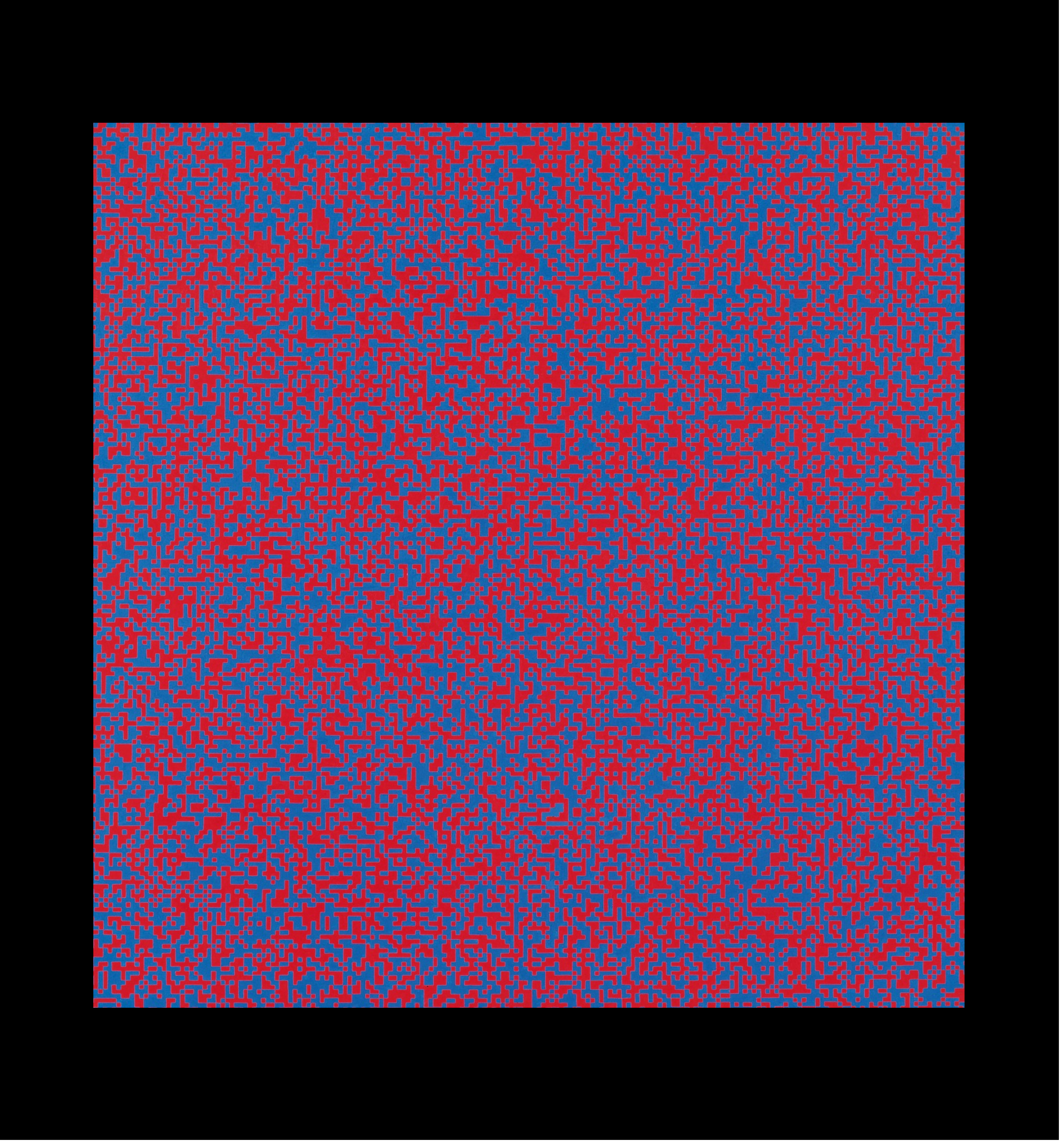


François Morellet
Random Distribution of 40,000 Squares using the Odd and Even Numbers of a Telephone Directory 1960

ATTRACT

In-Silico generation of random bit streams

RANDOM POWER

the value of unpredictability

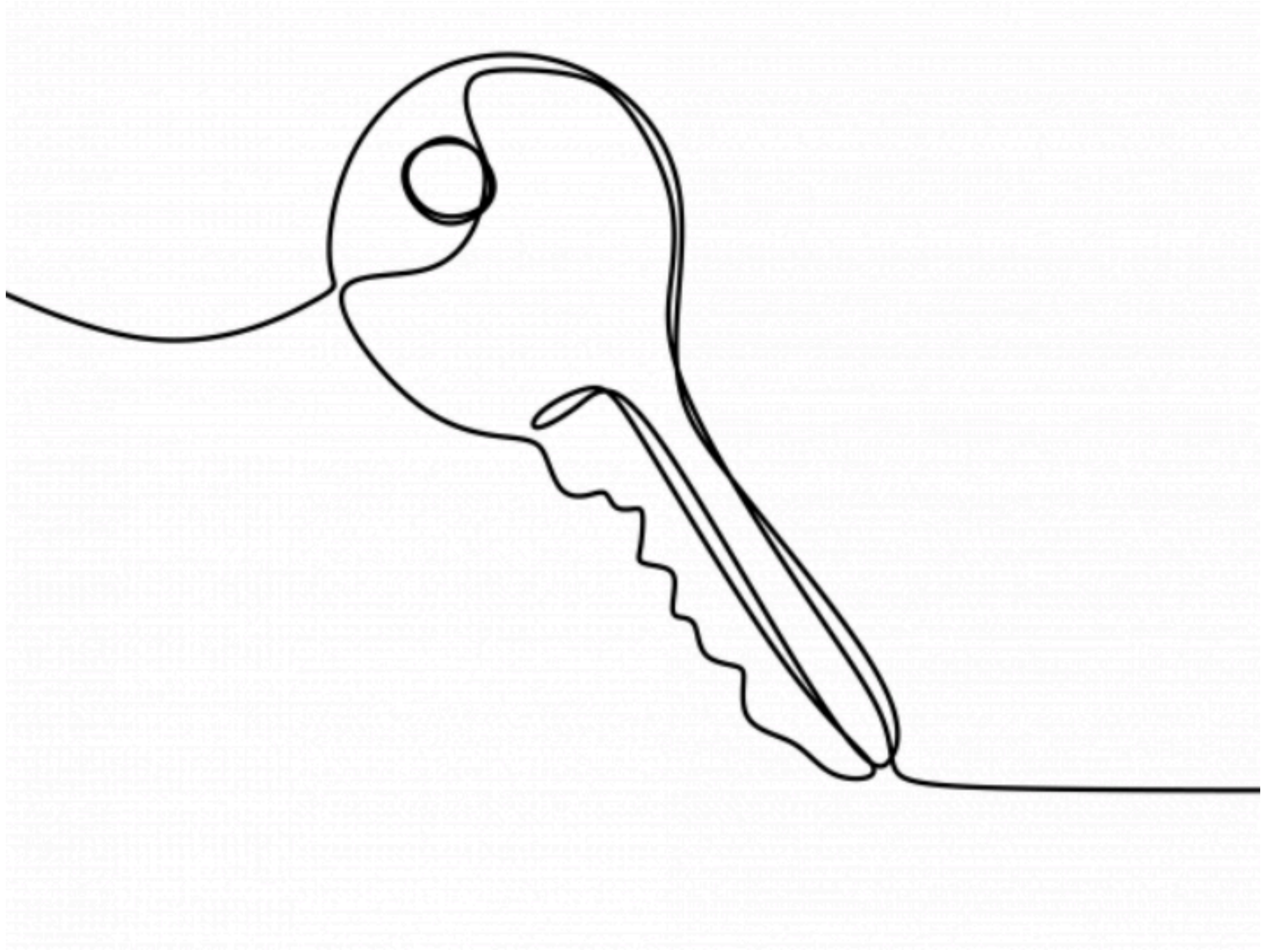
Massimo Caccia

Università dell'Insubria & Random Power s.r.l.

massimo.caccia@randompower.eu

ICHEP, Bologna, July 7th, 2022

WHAT DOORS TO HOMES & DIGITAL VAULTS HAVE IN COMMON?



In the Cryptographic world, keys are assembled using

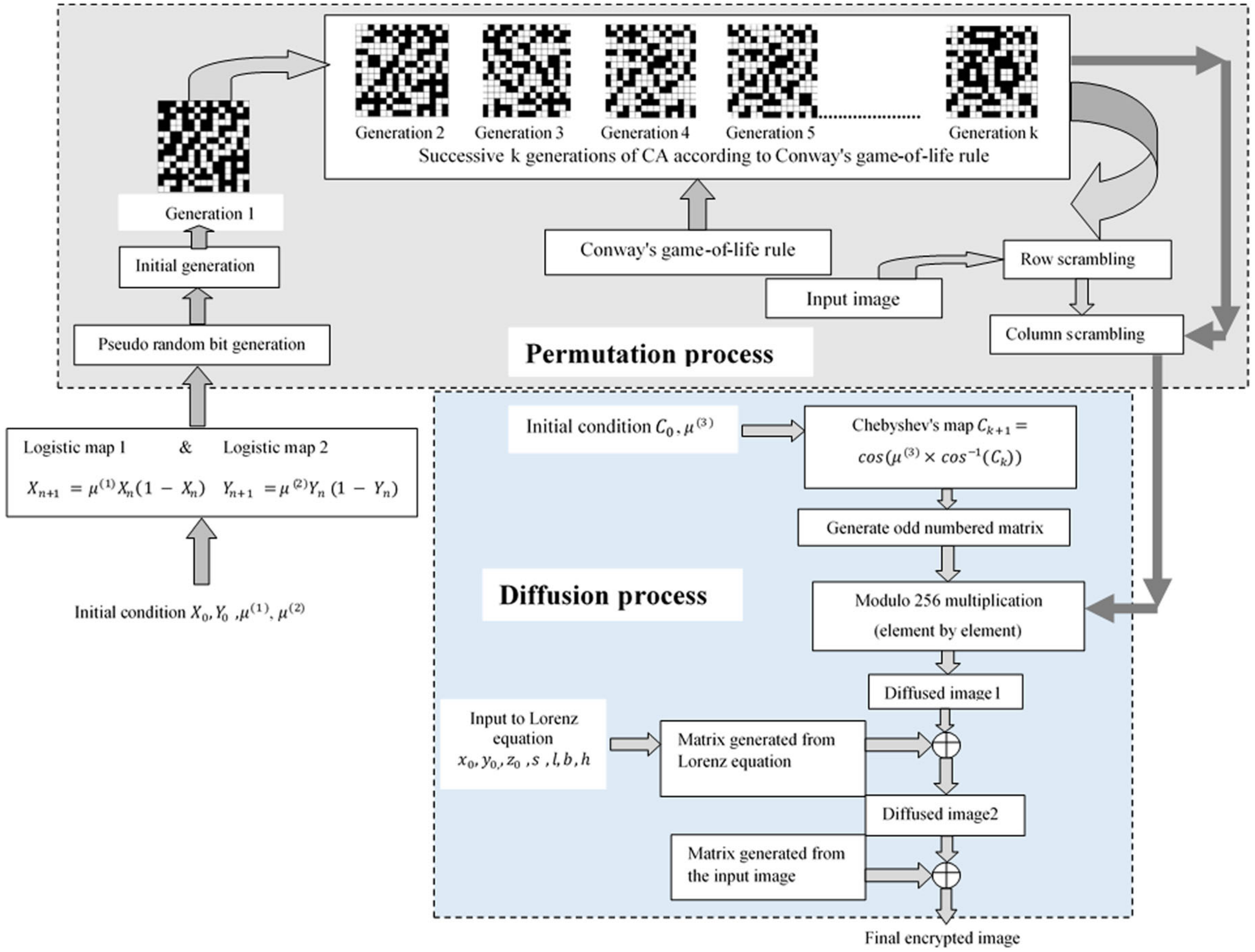
UNPREDICTABLE BIG PRIME NUMBERS*

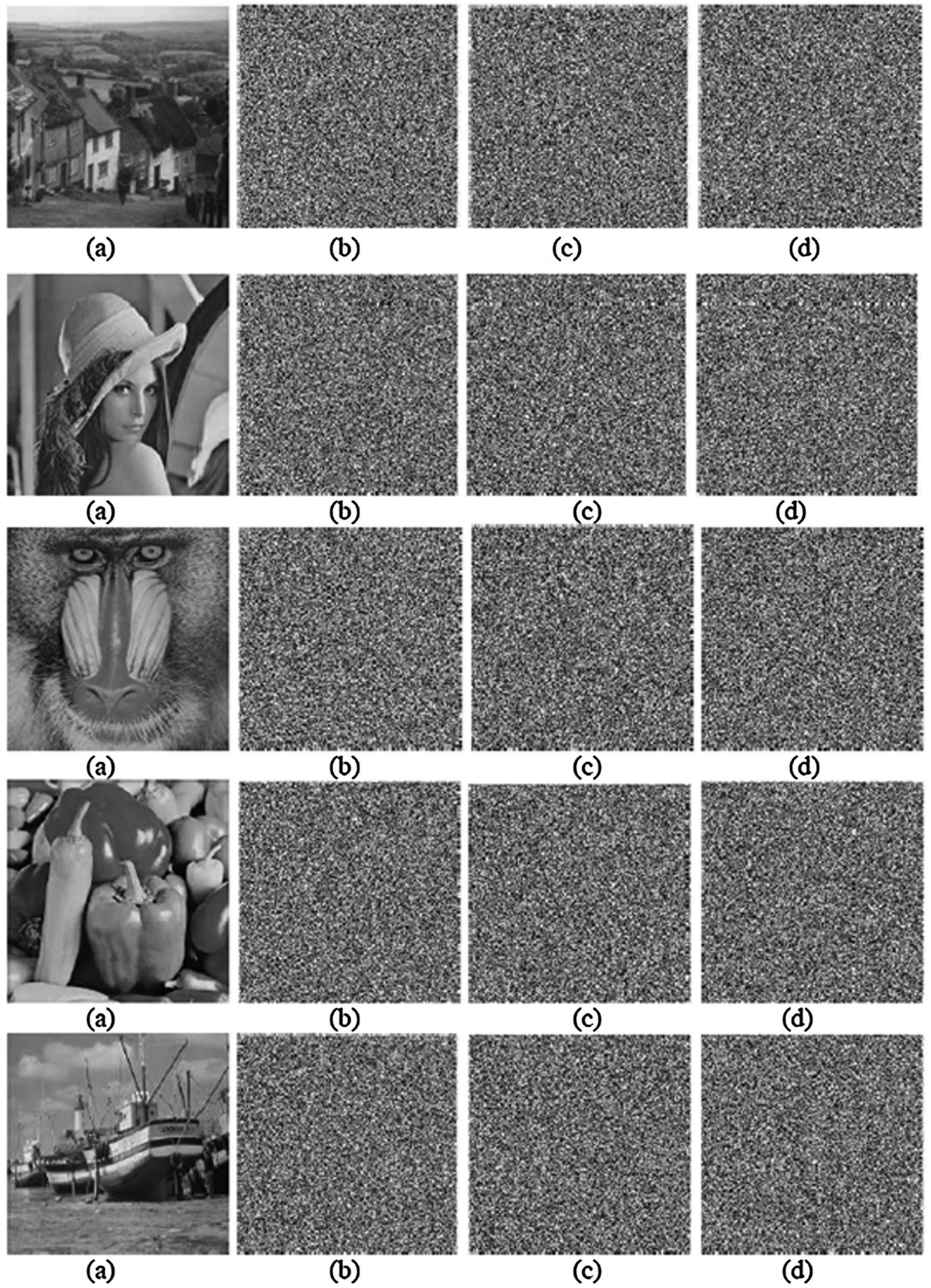
extracted from **random bit streams**

* in the RSA (Rivest–Shamir–Adleman) protocol, up to 2048 bit long

WHAT DOORS TO HOMES & DIGITAL VAULTS HAVE IN COMMON?

- **Image encryption** is also relying on random single-bit arrays:

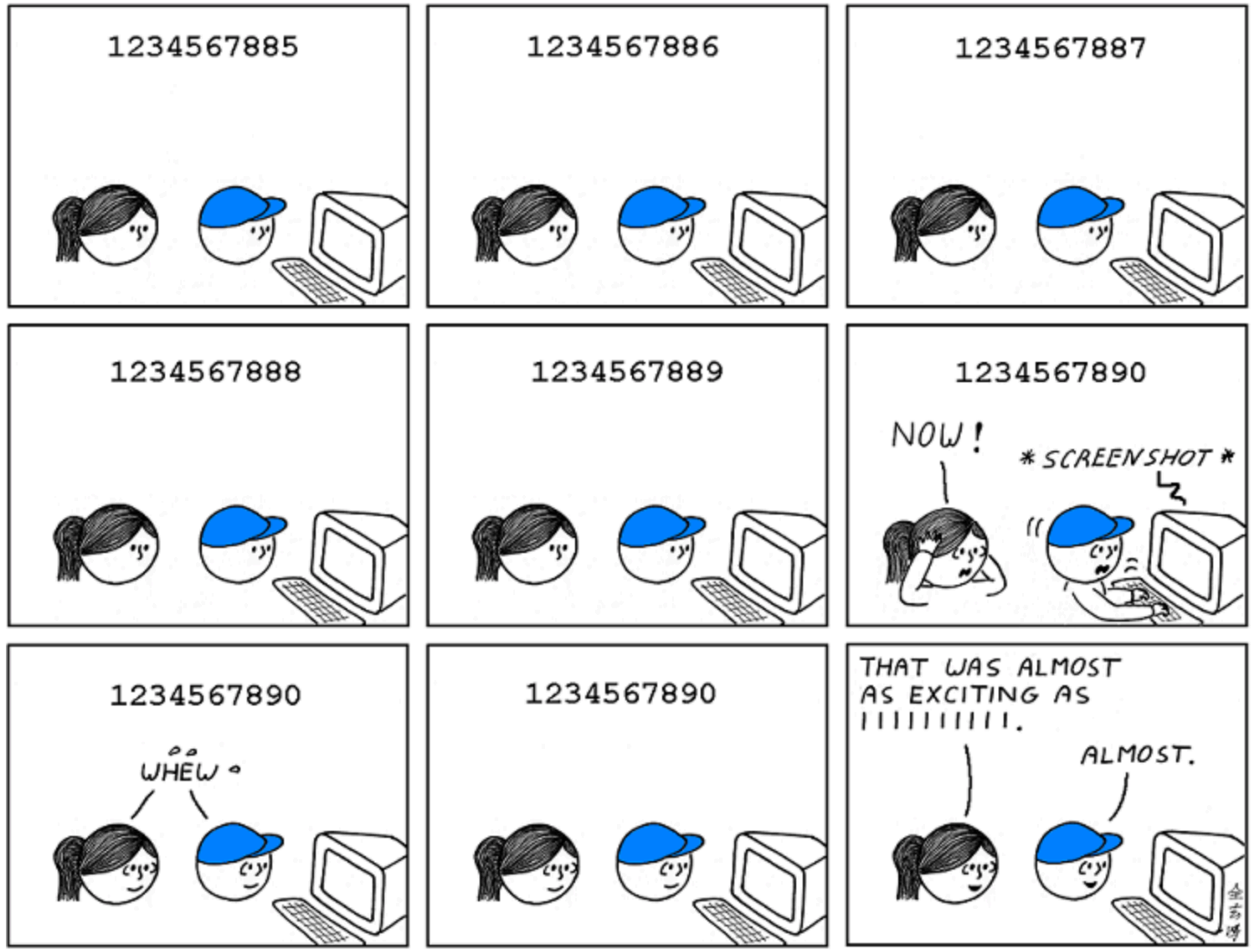




B. Murugan et al., A hybrid image encryption algorithm using chaos and Conway's game-of-life cellular automata, Security Comm. Networks 2016; 9:634–651, DOI: 10.1002/sec.1386

1. what for?

there is definitely a hype about Random bit streams, not only for crypto but also for gaming, virtual reality , Monte Carlo simulations and IoT (notably car security, smart houses, drones to guarantee authentication and secure transmission & control)



https://xkcd.com; Randall Munroe

https://www.cryptomathic.com/news-events/blog/generating-cryptographic-keys-with-random-number-generators-prng

INSIDE QUANTUM TECHNOLOGY

Primary Market:
cybersecurity & simulation

Quantum Random Number Generators: A Ten-year Market Assessment

Report IQT-QRNG-0121
Published January 19, 2021

Main findings: expected market volume of $7.2B by 2026

- most relevant segment: Data Centers [$3.1B]
- significant interest by financial service providers for improved Monte Carlo simulations & secure service access [$2.2B]

Georges de la Tour
The dice players (1651 c.a.)

Secondary Market:
gaming & gambling

Main applications:

- Replacement market of

“physical gambling devices”

[~ 7 Million cabinets worldwide, 5 years lifespan ⇒ ~1.4M new devices/year]

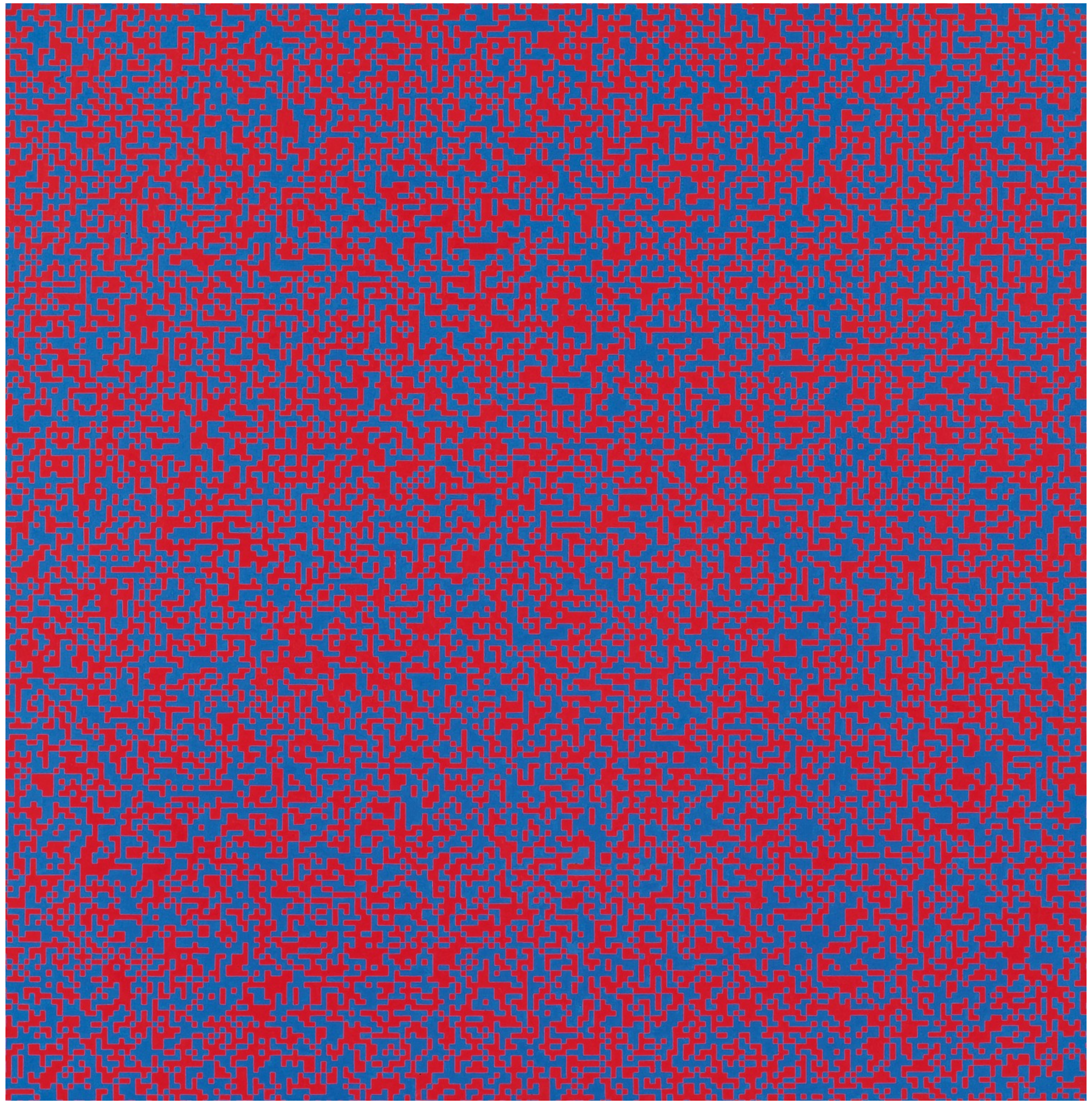
- Random number streaming to on-line platforms

HOW TO GENERATE AN UNPREDICTABLE RANDOM NUMBER?

It is always nice to consider an artist's point of view:

"With *Random Distribution*, the purpose of my system was to cause a reaction between two colours of equal intensity. **I drew horizontal and vertical lines to make 40,000 squares. Then my wife or my sons would read out the numbers from the phone book (except the first repetitive digits), and I would mark each square for an even number while leaving the odd ones blank.** The crossed squares were painted blue and the blank ones red. For the 1963 Paris Biennale I made a 3-D version of it that was shown among the Groupe de Recherche d'Art Visuel installations (and re-created it again on different occasions). I wanted to create a dazzling fight between two colours that shared the same luminosity. This balance of colour intensity was hard to adjust because daylight enhances the blue and artificial light boosts the red. I wanted the visitors to have a disturbing experience when they walked into this room – to almost hurt their eyes with the pulsating, flickering balance of two colours. I like that kind of aggression."

excerpt from https://www.tate.org.uk/context-comment/articles/65-38-21-4-72



François Morellet (1926-2016)
Random Distribution of 40,000 Squares using the Odd and Even Numbers of a Telephone Directory 1960
MOMA, New York

HOW TO GENERATE AN UNPREDICTABLE RANDOM NUMBER?

PRNG
(PseudoRandom Number Generators)

are essentially a piece of software code
⇒ they deterministic and in principle
predictable

$$x_n \equiv a x_{n-1} + b \; (mod\ m)$$

an example of linear congruential generator

J. Von Neumann: Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.

Von Neumann, John (1951). "Various techniques used in connection with random digits" (PDF). *National Bureau of Standards Applied Mathematics Series*. **12**: 36–38.

TRNG
(True Random Number Generators)

are essentially coin flipping,
namely get bits out observing unpredictable natural phenomena

http://glee.wikia.com/wiki/File:281735_1342370254-coin-flip.gif.gif

HOW TO GENERATE AN UNPREDICTABLE RANDOM NUMBER?

PRNG
(PseudoRandom Number Generators)

Fast, cheap & reasonably easy. However:

- software Random Number Generation is PSEUDO
- code can be bugged
- and it may have a BACKDOOR

2006


Attack Trends
Editor: David Ahmad, drma@mac.com

Two Years of Broken Crypto

Debian's Dress Rehearsal


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.

2013

TRNG
(True Random Number Generators)

Extracting bits from the observation of natural phenomena is not trivial and you may suffer from

- "coin bias" by the embodiment of a great principle
- weakness against environmental parameters
- a significant "attack surface", conditioning the device in use
- low bit rate

RANDOM POWER

HOW DO WE DO IT?

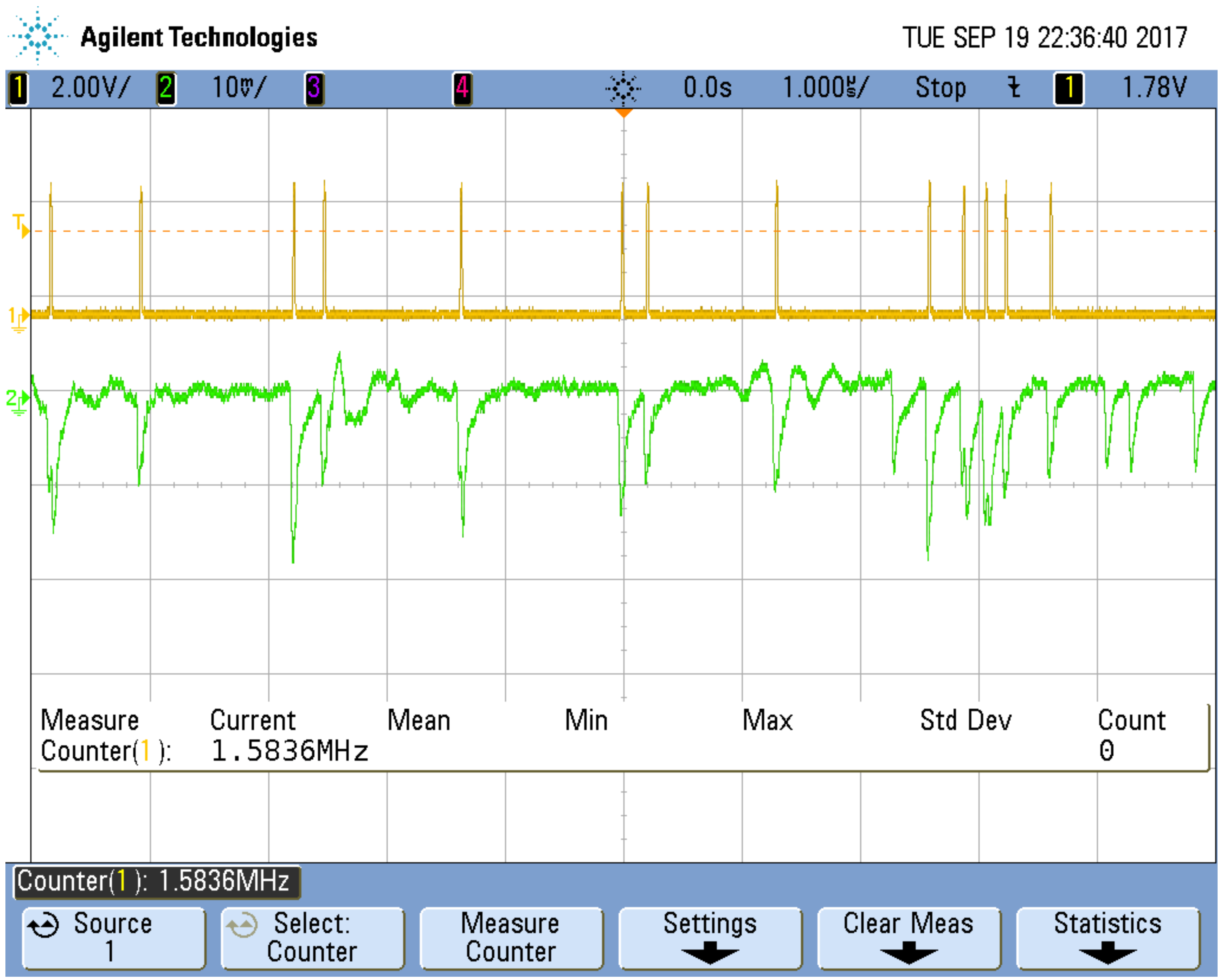
Inspired by Forrest Gump, we say:

RADIOACTIVE IS WHAT RADIOACTIVE DOES

- emission by a radioactive source is due to the quantum laws of Nature
- decays of unstable nuclei are unpredictable

⇒ 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



Sequence of pulses by the decay of a radioactive source in a nuclear physics detector

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.

What we do is essentially profiting from an effect well 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 μA with a variation of 11 decades for $p_{10}(I)$. The observation of a narrow turnoff interval is explained quantitatively.

JOURNAL OF APPLIED PHYSICS VOLUME 36, NUMBER 10 OCTOBER 1965

Mechanisms Contributing to the Noise Pulse Rate of Avalanche Diodes*

3

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 μA).[6–8]

from paper 2

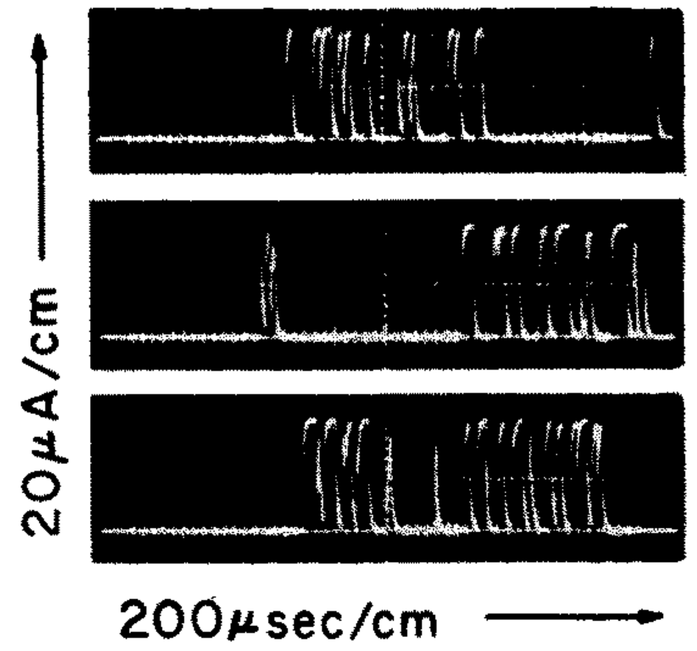
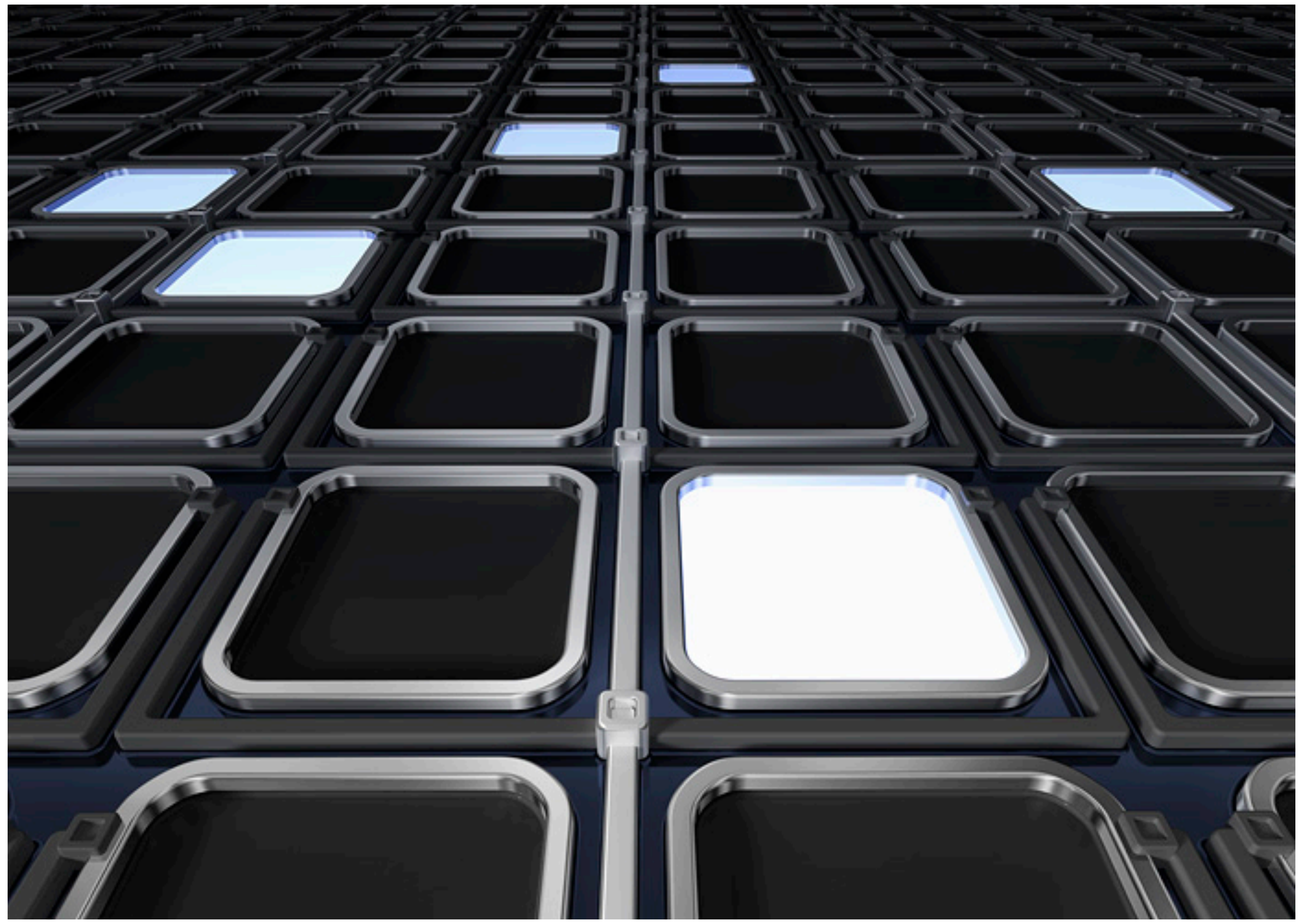


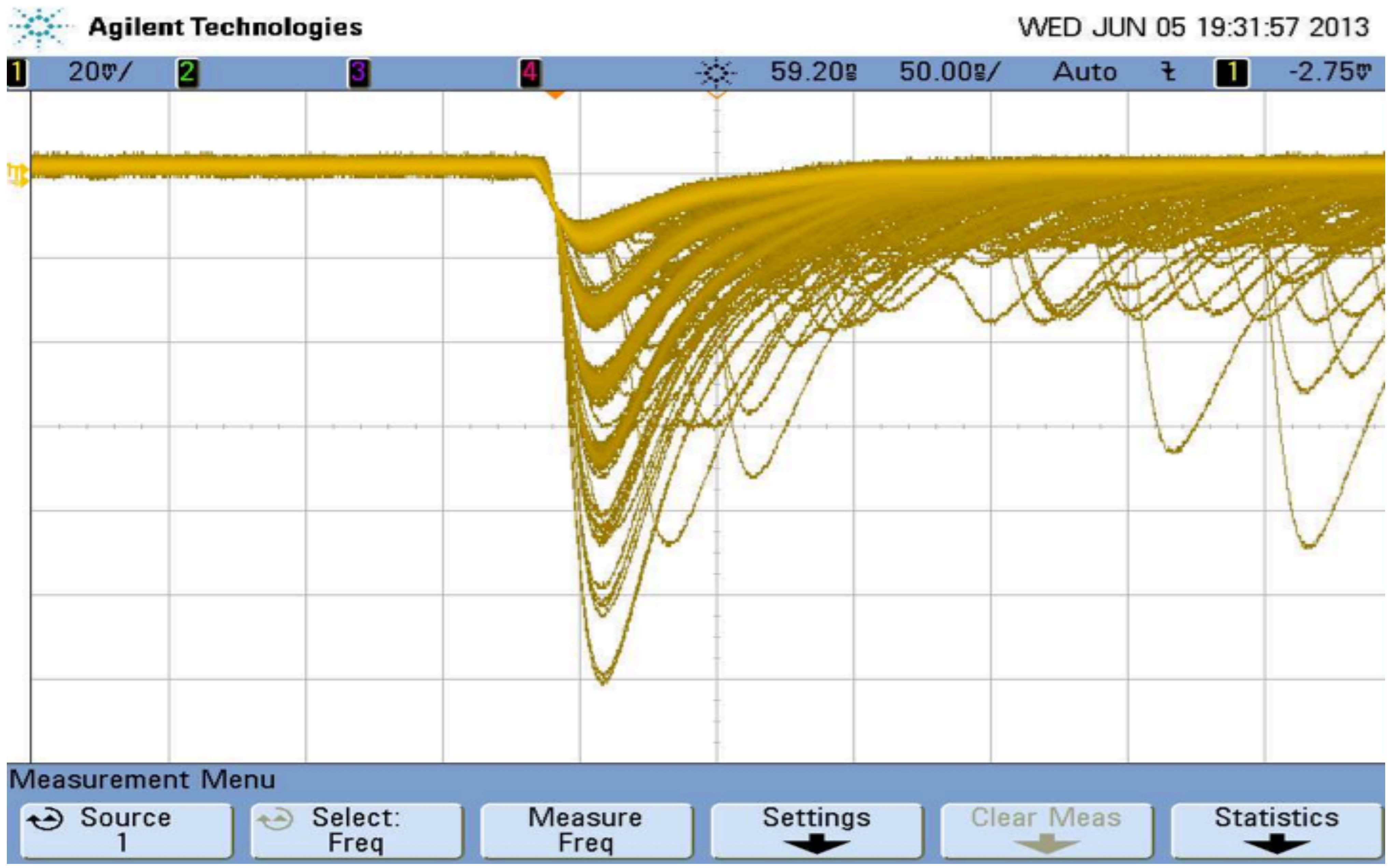
Fig. 5. Avalanche current as a function of time at low temperatures. The group character of the avalanche pulses is obvious.

from paper 3

Embodied in well known devices in their maturity stage, namely Silicon Photomultipliers, arrays of Single Photon Avalanche Diodes, (SPAD), p-n junctions operated beyond the breakdown voltage



- SiPM may be seen as a collection of binary cells, fired when a photon in absorbed



- "counting" cells provides an information about the intensity of the incoming light:

Silicon photomultipliers represent today the state-of-the-art detectors with

single photon sensitivity

and

photon number resolving capability

However, we know that charge carriers "seeding" the pulses can be generated "spontaneously", also when no light is illuminating the sensor and this is the name of the game

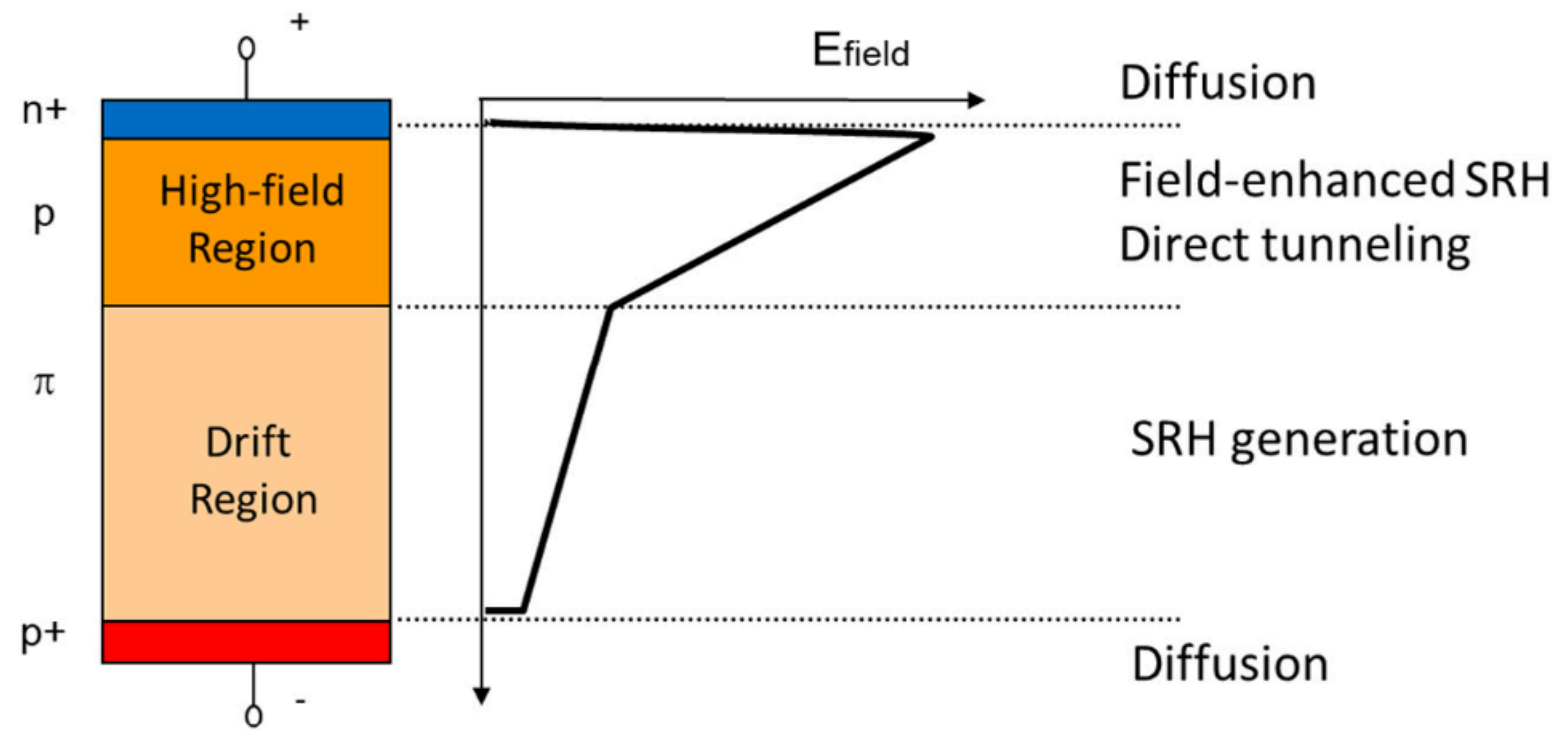


Fig. 8. Representation of the different sources of primary dark events and their location in the SPAD structure.

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

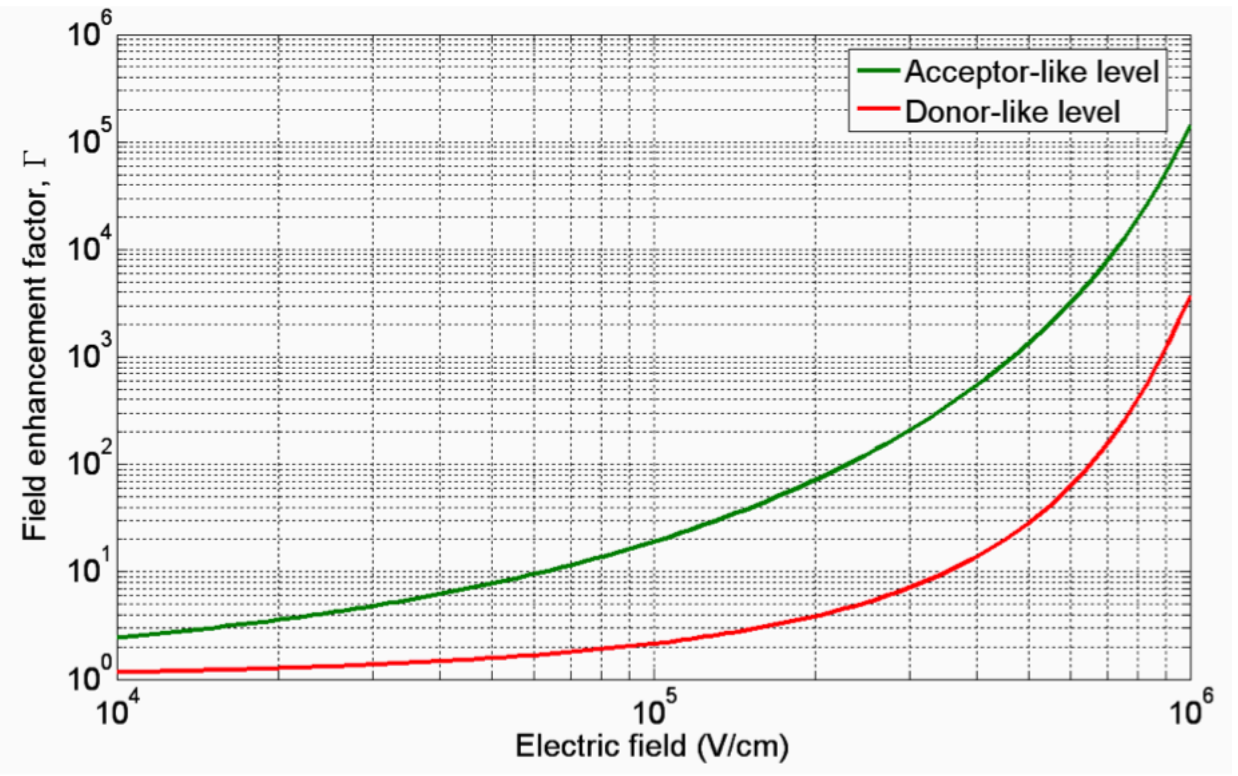
Thermal generation of carriers by states in the bang-gap (Shockley-Read-Hall statistics), where trapping and de-trapping is increased by the high electric field in the junction:

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

- E_0 = Fermi level
- E_t = trapping level
- n_i = intrinsic carrier concentration
- N_t = trapping concentration
- σ = trapping cross section
- v_{th} = thermal velocity

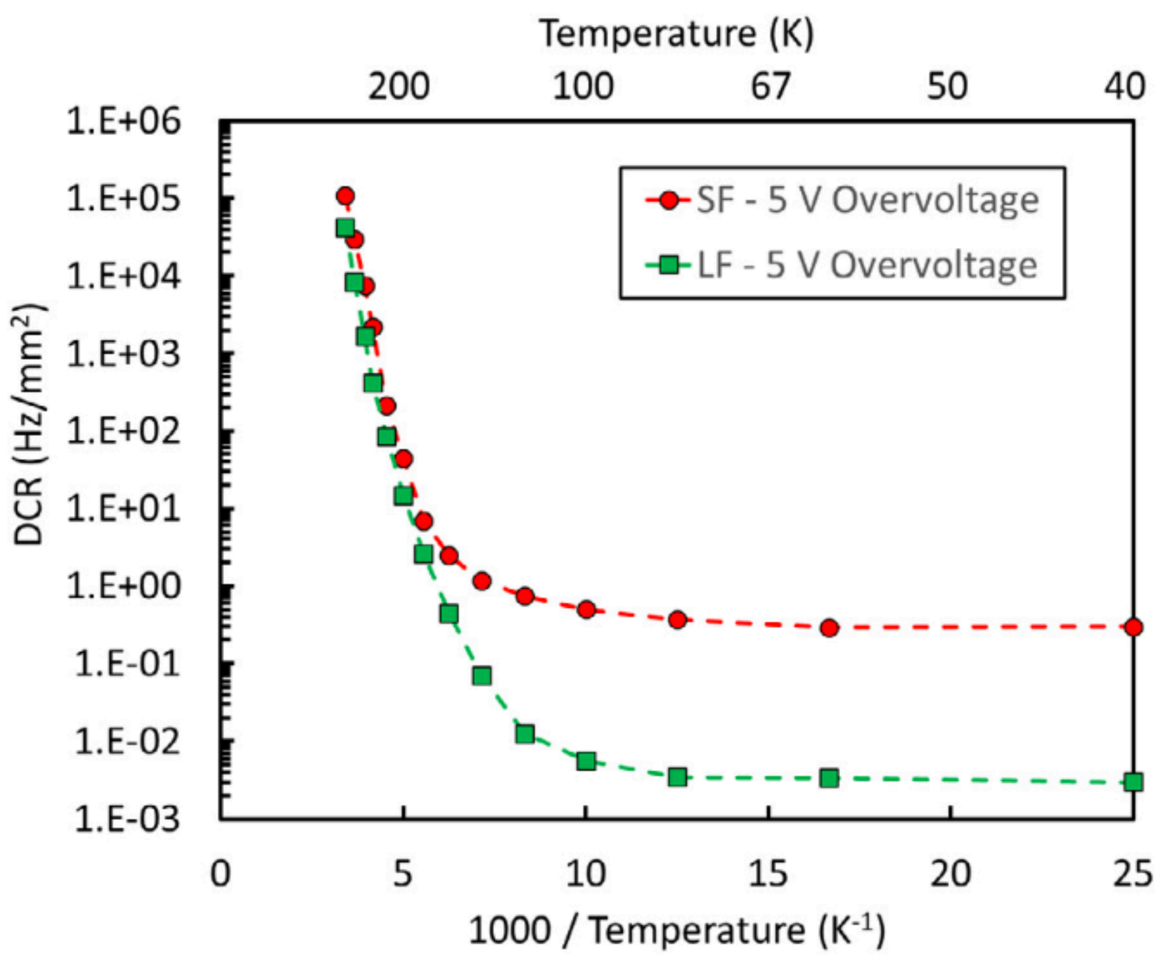
$$G = \frac{(1+\Gamma)\, n_i}{\tau_{g0}}$$

Γ "boost" by the field



Key issues:

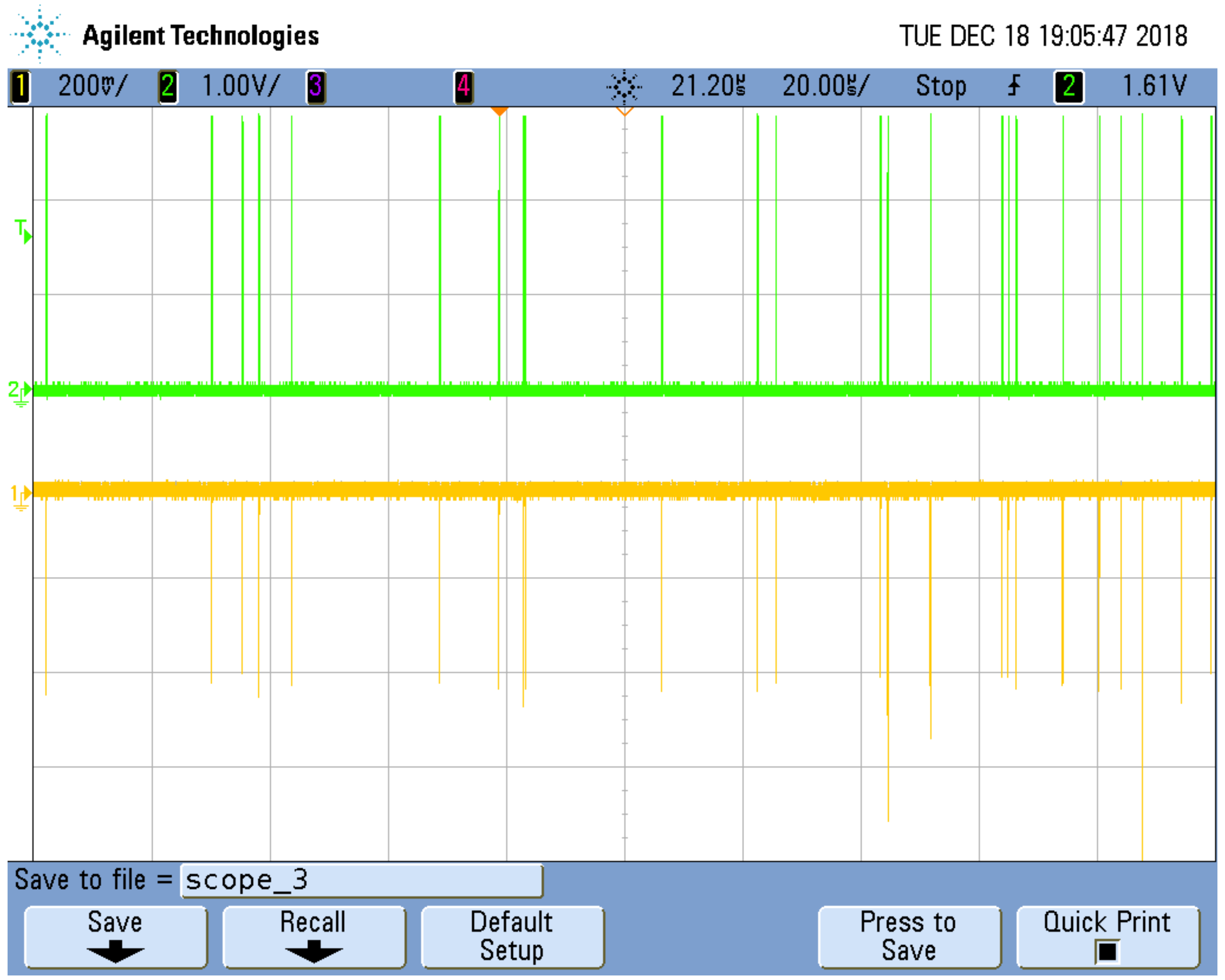
- **in SiPM, the Dark Count Rate is O(1 KHz)/cell, 50 μm pitch (it may be higher for SPAD arrays in CMOS technology)**
- provided the nature of the Dark Pulses, we have a significant dependence on Temperature



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

The essence of : RANDOM POWER

turning unpredictable "Dark Pulses" into bits:



1. tagging & time stamping the occurrences of the random pulses

2. analysing the time series of the pulses:

- Italian Patent granted in Sept., 2020
- EU patent granted in April 2022
- extension in US, China, Korea, Jp ongoing

WHERE ARE WE NOW

The MINIMUM VIABLE PRODUCT [MVP], the progenitor of a class of Quantum Random Bit Generators:

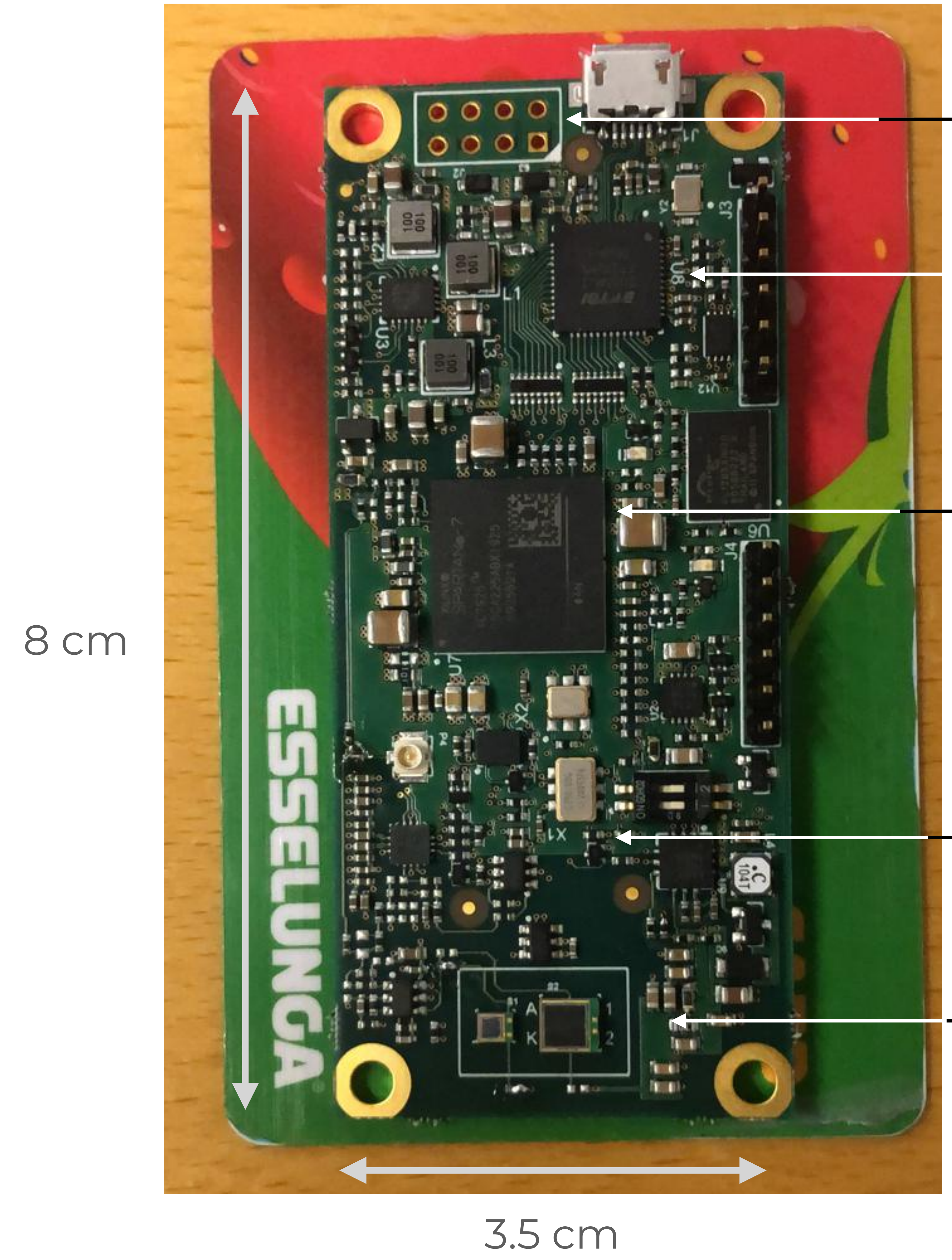
Qualified according to the NIST standards
(National Institute of Standard & Technology)

Developed thanks to the **seed capital [100 000 €]** granted by

ATTRACT

https://attract-eu.com

which selected Random Power as one of **170** "breakthrough projects" **out of 1211 submissions** - **Phase 1 (2019-2020)**



Upon request, bits can be routed to pins

FTDI chip for data routing on the USB (FT232HQ - Single Channel Hi-Speed USB to Multipurpose UART/FIFO IC

FPGA embedding a proprietary TDC and implementing the bit extraction + real-time sanity checks + SHA256 (Spartan-7 Family 23360 Cells 800MHz 28nm Technology 1V 225-Pin CSBGA Tray)

Amplification & discrimination (LTC6268HS6-10#TRMPBF amplifier by Linear technologies + ADCMP605BCPZ LVDS comparator by Analog Device)

Single generator (either 1x1 mm^2 or 3x3 mm^2 - **Bit rate for the smaller area device: O(100 kbps)** - operated with overvoltage stabilisation against Temperature variations 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, currently being qualified through the NIST and TESTU01 suites.**

Preliminary results over 250 Gb show that the stream looks extremely "white", essentially with no failures on the raw data:

- **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

WHAT'S NEXT

$\approx 10^5$ €	$\approx n \times 10^5$ €	$\approx 2\text{-}3 \times 10^6$ €
[2021-2022]	[2022-2024]	[2022-2025]

Time & Money

- **GO TO THE MARKET and EXPLOIT THE MVP**

N&G CONSULTING

LIFT GIVING IDEAS THE HIGHEST VALUE

- Get official certifications
- Enhance IP protection
- SEEK FOR FUNDING

- GO MACRO & SECURE:

- development of "agnostics" applications

RNG replacement

- GO MICRO & SECURE:

- High End applications [e.g. FULL HOMOMORPHIC ENCRYPTION] [prioritized after the end of the technology development]

RANDOM POWER

Phase II:

- submission Sept. 20th, 2021
- notification of approval Jan. 31st, 2022
- **Duration: May 2022 to August 2024**
- funding: 2 MEUR
- selection & competitiveness:

1211 submissions in Phase 1 ➜ 170 approved ➜ 87 submissions for phase II (68 R&D proposals) ➜ 18 R&D approved

Total proposals 87

Proposals received

	TOTAL FUNDING	SUBMITTED PROPOSALS
R&D&I Projects Thematic call	€25M	68
Academy call	€2M	10
Socioeconomic Studies call	€1M	9

combined success rate: 18/1211 = 1.5%, so we did well!

RANDOM POWER

ATTRACT

Our consortium:

UNIVERSITAS STUDIORUM INSUBRIAE

leading party

FONDAZIONE BRUNO KESSLER
FUTURE BUILT ON KNOWLEDGE

AGH

NAGRA
KUDELSKI GROUP

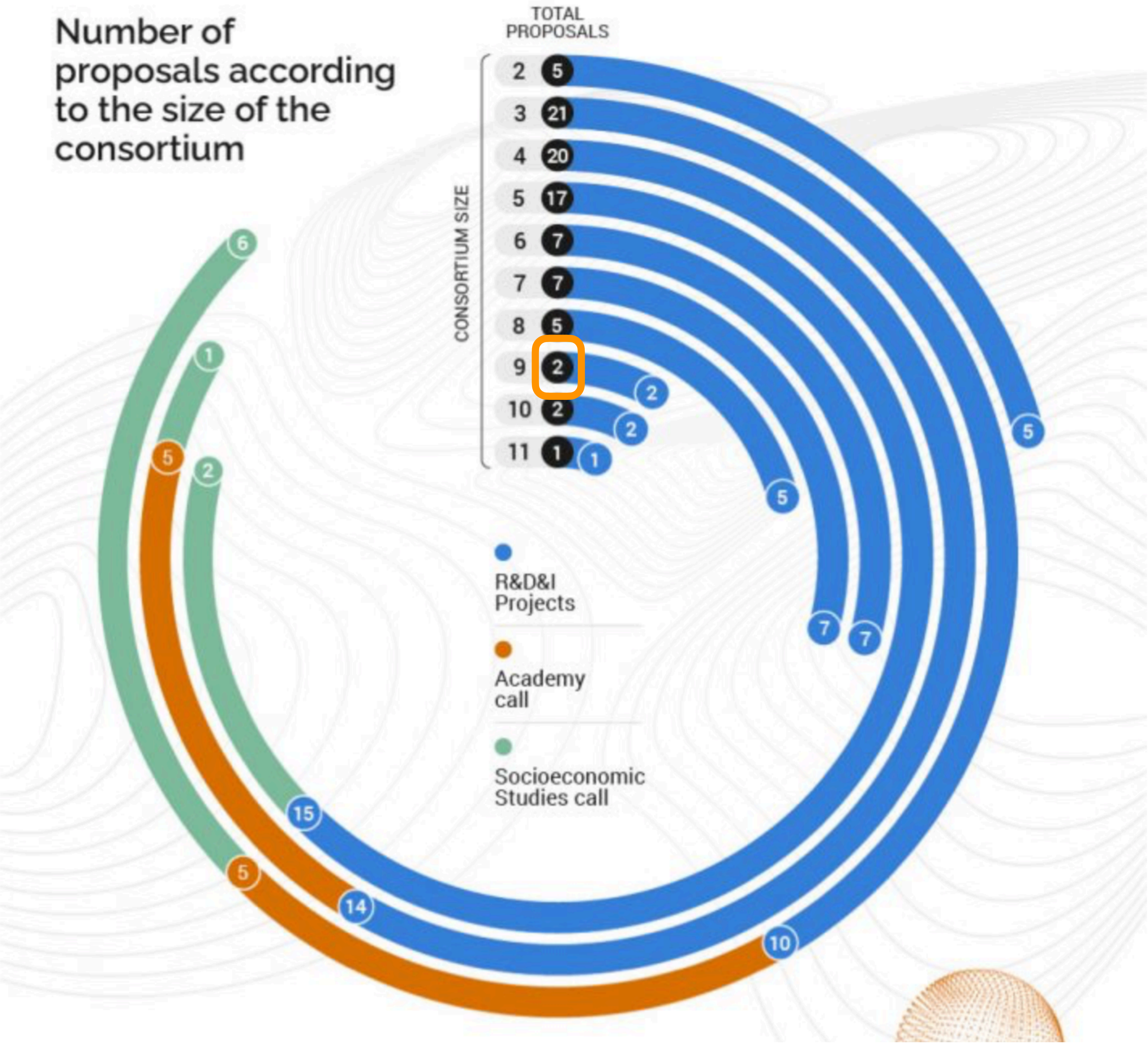
E4 COMPUTER ENGINEERING

SECO

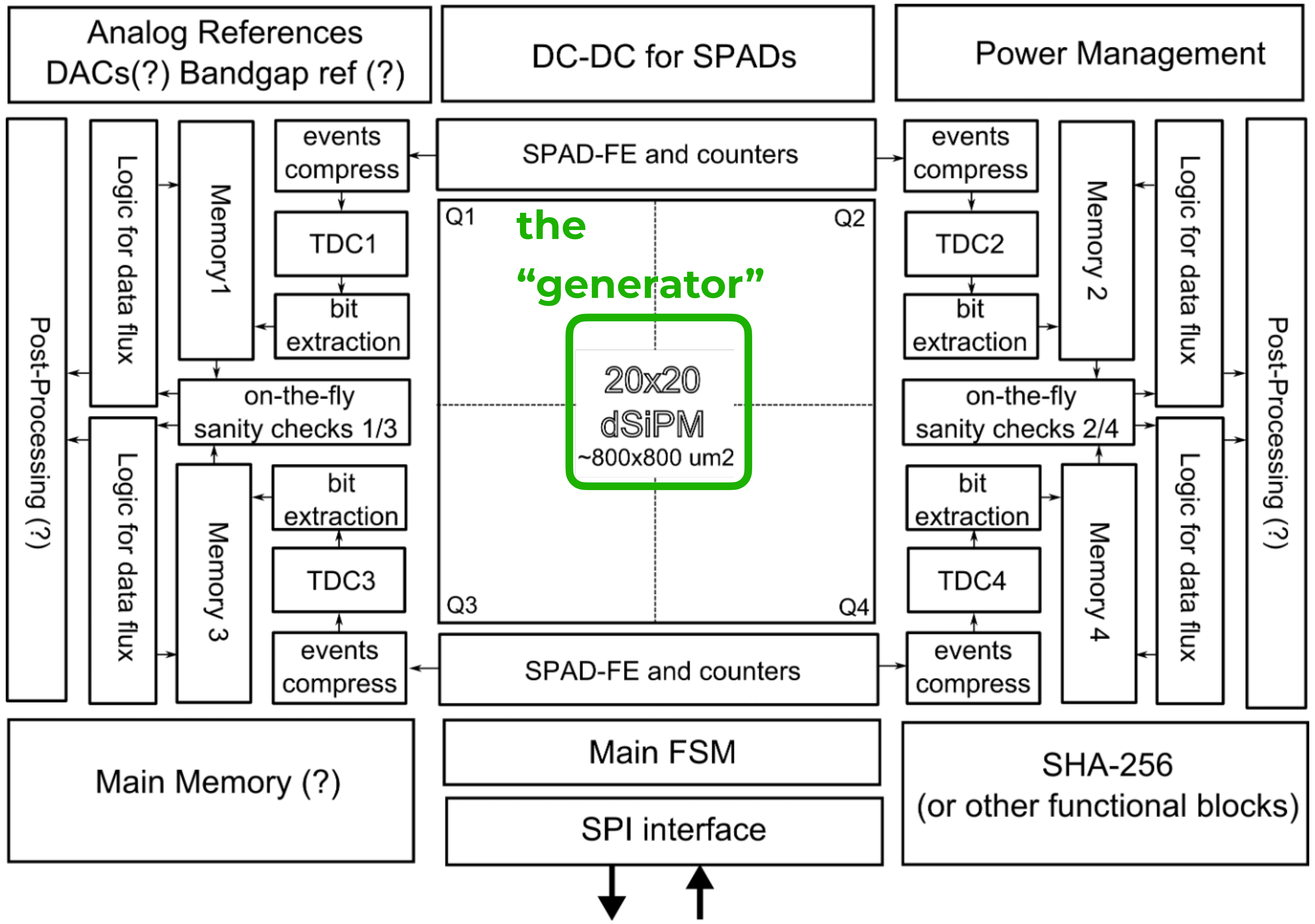
imasenic

weeroc

RANDOM POWER

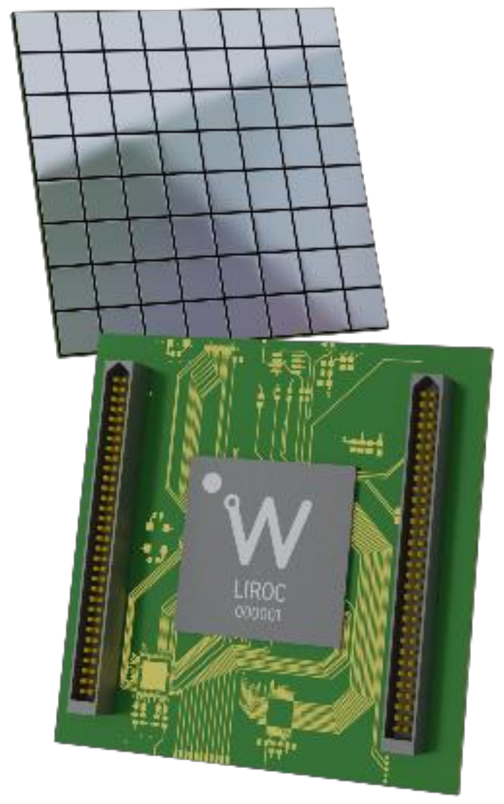


Our main goals:



- **design a FIPS-compliant ASIC embedding a SPAD array in standard CMOS technology**

- **design a scalable multi-generator system based on an array of SiPM and a LIROC front end ASIC by LIROC**



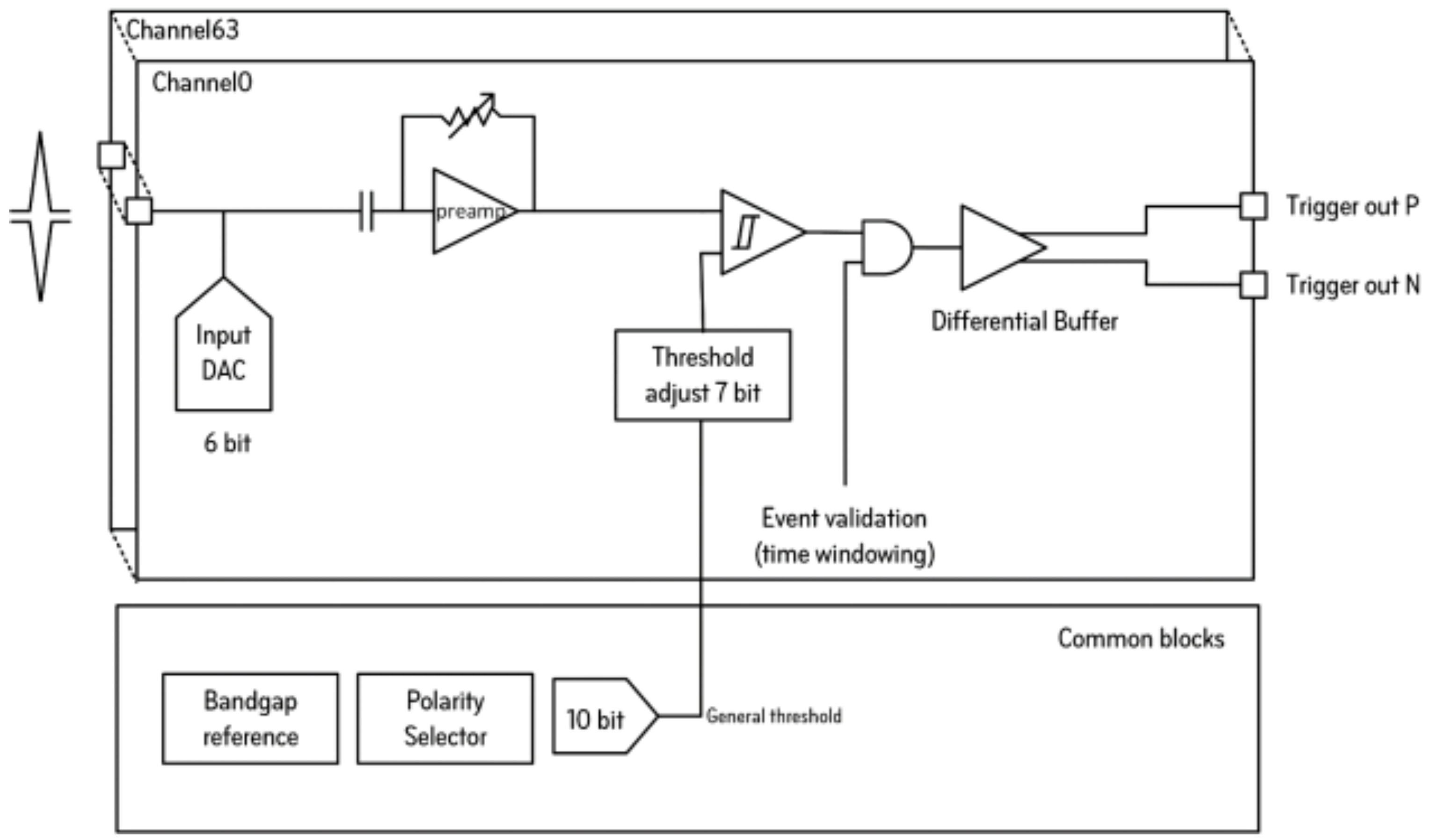


Table 2 - LIROC main features and performances

Detector Read-Out	SiPM, SiPM array
Number of Channels	64
Signal Polarity	Positive or Negative (selectable ASIC-wise)
Sensitivity	Trigger on 1/3 of photo-electron
Timing Resolution	Better than 20 ps FWHM on single photo-electron Better than 5ns double-peak separation on single photo-electron
Dynamic Range	Over 100MHz photon counting rate
Packaging & Dimension	BGA 20x20 mm2 Flip-Chip low inductance packaging technology

Power Consumption	210mW (TBC) – Supply voltage : 1.2 V
Inputs	64 analogue inputs with independent SiPM HV adjustments
Outputs	64 LVDS triggers
Internal Programmable Features (I2C)	64 HV adjustment for SiPM (64 x 6 bit), trigger threshold programming (10bits), 64 x 7 bit channel-wise threshold adjustment, ASIC-wise polarity selector, preamp gain adjustment, individual trigger masking and cell powering.

RANDOM POWER

www.randompower.eu

Established in June 2021

ATTRACT

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

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

CONTACT US at:

- massimo.caccia@randompower.eu
- marcello.esposito@randompower.eu
- lorenza.paolucci@randompower.eu