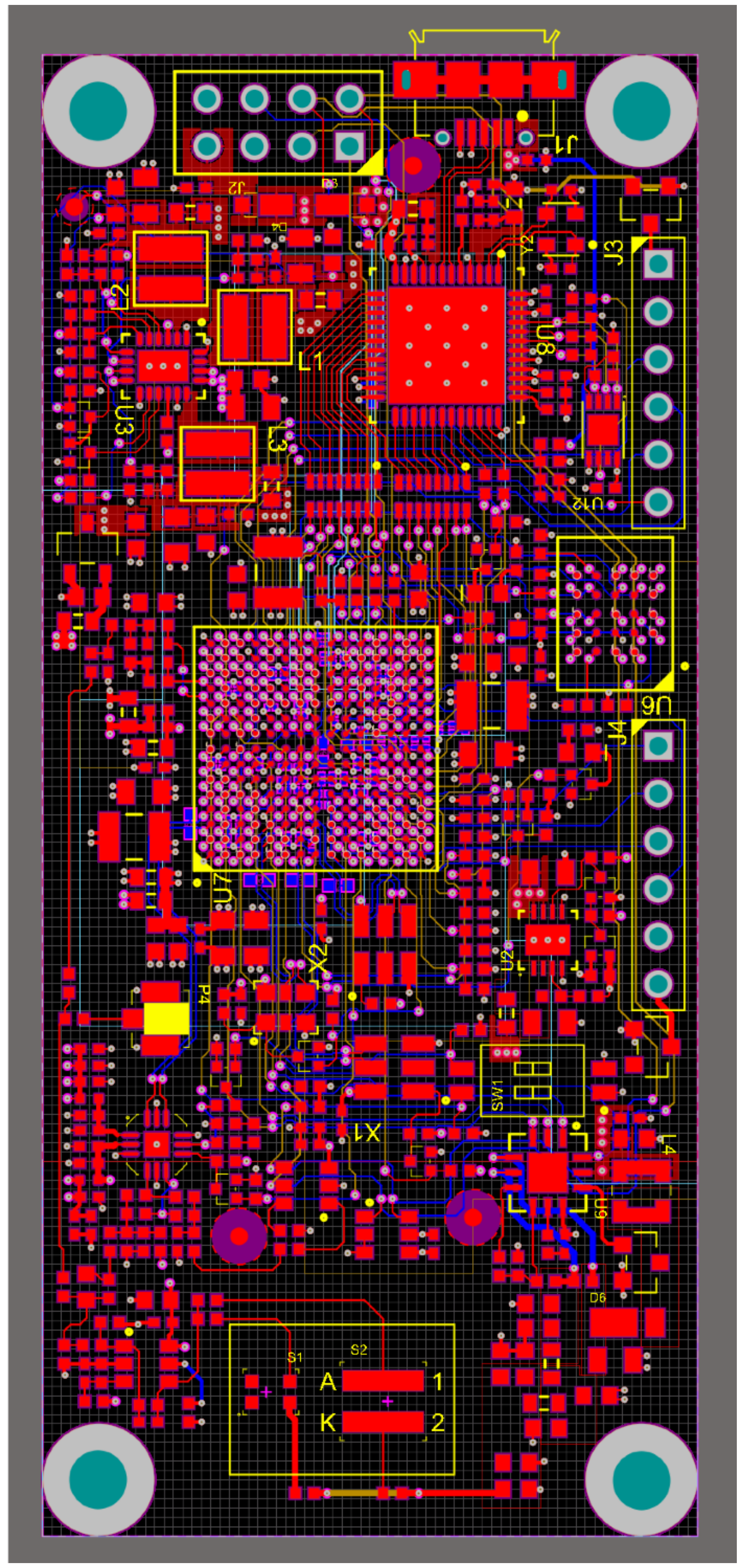
A **64 generator computer on a board,** for **Data Centers** (e.g. simulations & AI training)



A **full custom ASIC (a chip!)** for IoT, Authentication, gaming&gambling

RANDOM POWER

# THE SINGLE GENERATOR BOARD



8 cm


3.5 cm

| | |
|---|---|
| **Dimensions [cm²]** | 8x3.5 |
| **No. generators** | 1 array |
| **Raw bit stream:** | 100 kbps |
| **NIST DRBG output (SP800-90 A,B,C)** | NA |
| **Control:** | Xilinx Spartan 7 |
| **I/O:** | USB or bits-on-pin |
| **Power supply:** | through the USB (5V, 0.5A) |
| **Power consumption:** | <2.5W |
| **Encryption of the bit stream:** | No |
| **Specific Features:** | • Firmware implemented Real-Time sanity checks (MONOBIT and RUNS)<br>• Auxiliary post-processing through a SHA256 function |
| **State of development:** | • Completed<br>• Full qualification of 2 Tb through the NIST and TESTU01 protocols<br>• Single board control through a GUI or mini-farm control implementing also the NIST DRBG procedure (SP800-90 A,B,C) |

Main output of the ATTRACT Phase 1 project (May 2019-Oct.2020)

RANDOM POWER

finalAnalysisReport_PART2.txt

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is </Users/luca/Documents/Random_Power/ProgramAndTechnical/ATTRACT_Eu_Board_Fw8/TestFW8_4BitNoReshape_1GB_Part2.bin>

| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | P-VALUE | PROPORTION | STATISTICAL TEST |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 100 | 110 | 95 | 93 | 90 | 90 | 114 | 101 | 98 | 109 | 0.682823 | 986/1000 | Frequency |
| 97 | 102 | 94 | 103 | 107 | 97 | 105 | 106 | 102 | 87 | 0.941144 | 993/1000 | BlockFrequency |
| 95 | 95 | 101 | 100 | 113 | 106 | 93 | 100 | 89 | 108 | 0.842937 | 989/1000 | CumulativeSums |
| 94 | 112 | 117 | 90 | 93 | 91 | 89 | 96 | 123 | 95 | 0.125927 | 987/1000 | CumulativeSums |
| 100 | 93 | 91 | 112 | 93 | 112 | 99 | 110 | 101 | 89 | 0.647530 | 992/1000 | Runs |
| 105 | 91 | 96 | 80 | 121 | 99 | 85 | 100 | 107 | 116 | 0.092597 | 989/1000 | LongestRun |
| 100 | 104 | 89 | 110 | 97 | 88 | 126 | 84 | 99 | 103 | 0.148653 | 992/1000 | Rank |
| 95 | 109 | 103 | 113 | 85 | 94 | 90 | 100 | 106 | 105 | 0.630872 | 995/1000 | FFT |
| 104 | 98 | 91 | 89 | 104 | 90 | 110 | 104 | 115 | 95 | 0.632955 | 987/1000 | NonOverlappingTemplate |
| 111 | 93 | 112 | 88 | 96 | 95 | 100 | 101 | 106 | 98 | 0.798139 | 981/1000 | NonOverlappingTemplate |
| 111 | 100 | 93 | 94 | 101 | 109 | 93 | 87 | 117 | 95 | 0.514124 | 986/1000 | NonOverlappingTemplate |
| 86 | 94 | 119 | 101 | 107 | 98 | 93 | 103 | 98 | 101 | 0.626709 | 998/1000 | NonOverlappingTemplate |
| 93 | 112 | 93 | 103 | 91 | 89 | 94 | 99 | 115 | 111 | 0.498313 | 989/1000 | NonOverlappingTemplate |
| 84 | 106 | 101 | 109 | 86 | 119 | 111 | 96 | 94 | 94 | 0.249284 | 988/1000 | NonOverlappingTemplate |
| 114 | 92 | 98 | 96 | 105 | 105 | 101 | 100 | 83 | 106 | 0.682823 | 992/1000 | NonOverlappingTemplate |
| 117 | 87 | 98 | 101 | 100 | 106 | 91 | 94 | 105 | 101 | 0.697257 | 991/1000 | NonOverlappingTemplate |
| 90 | 93 | 97 | 107 | 99 | 89 | 100 | 116 | 108 | 101 | 0.689019 | 994/1000 | NonOverlappingTemplate |
| 99 | 108 | 98 | 99 | 116 | 104 | 98 | 85 | 96 | 97 | 0.743915 | 991/1000 | NonOverlappingTemplate |
| 88 | 93 | 103 | 101 | 112 | 94 | 111 | 99 | 100 | 99 | 0.829047 | 988/1000 | NonOverlappingTemplate |
| 96 | 97 | 103 | 103 | 106 | 108 | 114 | 97 | 93 | 83 | 0.651693 | 987/1000 | NonOverlappingTemplate |
| 108 | 95 | 97 | 109 | 84 | 94 | 101 | 101 | 91 | 120 | 0.388990 | 988/1000 | NonOverlappingTemplate |

series of tests on non-overlapping templates

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 80 | 98 | 115 | 100 | 98 | 115 | 107 | 91 | 83 | 113 | 0.106877 | 993/1000 | OverlappingTemplate |
| 86 | 116 | 121 | 101 | 91 | 87 | 96 | 101 | 87 | 114 | 0.084037 | 990/1000 | Universal |
| 97 | 90 | 107 | 116 | 110 | 95 | 103 | 93 | 92 | 97 | 0.668321 | 987/1000 | ApproximateEntropy |
| 70 | 62 | 54 | 60 | 55 | 66 | 60 | 63 | 77 | 65 | 0.668486 | 626/632 | RandomExcursions |
| 62 | 69 | 58 | 70 | 58 | 61 | 56 | 71 | 63 | 64 | 0.909311 | 626/632 | RandomExcursions |
| 60 | 53 | 59 | 62 | 76 | 72 | 60 | 59 | 66 | 65 | 0.681642 | 620/632 | RandomExcursions |
| 70 | 64 | 83 | 45 | 62 | 69 | 70 | 65 | 51 | 53 | 0.040275 | 622/632 | RandomExcursions |
| 66 | 69 | 69 | 73 | 73 | 73 | 38 | 49 | 52 | 70 | 0.009611 | 627/632 | RandomExcursions |
| 65 | 52 | 67 | 82 | 68 | 54 | 51 | 63 | 72 | 58 | 0.136536 | 627/632 | RandomExcursions |
| 61 | 55 | 60 | 72 | 66 | 71 | 67 | 56 | 55 | 69 | 0.711017 | 626/632 | RandomExcursions |
| 47 | 61 | 62 | 58 | 71 | 63 | 71 | 61 | 68 | 70 | 0.553450 | 625/632 | RandomExcursions |
| 60 | 57 | 66 | 62 | 58 | 61 | 67 | 67 | 73 | 61 | 0.941564 | 624/632 | RandomExcursionsVariant |
| 60 | 70 | 43 | 60 | 64 | 58 | 58 | 88 | 64 | 67 | 0.030676 | 622/632 | RandomExcursionsVariant |
| 66 | 58 | 51 | 65 | 51 | 61 | 72 | 72 | 71 | 65 | 0.447593 | 624/632 | RandomExcursionsVariant |
| 63 | 67 | 59 | 46 | 67 | 60 | 68 | 70 | 73 | 59 | 0.483876 | 623/632 | RandomExcursionsVariant |
| 61 | 67 | 58 | 69 | 63 | 74 | 48 | 60 | 66 | 66 | 0.615645 | 624/632 | RandomExcursionsVariant |
| 75 | 62 | 63 | 58 | 63 | 55 | 66 | 54 | 71 | 65 | 0.717488 | 624/632 | RandomExcursionsVariant |
| 68 | 63 | 66 | 54 | 57 | 65 | 63 | 67 | 56 | 73 | 0.827336 | 620/632 | RandomExcursionsVariant |
| 75 | 54 | 64 | 57 | 65 | 64 | 56 | 62 | 64 | 71 | 0.733547 | 623/632 | RandomExcursionsVariant |
| 76 | 68 | 70 | 56 | 55 | 50 | 66 | 52 | 64 | 75 | 0.176734 | 624/632 | RandomExcursionsVariant |
| 89 | 63 | 57 | 59 | 59 | 55 | 58 | 68 | 63 | 61 | 0.134074 | 624/632 | RandomExcursionsVariant |
| 67 | 68 | 61 | 57 | 60 | 69 | 66 | 63 | 63 | 58 | 0.979797 | 624/632 | RandomExcursionsVariant |
| 65 | 64 | 62 | 71 | 58 | 68 | 67 | 53 | 60 | 64 | 0.917568 | 626/632 | RandomExcursionsVariant |
| 71 | 58 | 56 | 62 | 75 | 62 | 67 | 64 | 53 | 64 | 0.701268 | 626/632 | RandomExcursionsVariant |
| 64 | 71 | 49 | 62 | 61 | 69 | 69 | 59 | 59 | 69 | 0.694743 | 626/632 | RandomExcursionsVariant |
| 61 | 65 | 54 | 59 | 63 | 63 | 64 | 76 | 62 | 65 | 0.879806 | 626/632 | RandomExcursionsVariant |
| 58 | 55 | 57 | 67 | 65 | 66 | 54 | 66 | 76 | 68 | 0.642077 | 629/632 | RandomExcursionsVariant |
| 46 | 64 | 65 | 61 | 64 | 61 | 81 | 59 | 75 | 56 | 0.150772 | 624/632 | RandomExcursionsVariant |
| 50 | 56 | 65 | 67 | 74 | 67 | 51 | 63 | 73 | 66 | 0.353061 | 629/632 | RandomExcursionsVariant |
| 106 | 107 | 87 | 107 | 94 | 109 | 100 | 83 | 92 | 115 | 0.352107 | 989/1000 | Serial |
| 105 | 100 | 94 | 98 | 96 | 95 | 96 | 101 | 95 | 120 | 0.790621 | 991/1000 | Serial |
| 105 | 97 | 89 | 101 | 96 | 106 | 92 | 112 | 105 | 97 | 0.875539 | 991/1000 | LinearComplexity |

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 980 for a sample size = 1000 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately = 618 for a sample size = 632 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

- **A proto-randomness farm based on 10 boards have been collecting about 1.5 Tb, qualified through the NIST and TESTU01 suites.**

**Results show that the stream looks extremely "white", essentially with no failures on the raw data beside what can be statistically expected.**

- **A SHA256 vetted conditioning function firmware implemented**
- **Two tests have been implemented in firmware to guarantee real-time sanity checks:**

✳ **MONOBIT: essentially testing the asymmetries between 0's and 1's in a bit string:**

1 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1

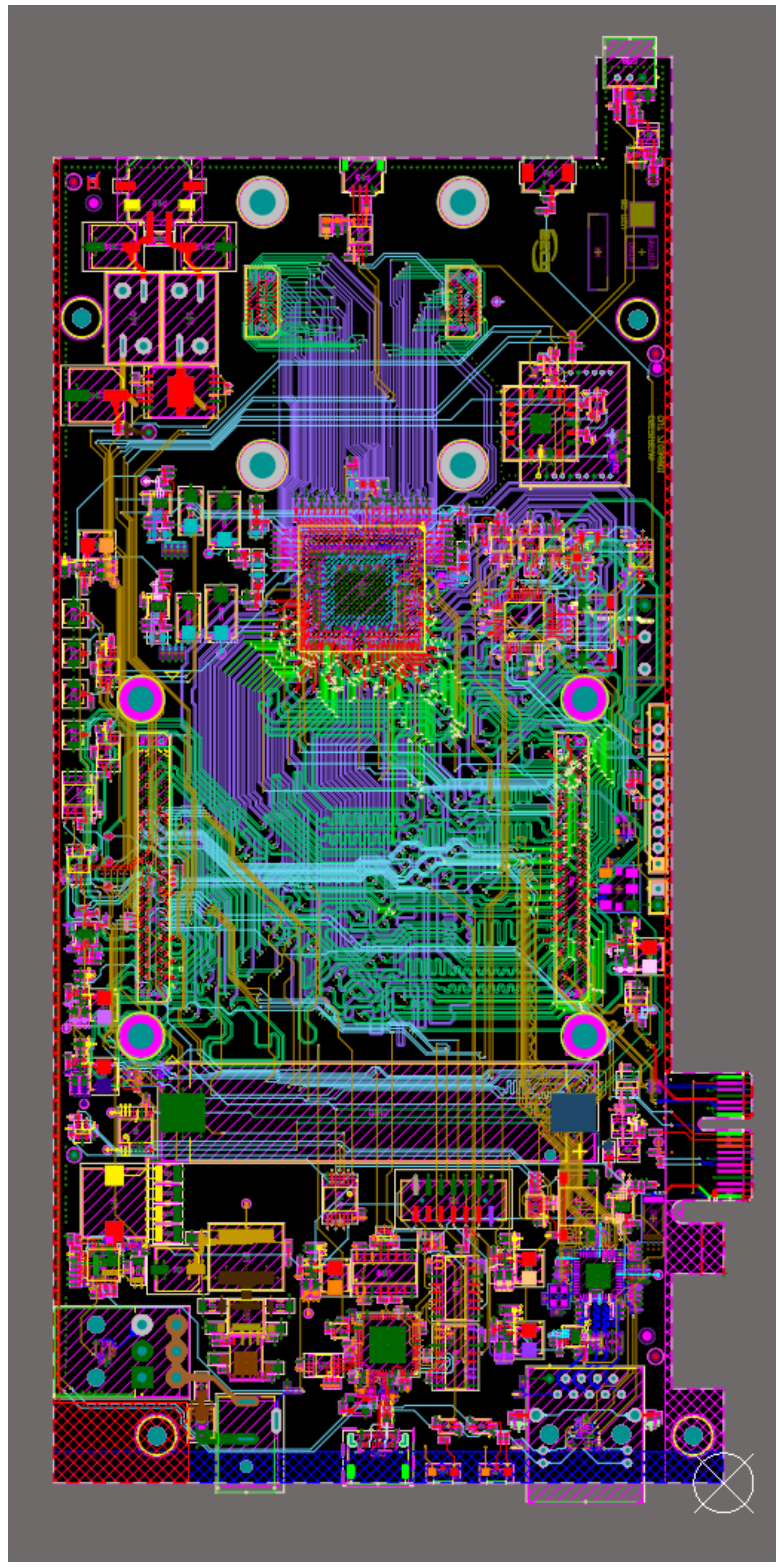
✳ **RUNS: testing the statistics of the number of sequences of identical bits in a string**

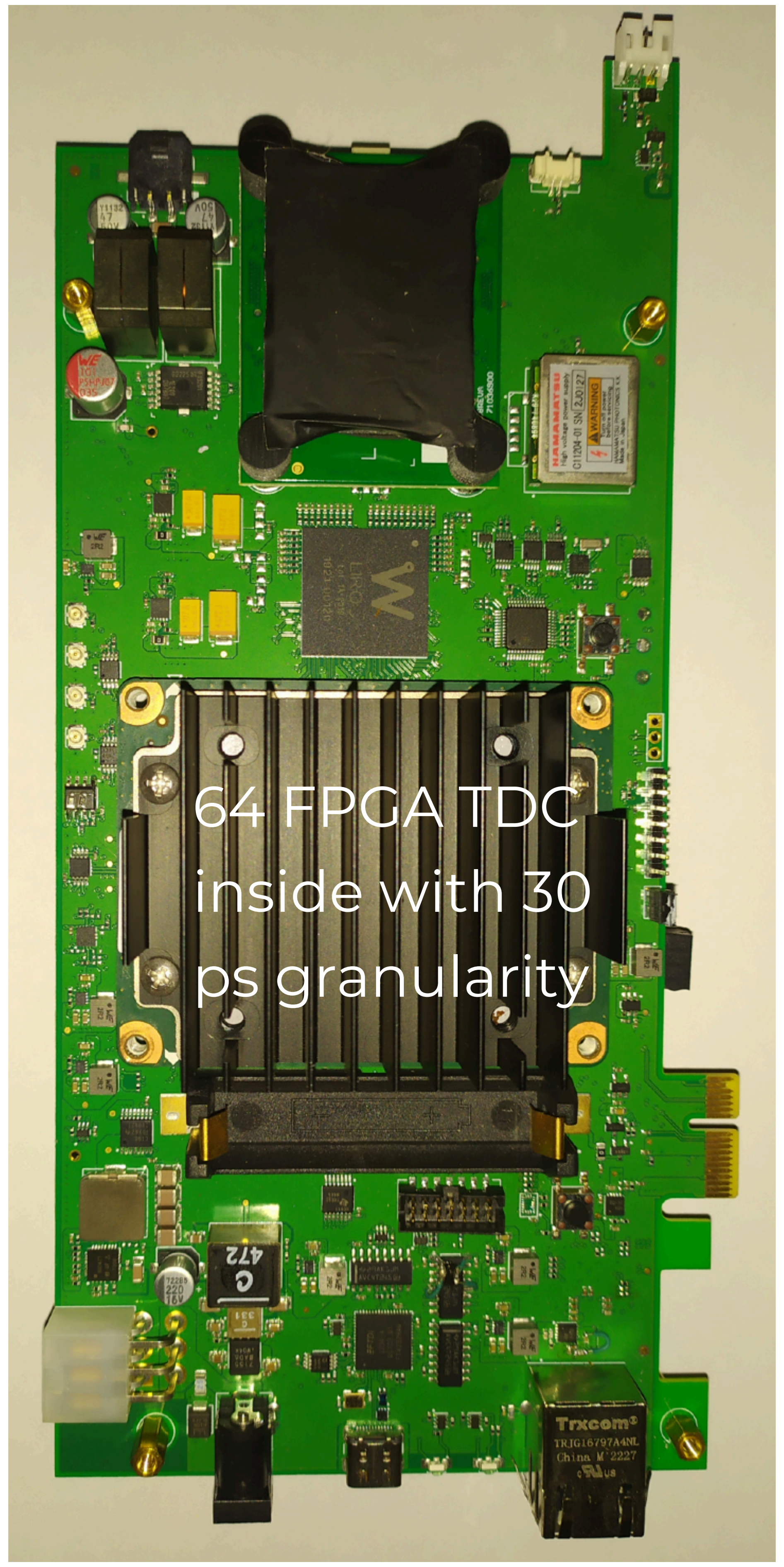
1 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1

5 bits 1 bit 2 bits 3 bits 3 bits 1 bit

RANDOM POWER

# THE 64 GENERATORS BOARD






| | |
|---|---|
| **Dimensions [cm²]** | 11.1x31.2x2.0 |
| **No. generators** | 64 arrays |
| **Raw bit stream:** | 32 Mbps |
| **NIST DRBG output (SP800-90 A,B,C)** | 1 Gbps |
| **Control:** | Xilinx KRIA K26 SOM |
| **I/O:** | Eth or PCI-Express |
| **Power supply:** | 12V, 8A |
| **Power consumption:** | 20W |
| **Encryption of the bit stream:** | Yes (AES-256) |
| **Specific Features:** | • Firmware implemented Real-Time sanity checks (MONOBIT, RUNS, Adaptive proportion test, Repetition Count Test)<br>• Auxiliary post-processing through a SHA256 function<br>• Interface through the Trusted Execution Environment<br>• Temperature control though a Peltier cooler<br>• FIPS-140-3 compliant by design |
| **State of development:** | **v1.0 delivered in July 2023, qualified**<br>**v2.0, product grade, delivered in September 2024, being qualified**<br>**software architecture under development** |

Goal of the ATTRACT Phase 2 project (May 2022-Fall.2023)

RANDOM POWER

# BEYOND A PURE TRUE RANDOM NUMBER GENERATOR (TRNG)

**NIST Special Publication 800-90B**

**Recommendation for the Entropy Sources Used for Random Bit Generation**

How to design and test entropy sources to be used to feed Deterministc Random Bit Generators (DRBG)

**NIST Special Publication 800-90A Revision 1**

**Recommendation for Random Number Generation Using Deterministic Random Bit Generators**

Approved DRBG mechanisms

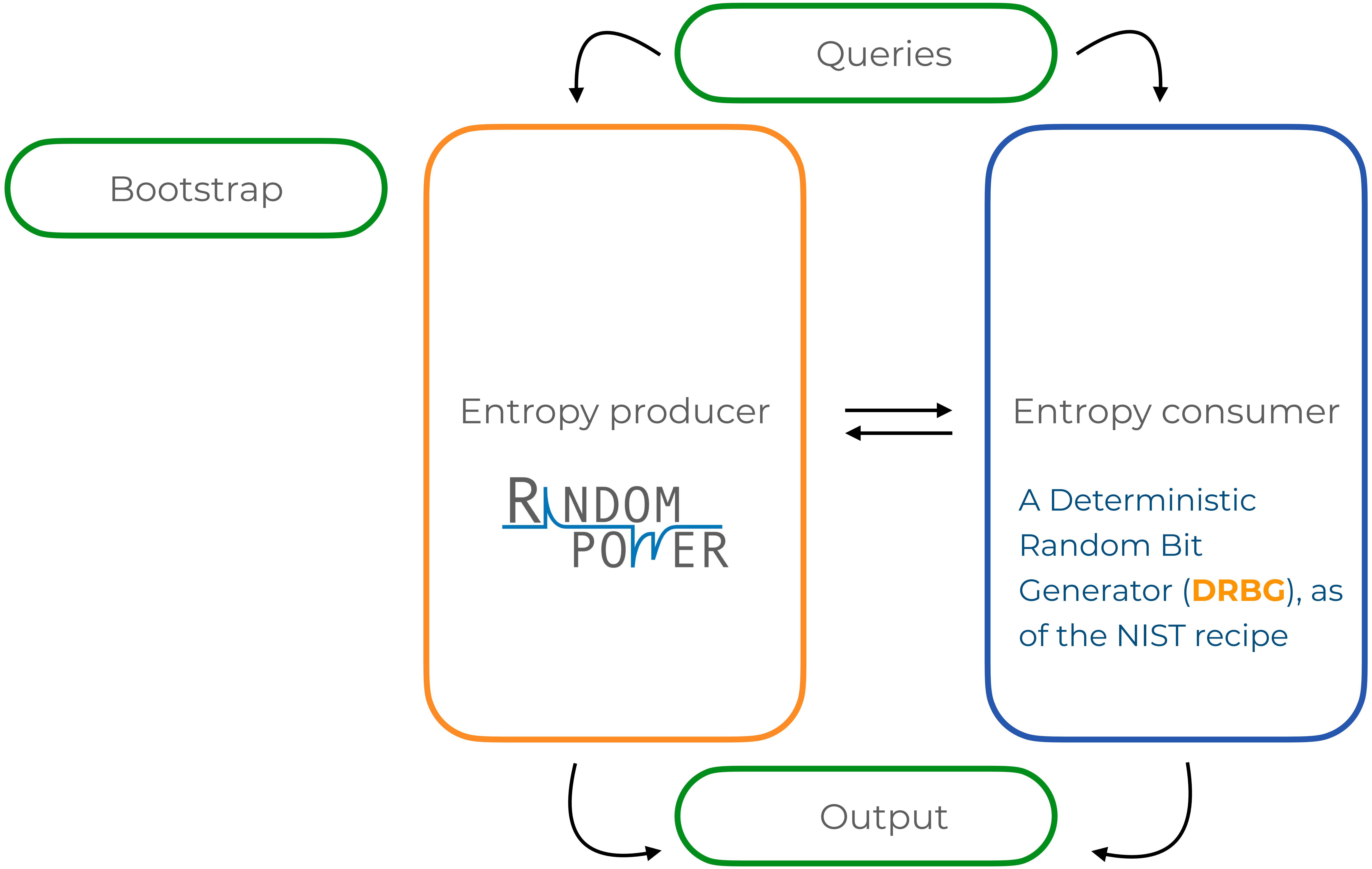
**(Second Draft) NIST Special Publication 800-90C**

**Recommendation for Random Bit Generator (RBG) Constructions**

Construction of RBG from A+B

- pre-requisites for entering the programs eventually leading to the FIPS-140-3 certification
- impacting on the design of both the ASIC, the multiple generator board and its embodiment in a “system”

# GO BEYOND A PURE TRUE RANDOM NUMBER GENERATOR (TRNG)




- Essentially, the True Random Bits generated by Random Power are used to seed a NIST approved Pseudo Random Bit Generator
- when reseeding occurs after EVERY iteration of the Deterministic machine, you obtain the highest level of security, namely **Prediction Resistance***

* QUOTING NIST: Prediction resistance means that a compromise of the DRBG internal state has no effect on the security of future DRBG outputs.

# BEYOND A PURE TRUE RANDOM NUMBER GENERATOR (TRNG)

**Why this is done?** in principle, the majority of the randomness tests qualify the stream against modelled pitfalls but you cannot exclude a priori unknown deviations.

"Universal tests" have been proposed, connected to "compression" algorithms but even Maurer's test, the most widely known, in its practical implementation can possibly have a reduced diagnostics power:

J. Cryptology (1992) 5: 89–105

Journal of Cryptology


## A Universal Statistical Test for Random Bit Generators*

Ueli M. Maurer
Institute for Theoretical Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland

Communicated by Rainer A. Rueppel

Received 2 April 1990 and revised 23 June 1991

**Abstract.** A new statistical test for random bit generators is presented which, in contrast to presently used statistical tests, is universal in the sense that it can detect any significant deviation of a device's output statistics from the statistics of a truly random bit source when the device can be modeled as an ergodic stationary source with finite memory but arbitrary (unknown) state transition probabilities. The test parameter is closely related to the device's per-bit entropy which is shown to be the correct quality measure for a secret-key source in a cryptographic application. The test hence measures the cryptographic badness of a device's possible defect. The test is easy to implement and very fast and thus well suited for practical applications. A sample program listing is provided.

## AN ACCURATE EVALUATION OF MAURER'S UNIVERSAL TEST

**Jean-Sébastien Coron**
Ecole Normale Supérieure
45 rue d'Ulm
Paris, F-75230, France
coron@clipper.ens.fr

**David Naccache**
Gemplus Card International
34 rue Guynemer
Issy-les-Moulineaux, F-92447, France
naccache@compuserve.com

**Abstract.** Maurer's universal test is a very common randomness test, capable of detecting a wide gamut of statistical defects. The algorithm is simple (a few Java code lines), flexible (a variety of parameter combinations can be chosen by the tester) and fast.

Although the test is based on sound probabilistic grounds, one of its crucial parts uses the heuristic approximation :

$$c(L,K) \cong 0.7 - \frac{0.8}{L} + \left(1.6 + \frac{12.8}{L}\right) K^{-4/L}$$

In this work we compute the precise value of $c(L,K)$ and show that the inaccuracy due to the heuristic estimate can make the test 2.67 times more permissive than what is theoretically admitted.

RANDOM POWER

# BEYOND A PURE TRUE RANDOM NUMBER GENERATOR (TRNG)

**Why this is done?** in principle, the majority of the randomness tests qualify the stream against modelled pitfalls but you cannot exclude a priori unknown deviations.

On the other hand, if you can mathematically prove the strength of an algorithm, you can feel relieved. **Maybe**:

## Security Analysis of NIST CTR-DRBG

Viet Tung Hoang[1] and Yaobin Shen[2]

[1] Dept. of Computer Science, Florida State University
[2] Dept. of Computer Science & Engineering, Shanghai Jiao Tong University, China

**Abstract.** We study the security of CTR-DRBG, one of NIST's recommended Pseudorandom Number Generator (PRNG) designs. Recently, Woodage and Shumow (Eurocrypt' 19), and then Cohney et al. (S&P' 20) point out some potential vulnerabilities in both NIST specification and common implementations of CTR-DRBG. While these researchers do suggest counter-measures, the security of the patched CTR-DRBG is still questionable. Our work fills this gap, proving that CTR-DRBG satisfies the robustness notion of Dodis et al. (CCS'13), the standard security goal for PRNGs.

## An Analysis of the NIST SP 800-90A Standard

Joanne Woodage[1], Dan Shumow[2]

[1] Royal Holloway, University of London
[2] Microsoft Research

**Abstract.** We investigate the security properties of the three deterministic random bit generator (DRBG) mechanisms in the NIST SP 800-90A standard [2]. This standard received a considerable amount of negative attention, due to the controversy surrounding the now retracted DualEC-DRBG, which was included in earlier versions. Perhaps because of the attention paid to the DualEC, the other algorithms in the standard have received surprisingly patchy analysis to date, despite widespread deployment. This paper addresses a number of these gaps in analysis, with a particular focus on HASH-DRBG and HMAC-DRBG. We uncover a mix of positive and less positive results. On the positive side, we prove (with a caveat) the robustness [16] of HASH-DRBG and HMAC-DRBG in the random oracle model (ROM). Regarding the caveat, we show that if an optional input is omitted, then – contrary to claims in the standard — HMAC-DRBG does not even achieve the (weaker) property of forward security. We also conduct a more informal and practice-oriented exploration of flexibility in implementation choices permitted by the standard. Specifically, we argue that these DRBGs have the property that partial state leakage may lead security to break down in unexpected ways. We highlight implementation choices allowed by the overly flexible standard that exacerbate both the likelihood, and impact, of such attacks. While our attacks are theoretical, an analysis of two open source implementations of CTR-DRBG shows that potentially problematic implementation choices are made in the real world.

EMV-SWG-NC62r3

EMVCo

EMVCo Position Statement on

**The Alleged backdoor in a NIST Random Number Generator (Dual EC DRBG)**

January 2014

This paper provides the EMVCo position regarding an alleged backdoor in the NIST Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC-DRBG).

**Background**

Recent allegations arising from Snowden-NSA disclosures are in fact a re-surfacing of publicly aired concerns dating back to 2007 regarding a random number generator being standardised by NIST, ANSI and ISO. This random number generator uses elliptic curve cryptography to produce an output sequence of pseudo random bits. However researchers showed that anyone knowing the inverse of one of the ECC parameters of the generator and also knowing just 32 bytes of the generator's output will be able to determine the secret internal state of the generator and thus be able to predict all the generator's output bits.

Thus the security of the Dual EC-DRBG rests on the secrecy of the inverse of the ECC parameter. NIST, ANSI and ISO Standards specify the use of a parameter originating from the NSA and the allegations are that the NSA knows its inverse. Note that in the NIST, ANSI and ISO Standards the Dual EC-DRBG is just one of multiple ways of generating random bits.

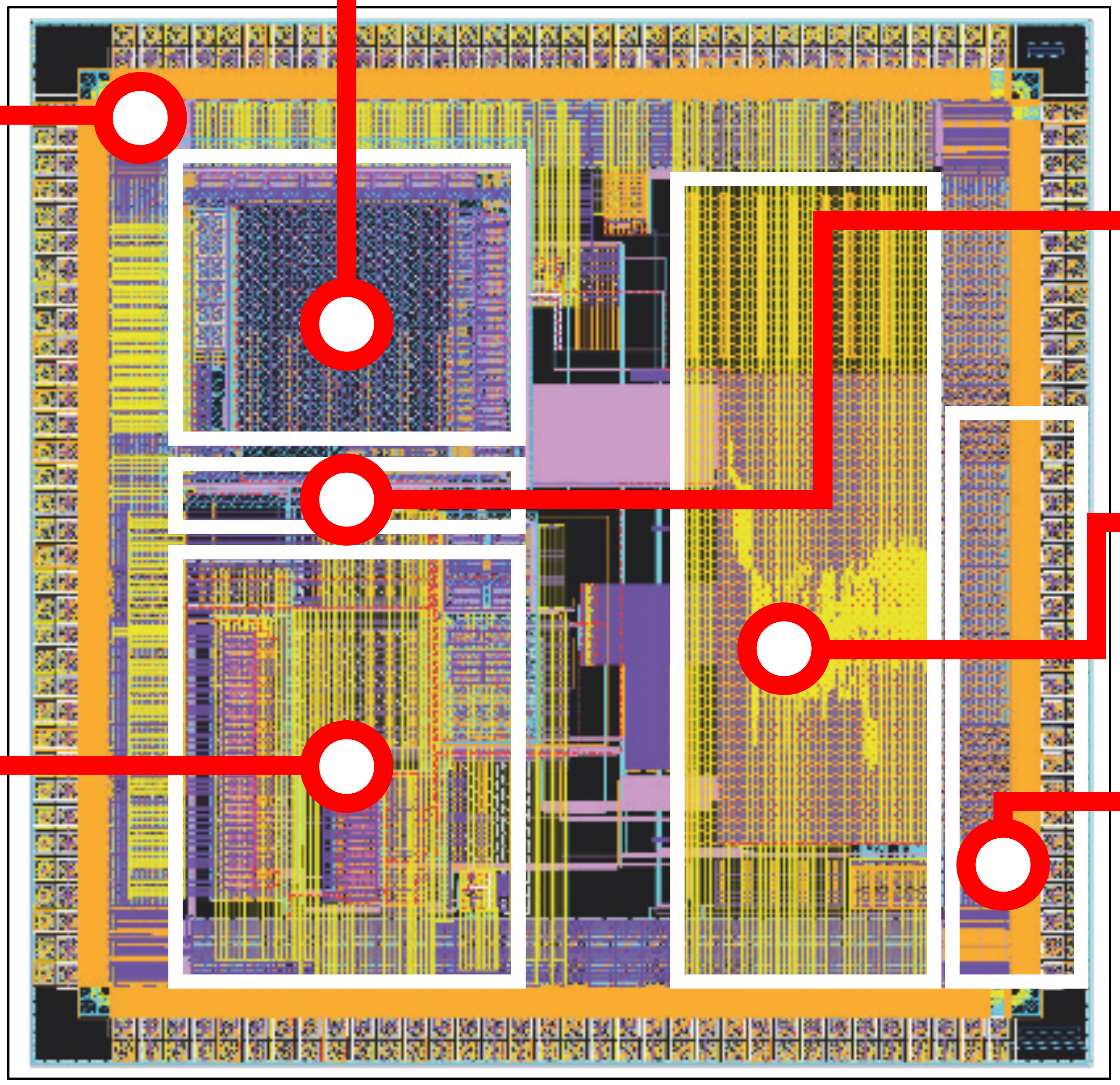
# THE ASIC:

Authentication at 3 levels, starting by a Silicon embedded primary key and a Key Derivation Function

32x 32-cell digital array of quantum entropy generator based on direct and trap assisted quantum tunneling

On-chip secure eFuses for key storage

High-resolution sub-nanosecond-level time to digital converters with near-zero dead time. Logic for the patented random bit generation



High-throughput streaming of the pulses to the readout electronics

FIPS compliant DRGB, realtime AES256 bitstream encryption

2x24 MHz SPI Interface for easy integration with any commercial SoC, CPU, Microcontroller and FPGA

AES-256 encryption of the bit stream

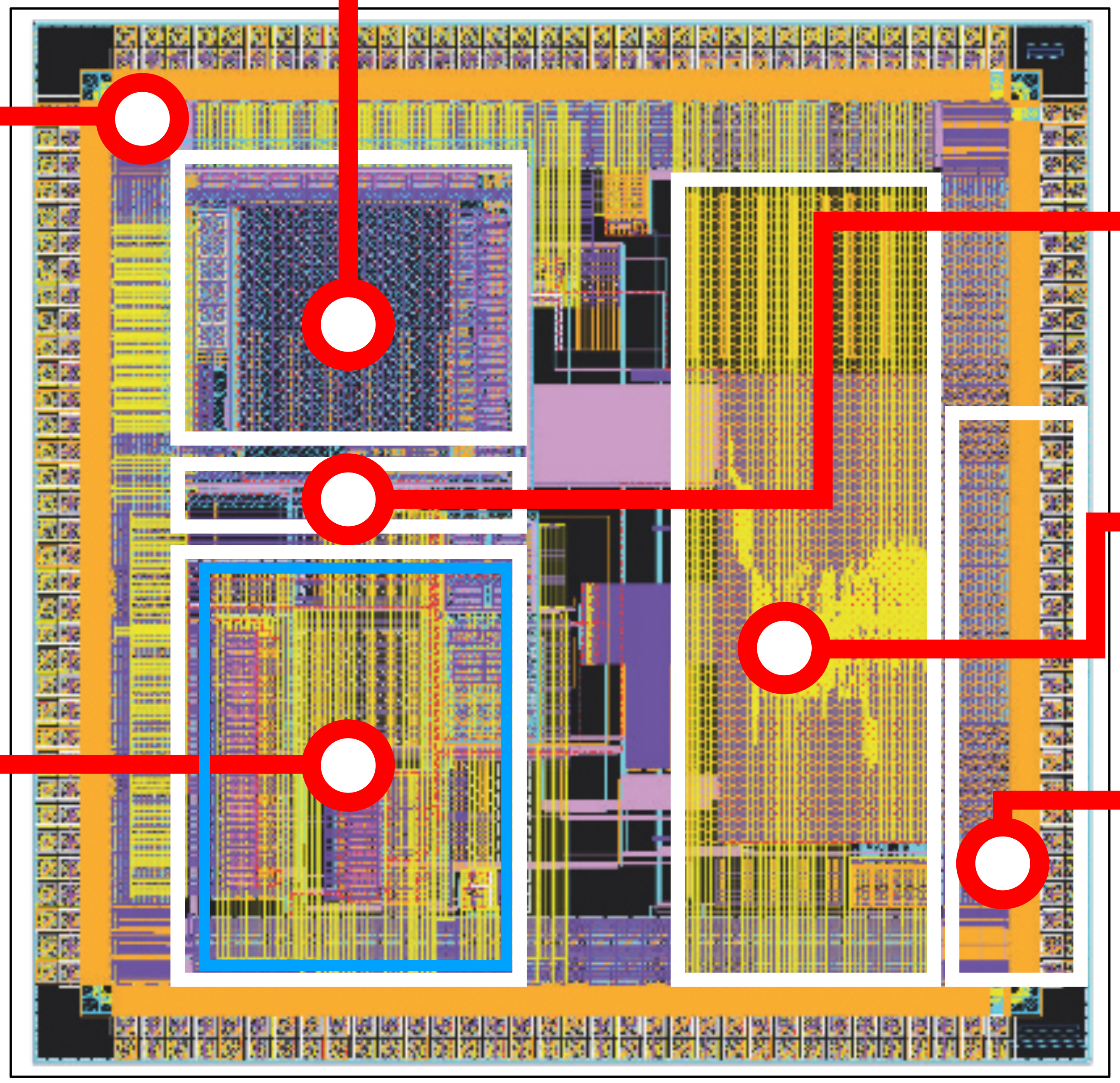
| | |
|---|---|
| **Dimensions [cm²]** | 1x1 |
| **No. generators** | 1 array |
| **Raw bit stream:** | 2-8 Mbps |
| **NIST DRBG output (SP800-90 A,B,C)** | 32 Mbps |
| **Control:** | SPI at 24 MHz |
| **I/O:** | SPI at 24 MHz |
| **Power supply:** | 5V, 1.8V |
| **Power consumption:** | 100 mW |
| **Encryption of the bit stream:** | Yes (AES-256) |

| | |
|---|---|
| **Specific Features:** | • On Silicon implementation of the NIST Real-Time sanity checks (Adaptive Proportion Test and Repetition Count Test)<br>• On Silicon implementation of the NIST DRBG protocol<br>• Package: QFN100<br>• FIPS 140-3 compliancy by design;<br>• CAVP (Cryptographic Algorithm Validation Program) granted |

- Out-of-the fab in June 2024, result of an engineering run
- Full qualification close to completion

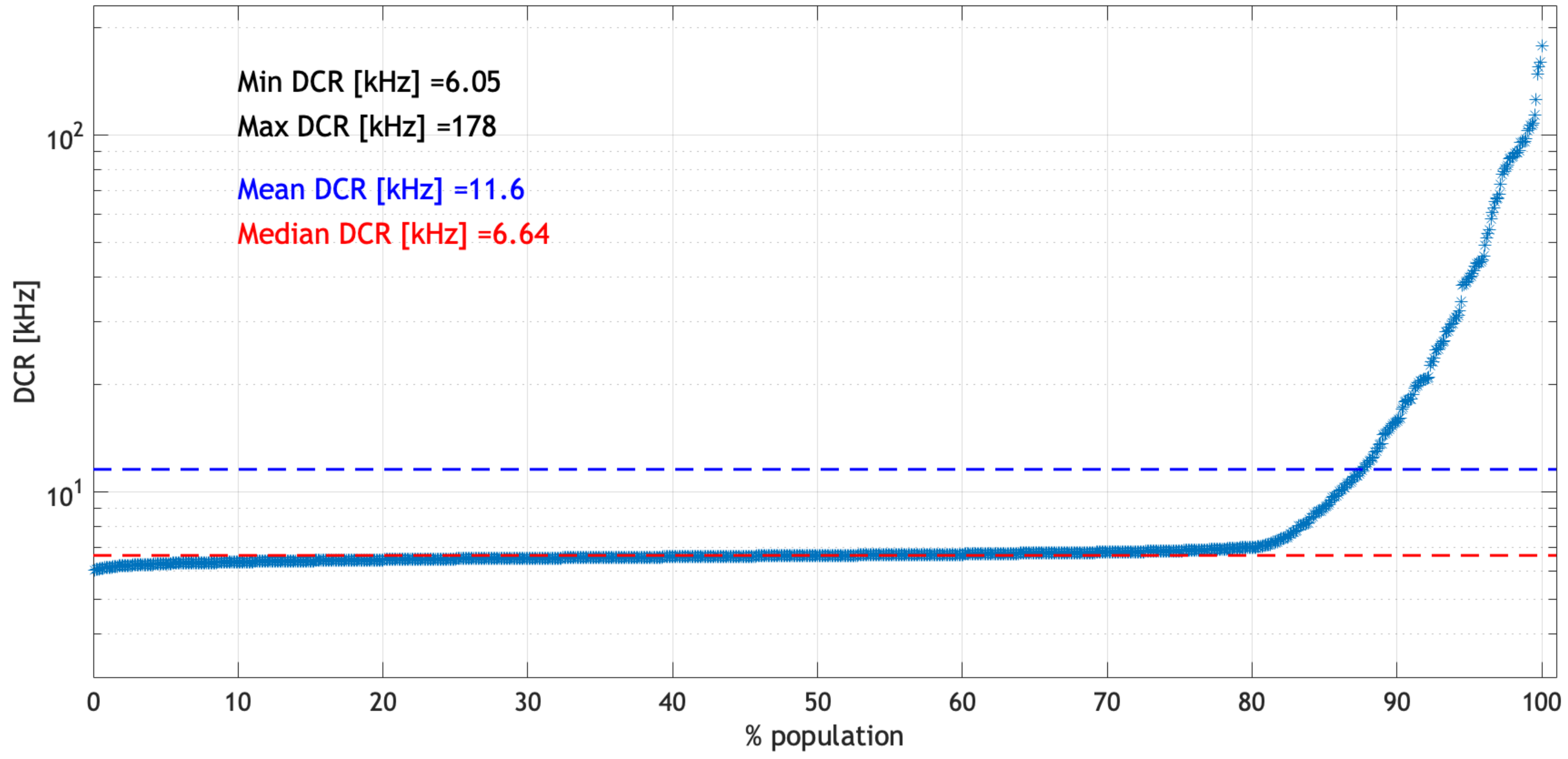
RANDOM POWER

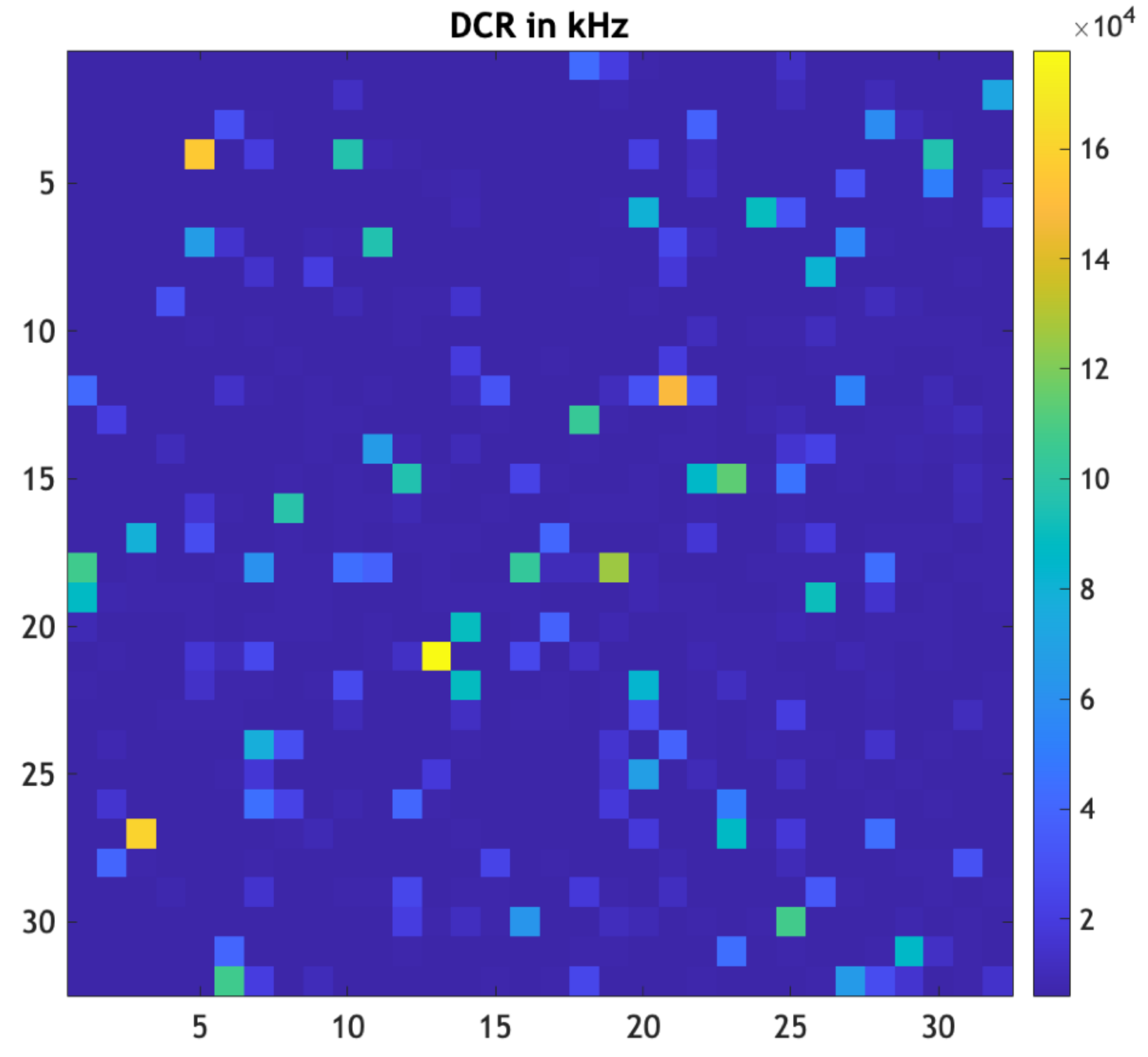
# THE ASIC:




It embodies also:

- two different TDC architectures
- a two stage mechanism to implement "screamers identification" and a procedure for the rate stabilisation:




RANDOM POWER

Beside hardware:

BEST PAPER AWARD

CERTIFICATE

IEEE CSR
Cyber Security and Resilience

The IEEE CSR 2024 conference chairs:

Stavros Shiaeles

Nicholas Kolokotronis

Emanuele Bellini

Awarded to:

On-line anomaly detection and qualification of random bit streams

Authored by:

C. Caratozzolo, V. Rossi, K. Witek, A. Trombetta, and M. Caccia

Presented at:

2024 IEEE International Conference on Cyber Security and Resilience
September 2–4, 2024 • London, UK

The IEEE International Conference on Cyber Security and Resilience (IEEE CSR) is an annual event cosponsored by the IEEE Systems, Man, and Cybernetics (SMC) Society

available on ArXiv at https://arxiv.org/abs/2409.05543

# Essentially, Thanks to the EC

ATTRACT

**Our consortium:**

UNIVERSITAS STUDIORUM INSUBRIAE — leading party

FONDAZIONE BRUNO KESSLER — FUTURE BUILT ON KNOWLEDGE

AGH

NAGRA KUDELSKI GROUP

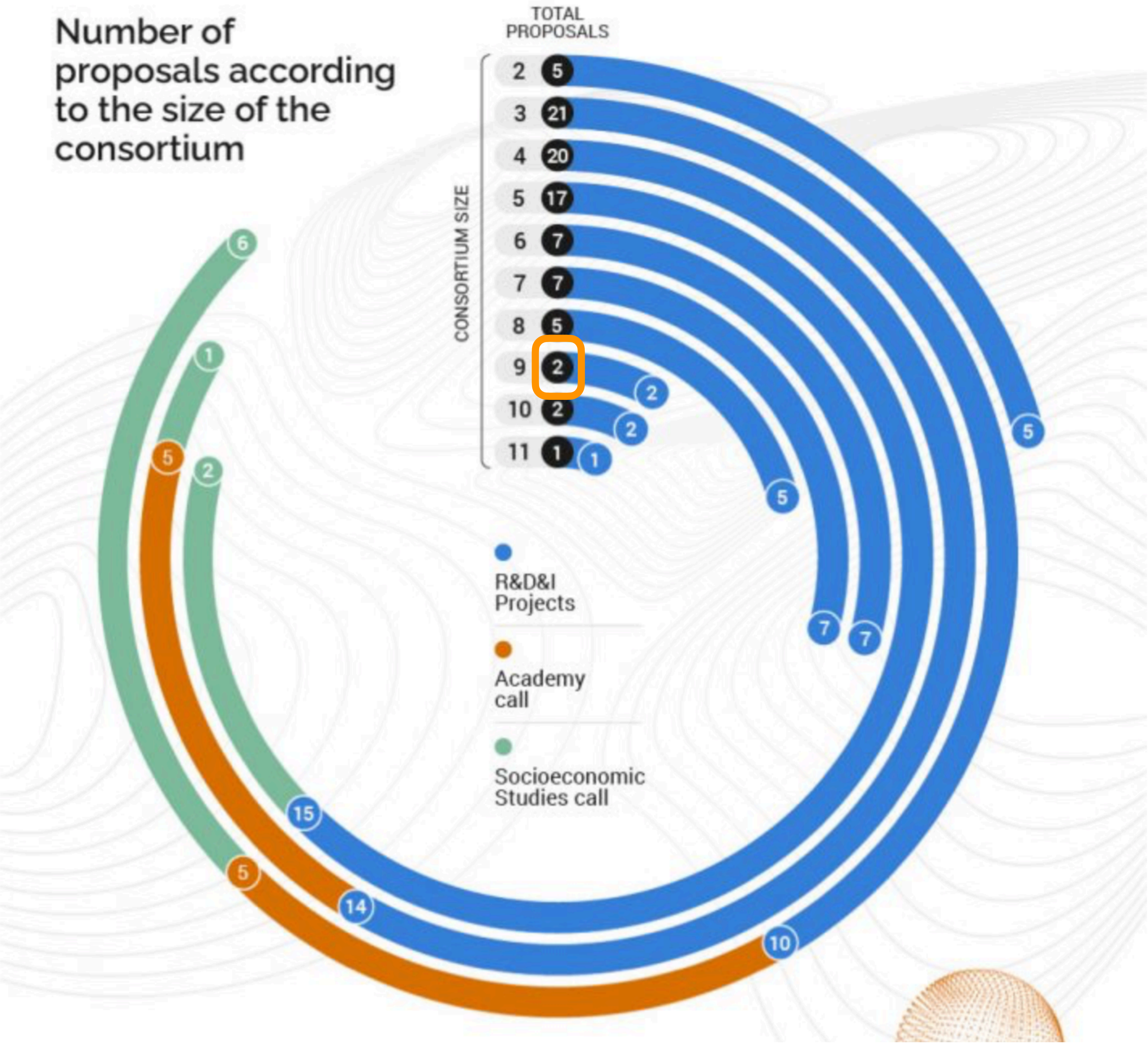
E4 COMPUTER ENGINEERING

SECO

imasenic

weeroc

RANDOM POWER




**18 man-years dedicated to the project**

RANDOM POWER

# HISTORY & TEAM: pre-incorporation

2016

The principle at the base of RandomPower emerges, as result of a genuine serendipity event. Initial tests performed with lab

2017

Unpredictability of the generated random bit sequence is assessed

2018

- A **demo board** is designed, commissioned and qualified;
- Italian patent filing completed (October)
- launch at the CyberSecurity week in Le Hague (October)
- **submission** of the **ATTRACT Phase 1** proposal (October)

2019

- **Approval** & **kick-off** of the **ATTRACT Phase 1** proposal (May)
- design, commissioning and production of the single generator board;

2020

- **End** of the **ATTRACT Phase 1** project (October)
- **Full characterisation** of the single generator board
- **winner** of the **Start-Cup competition** (regional level; 20 kEUR)
- **winner** of two special prizes by investors at PNI, start-up competition at **national level**

RANDOM POWER

# HISTORY & TEAM: post-incorporation (2021)

- **approval** of the **ATTRACT Phase 2** proposal (January) (**2 MEUR**)
- **kick-off** of the ATTRACT Phase 2 (May)
- proto-farm commissioned
- implementation of the TESTU01 suite, complementing the NIST test (1.5 Tb qualified)
- **winner** of the Falling Walls venture int'l competition (November)

2021

- first implementation of real-time sanity checks
- **company establishment** (June)
- **investment (200 kEUR)** by **LifTT**, our VC (June)
- **Submission** of the **ATTRACT**

2022

- real-time sanity check implemented
- design of the multi-gen board completed (April) v1.0
- commissioning of v1.0 started (July) ; qualification completed in December
- **chip submission in mid-September**

2023

- **Chip delivery (Q2)**
- Chip qualification (Q4)
- 64x board product grade qualification (Q3)
- v1.0 of the FIPS compliant sw architecture for the multi-age board
- **FIPS 140-3 certification started**
- **Business plan v2.0**
- **End of the ATTRACT Phase 2 (fall; Extended by now!**
- **Execution of the next investment round**

2024

RANDOM POWER

Join us, we will be happy to walk with you!

2020-11 Winner of 2 “special prizes”

2020-10 Winner - ICT

2021-06 PoC investment by LifTT, a VC located in Torino (ITALY)

2022-11 winner @the Falling Walls venture competition
for curious people:
here & and there

I AM A FALLING WALLS WINNER

2024-03 Random Power goes to the most important trade fair on IoT technologies, hosted at the SECO booth.

www.randompower.eu

**Established in June 2021**

This project has received funding from the ATTRACT project funded by the EC under Grant Agreement 777222