

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



the value of unpredictability

Massimo Caccia

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

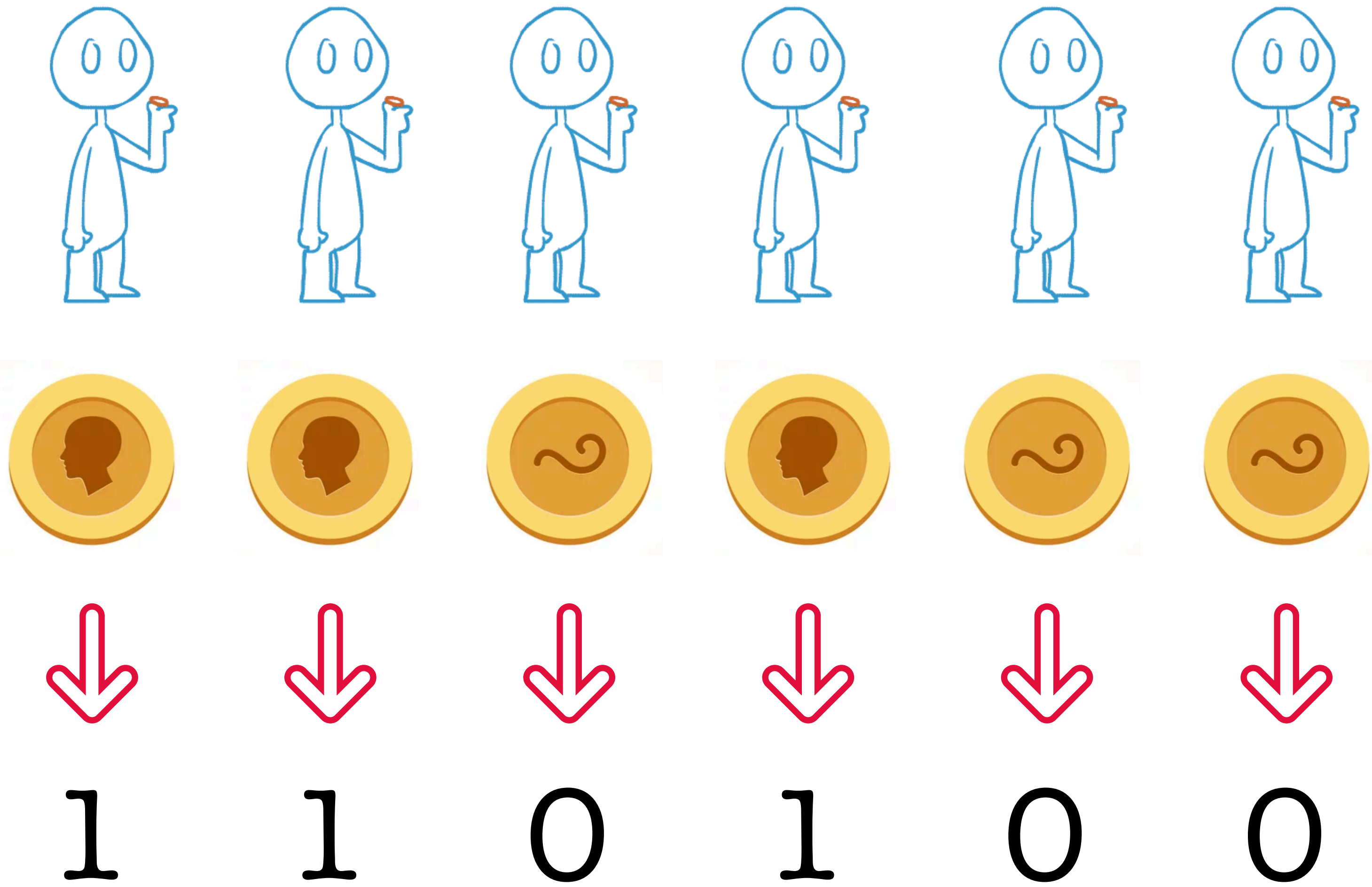
massimo.caccia@randompower.eu



HKUST-IAS program in Particle Physics 2024
Hong Kong, Jan. 24th



FALLING WALLS VENTURE



WHAT FOR?

there is definitely a hype about Random bit streams, not only for **crypto** but also for **gaming, virtual reality, Monte Carlo simulations, IoT, Satellite communication & control** and notably **Privacy Preservation Procedures**



“Differential privacy makes it possible for tech companies to collect and share aggregate information about user habits, while maintaining the privacy of individual users.”

► [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

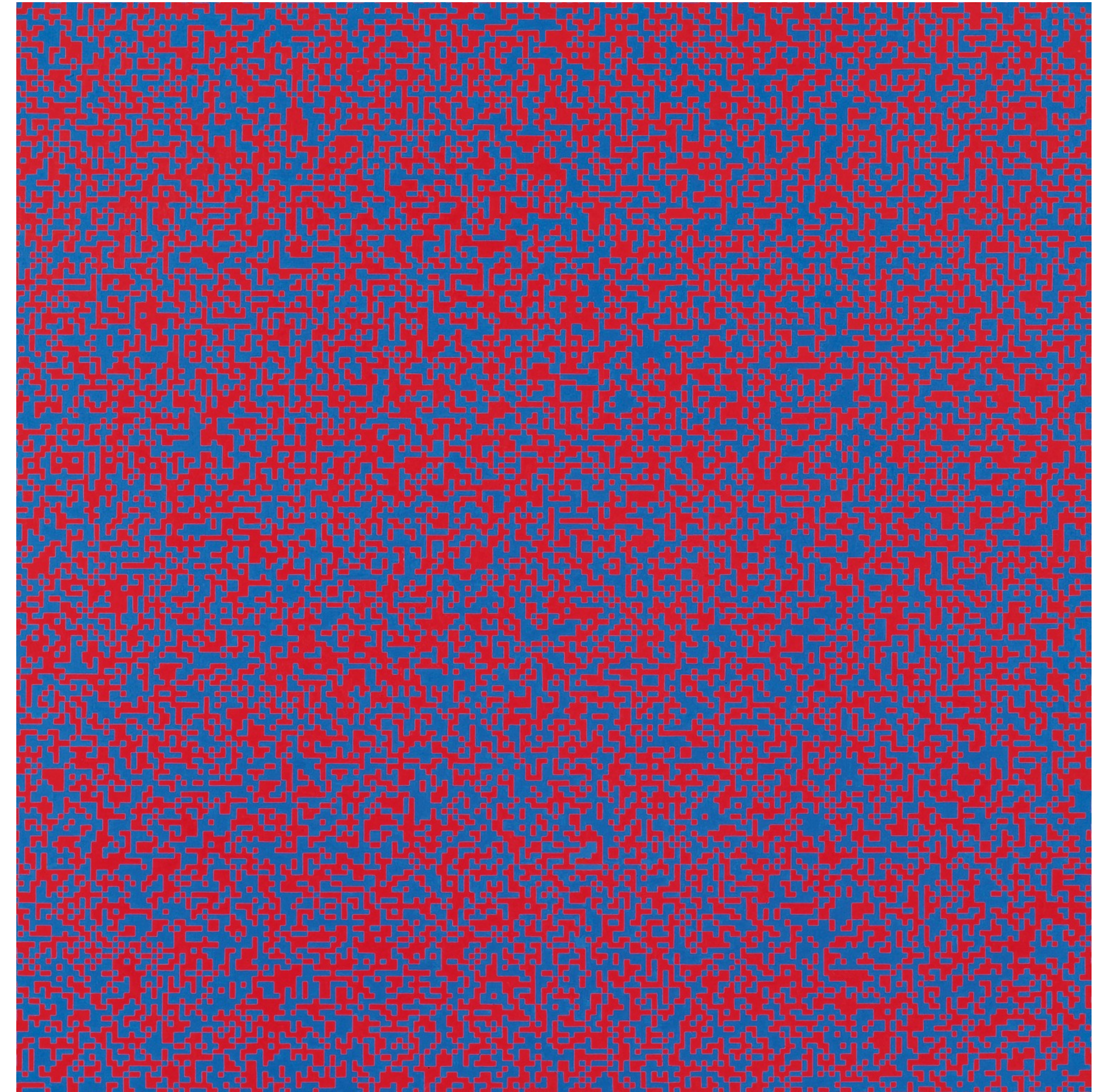
2 . t h e e s s e n c e o f r a n d o m n u m b e r g e n e r a t i o n :

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

$$x_n \equiv ax_{n-1} + b \pmod{m}$$

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

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

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

Two Years of Broken Crypto

Debian's Dress Rehearsal

2006



HOW DO WE DO IT?

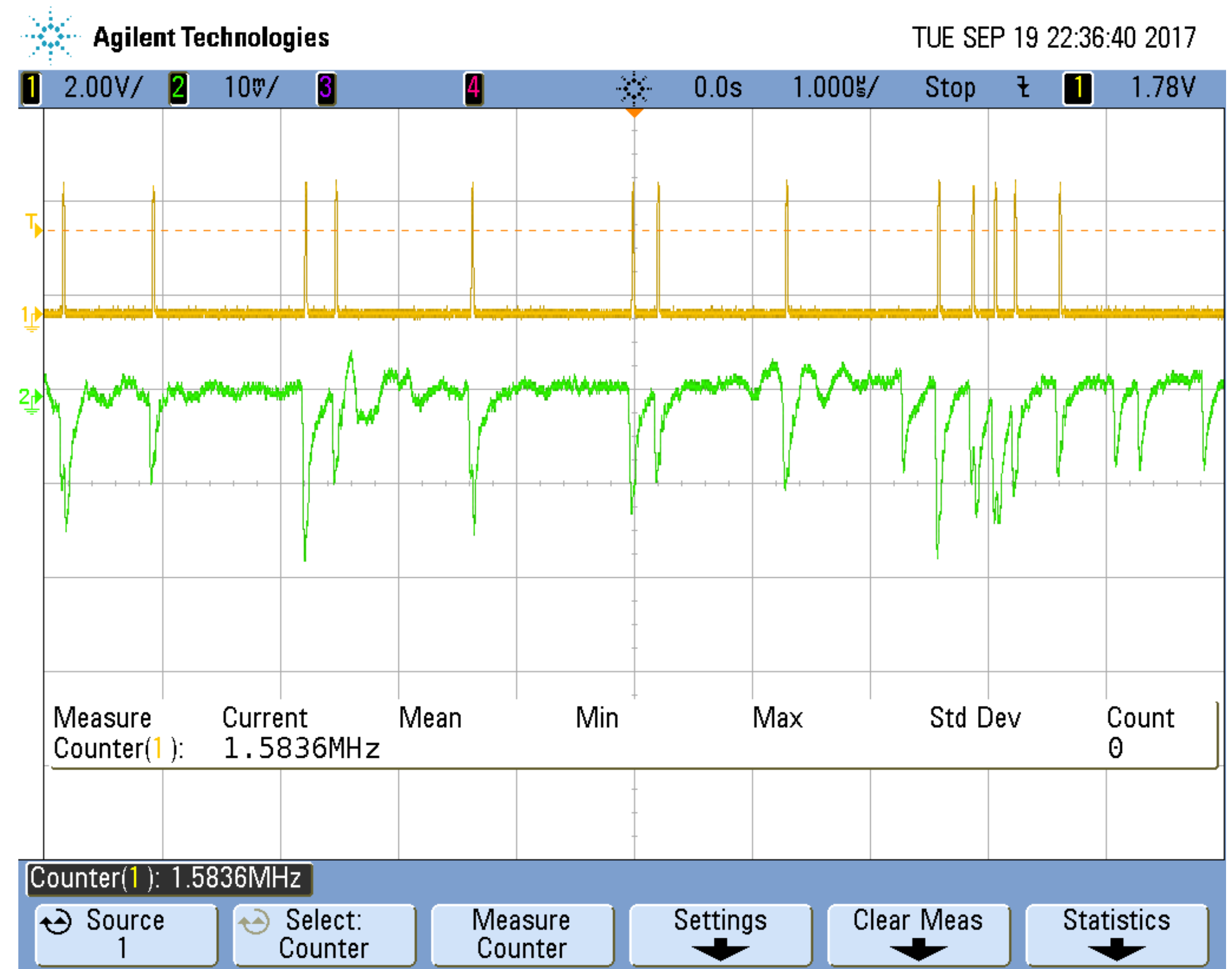
Inspired by Forrest Gump, we say:

RADIOACTIVE IS AS 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

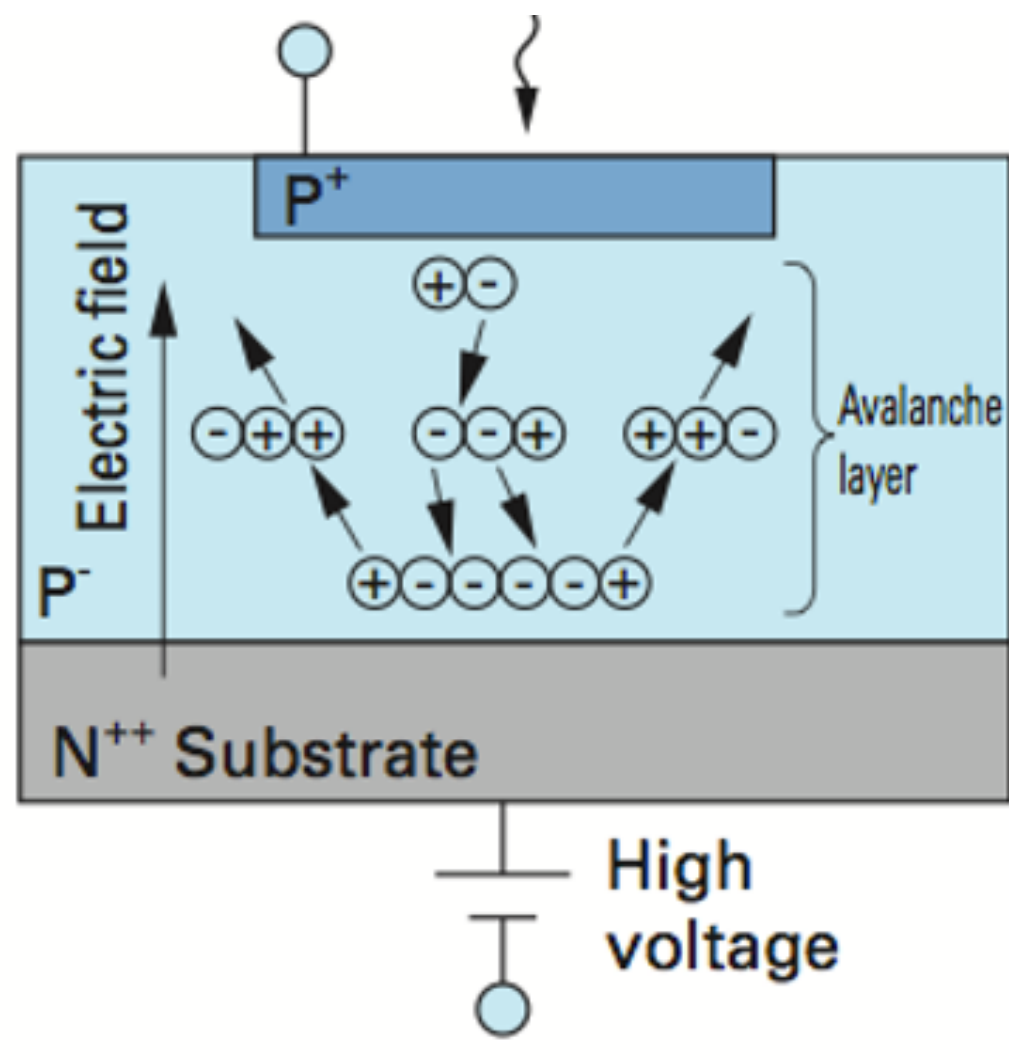
The idea behind **RANDOM POWER** is to replace a radioactive source with something safer, more handy, cost effective, simple, robust, providing sequences of pulses mimicking radioactive decays.

► The generator, an array of Single Photon Avalanche Diodes, namely p-n junctions operated beyond the breakdown voltage:

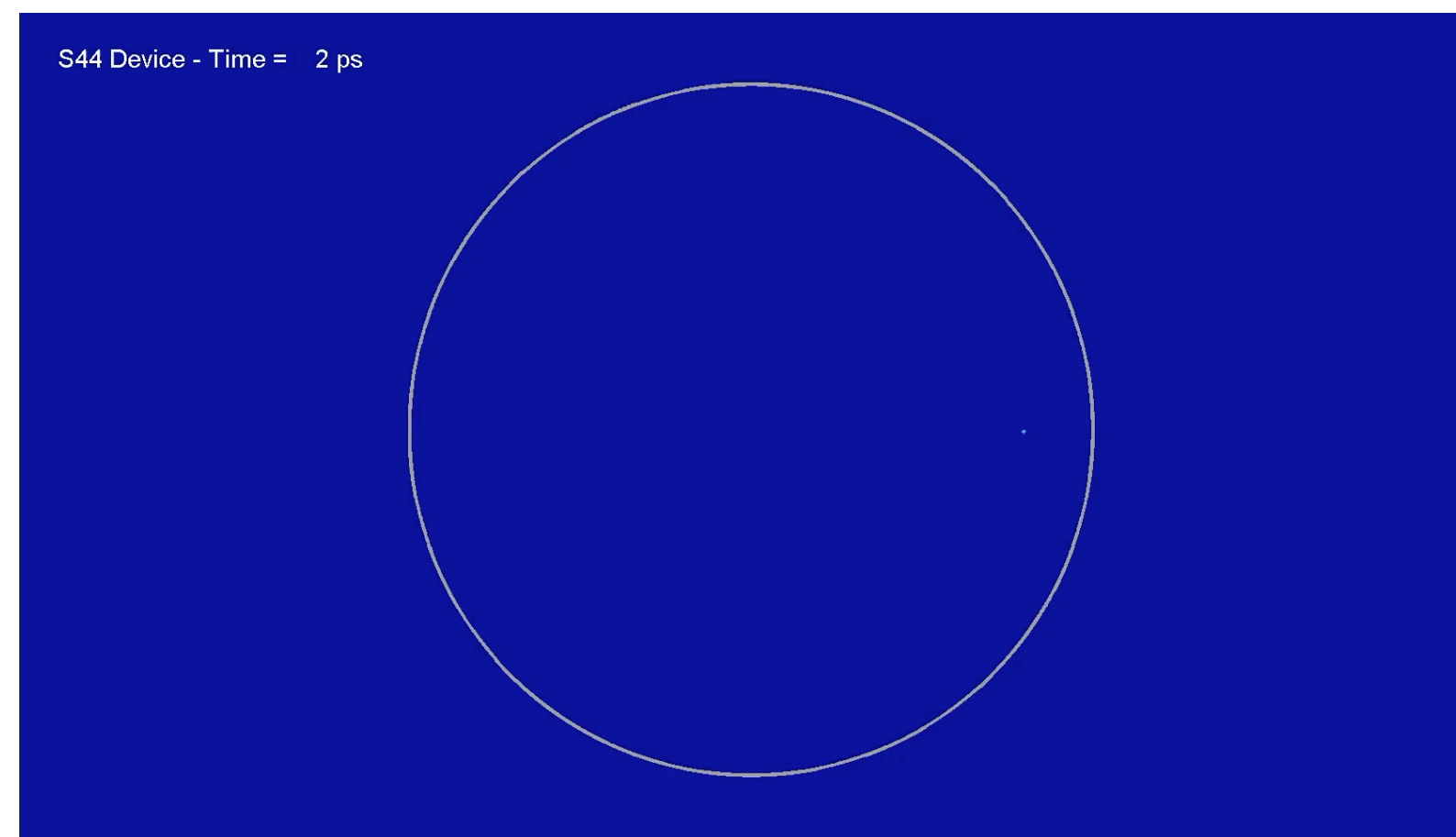
A pioneering development by Prof. S. Cova at Politecnico di Milano

Cova, S., Ghioni, M., Lacaita, A. L., Samori, C., and Zappa, F. "Avalanche photodiodes and quenching circuits for single-photon detection", Applied Optics, 35(12), 1956—1976 (1996)

The essence of a cell



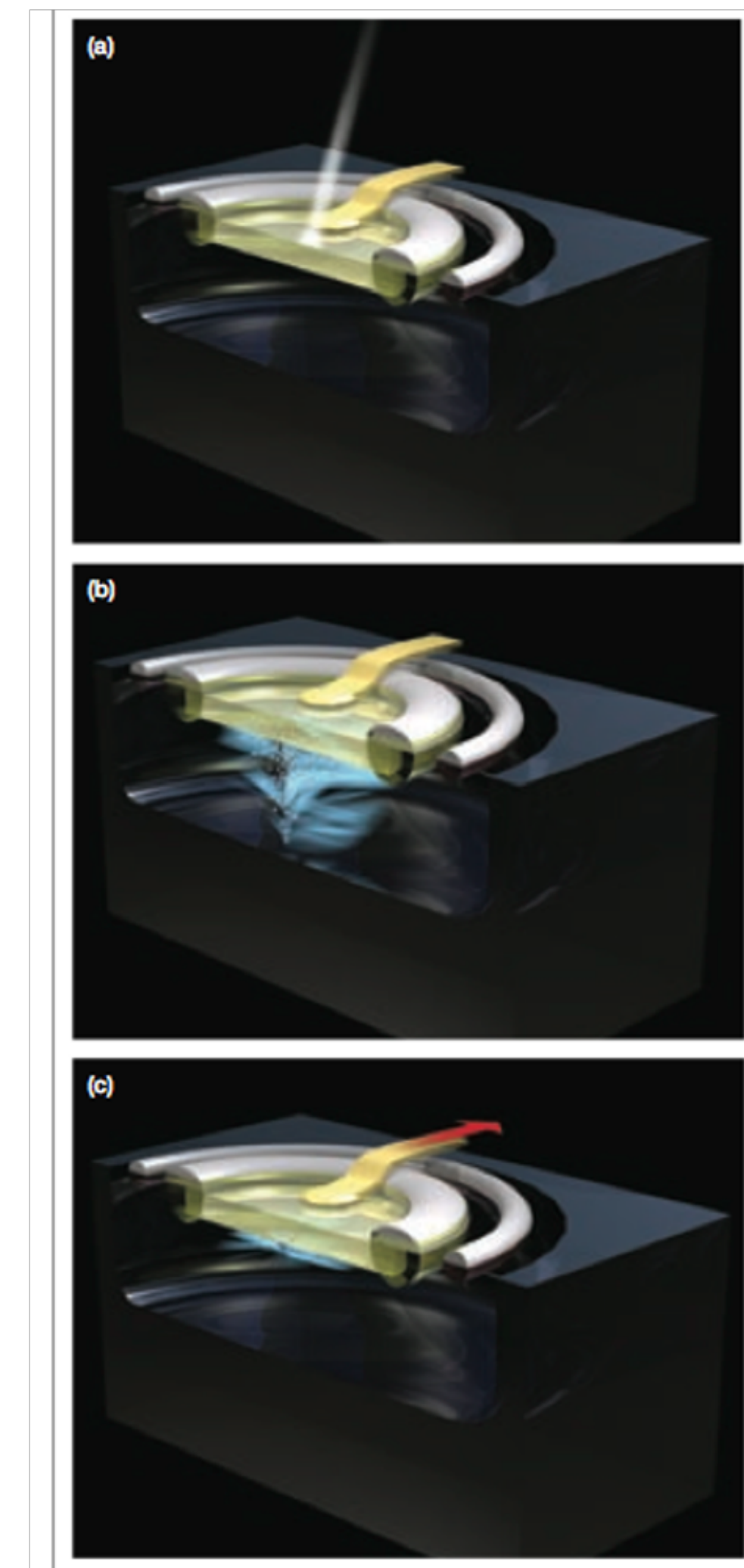
Simulation of an avalanche development



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

Multiplication by about 1 000 000

- Very shallow p-n junction → ~ 1 μm
- High electric field → > 3 x 10⁵ V/cm
- Mean free path → ≈ 0.01 μm



E. Charbon & S. Donati, OPN Optics & Photonics News, February 2010

► **The name of the game:** charge carriers can be generated “spontaneously”, also when no light is illuminating the sensor

A lesson from the past, when this was known since the early days of the Silicon technology development:

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

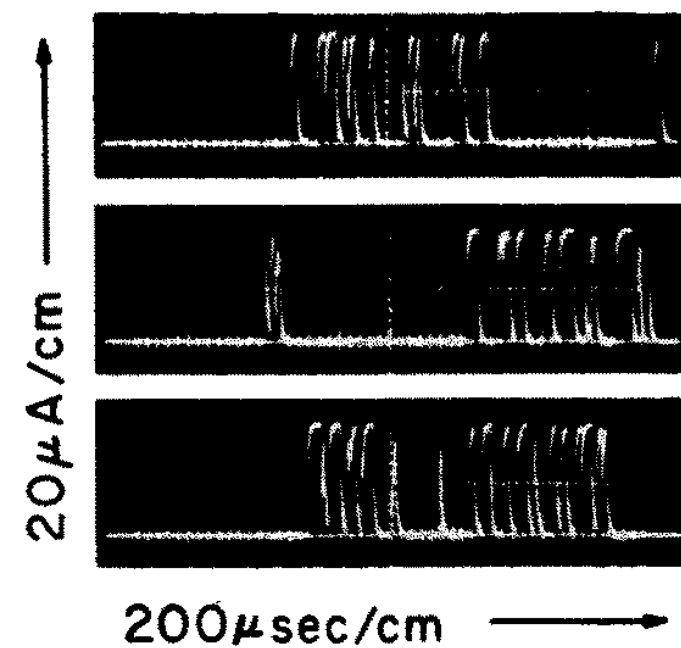


FIG. 5. Avalanche current as a function of time at low temperatures. The group character of the avalanche pulses is obvious.

from paper 3

Avalanche Breakdown in Silicon

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

1

Model for the Electrical Behavior of a Microplasma*

ROLAND H. HAITZ†
Shockley Laboratory, Clevite Corporation Semiconductor Division, Palo Alto, California
(Received 5 November 1963)

2

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.

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)

3

► **The name of the game:** charge carriers can be generated “spontaneously”, also when no light is illuminating the sensor, by quantum tunnelling

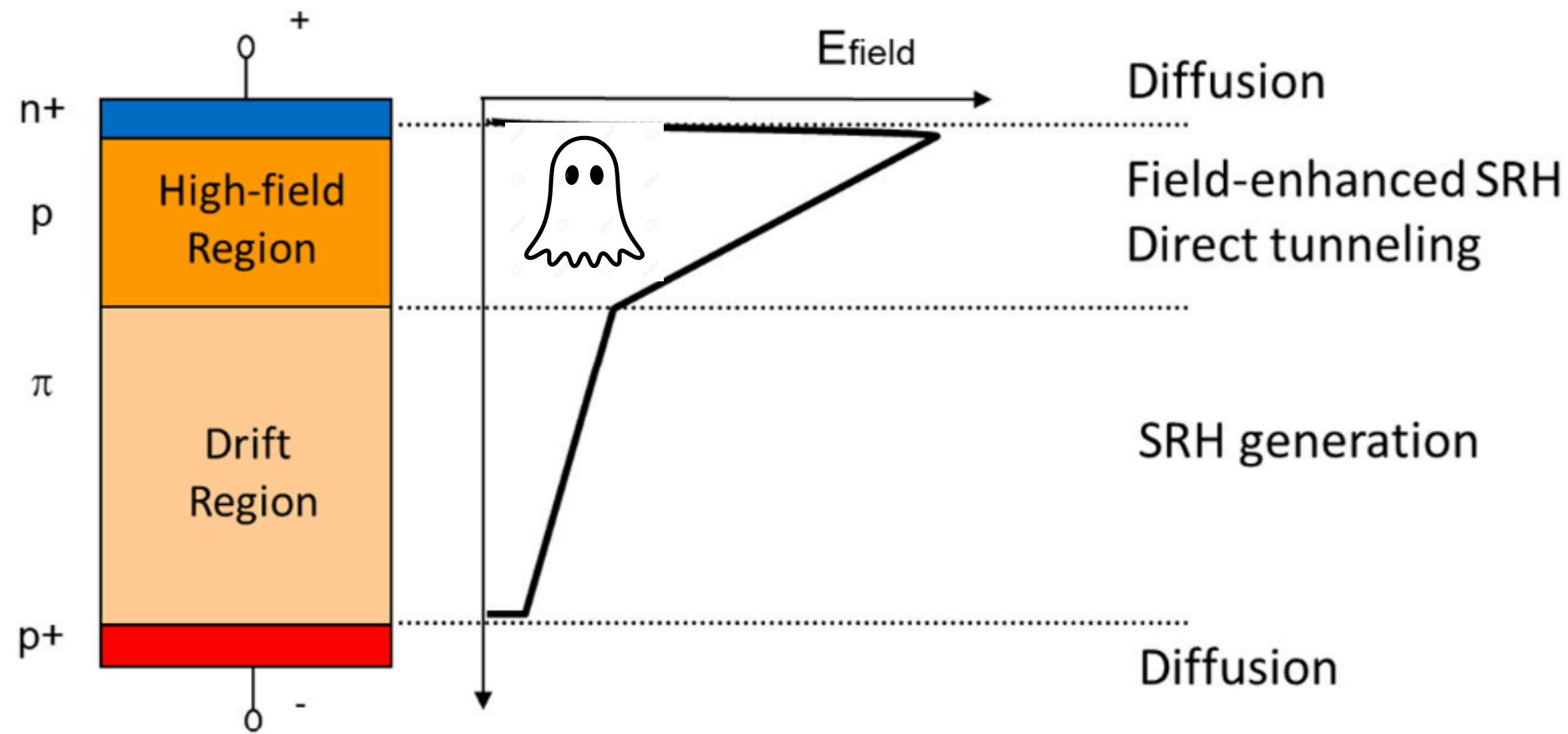


Fig. 8. Representation of the different sources of primary dark events and their location in the SPAD structure.

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

Key issues:

- * the 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
- * forget-me-not: the Over-voltage is affecting the triggering probability

Thermal generation of carriers by states in the bang-gap

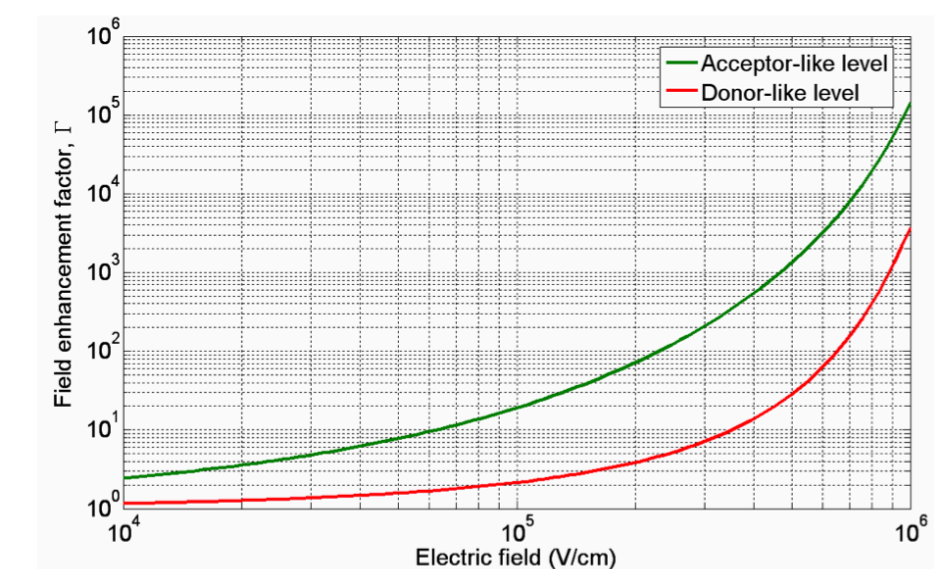
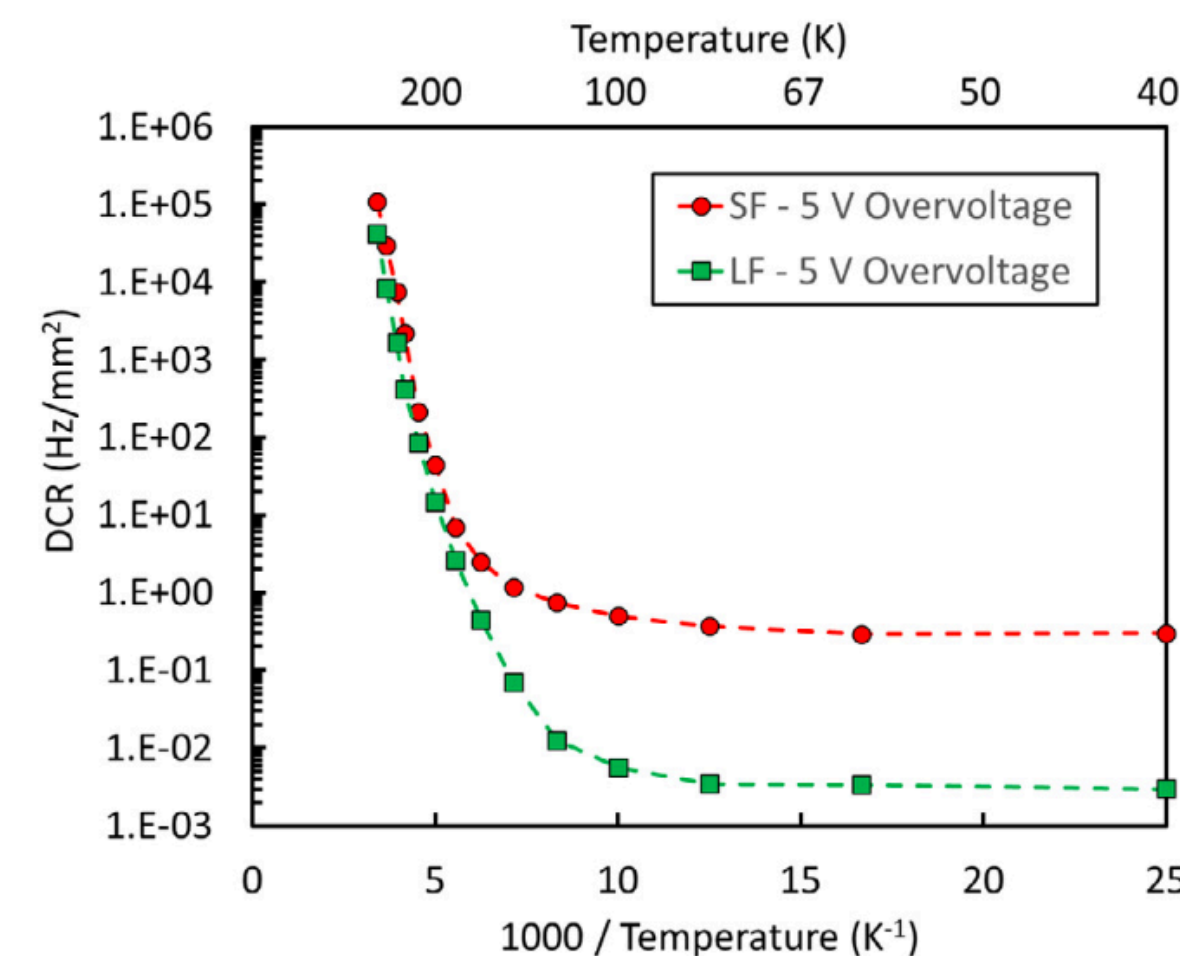
(Shockley-Read-Hall statistics), where trapping and de-trapping is increased by the high electric field in the junction. The

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
- σ = trapping cross section
- v_{th} = thermal velocity

$$G = \frac{(1 + \Gamma) n_i}{\tau_{g0}} \quad \Gamma \text{ "boost" by the field}$$



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

3 . t h e R a n d o m P o w e r p r i n c i p l e :

This is the essence of

RUNDOM POWER

- Italian Patent granted in Sept. 2020
- EU patent granted in 2022
- first iteration in the US and Japan
- still in the examination phase in China & South Korea (since April 2021)

A genuine **Q(quantum)-True Random Number Generator**, namely **a Quantum Coin Flipper**

providing virtually endless streams of

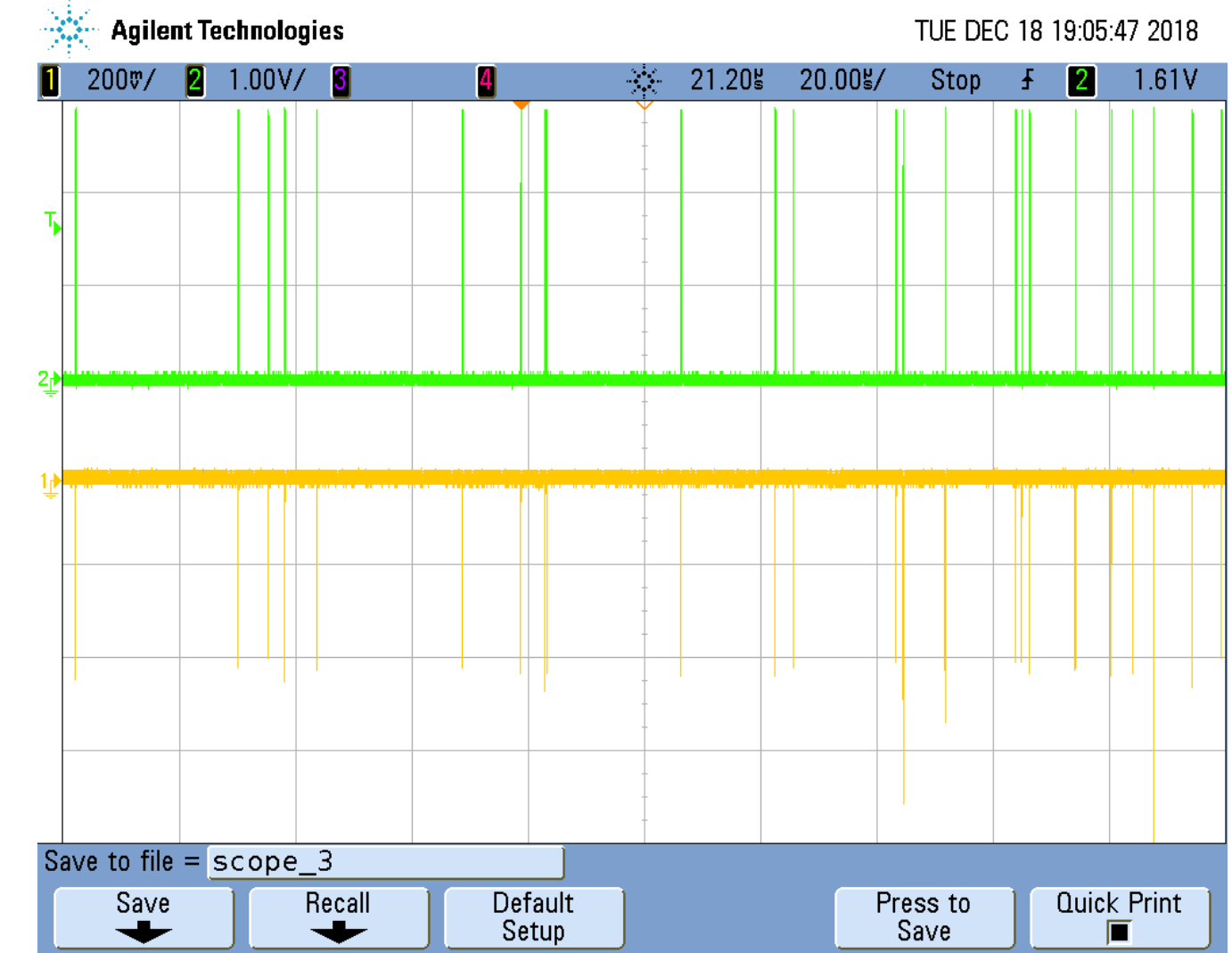
RANDOM BITS → CRYPTOGRAPHIC KEYS

shielded against any bias by the fundamentals of Quantum Mechanics



► The essence of Random Power: turning unpredictable “Dark Pulses” into bits

1. tag & time stamp the occurrences of the random pulses



2. analyse the time series of the pulses:



*bit 1: Δt_{12} vs Δt_{34}

*bit 2: Δt_{23} vs Δt_{45}

*bit 3: Δt_{56} vs Δt_{78}

*bit 4: Δt_{67} vs Δt_{89}

→ Easy to see that ANY systematics in “time stamping” (e.g. dead time, granularity and phase wrt a continuous clock) implies a possible systematics in the bit generation

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



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

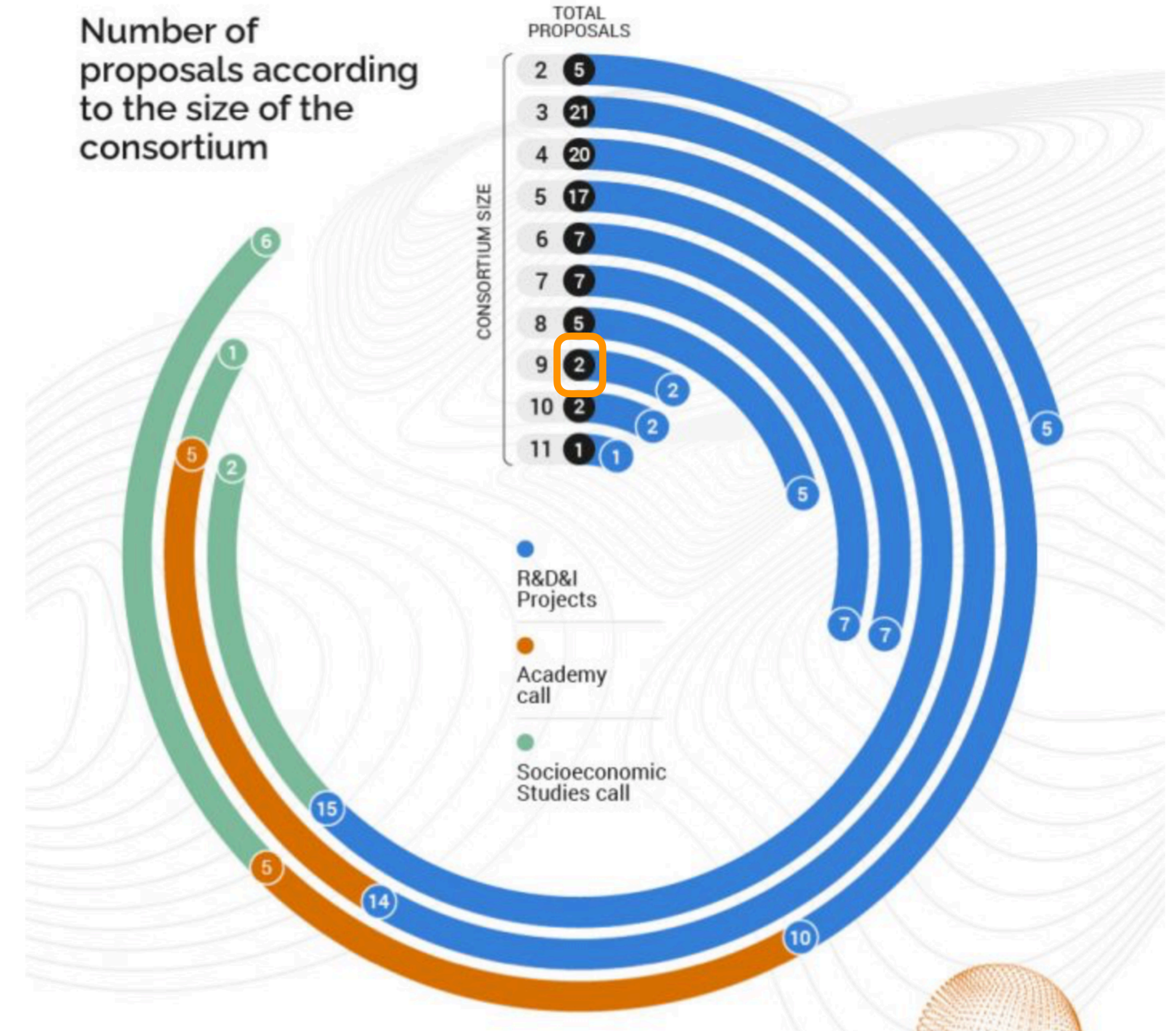
combined success rate: $18/1211 = 1.5\%$, so we did well!



Our consortium:



leading party

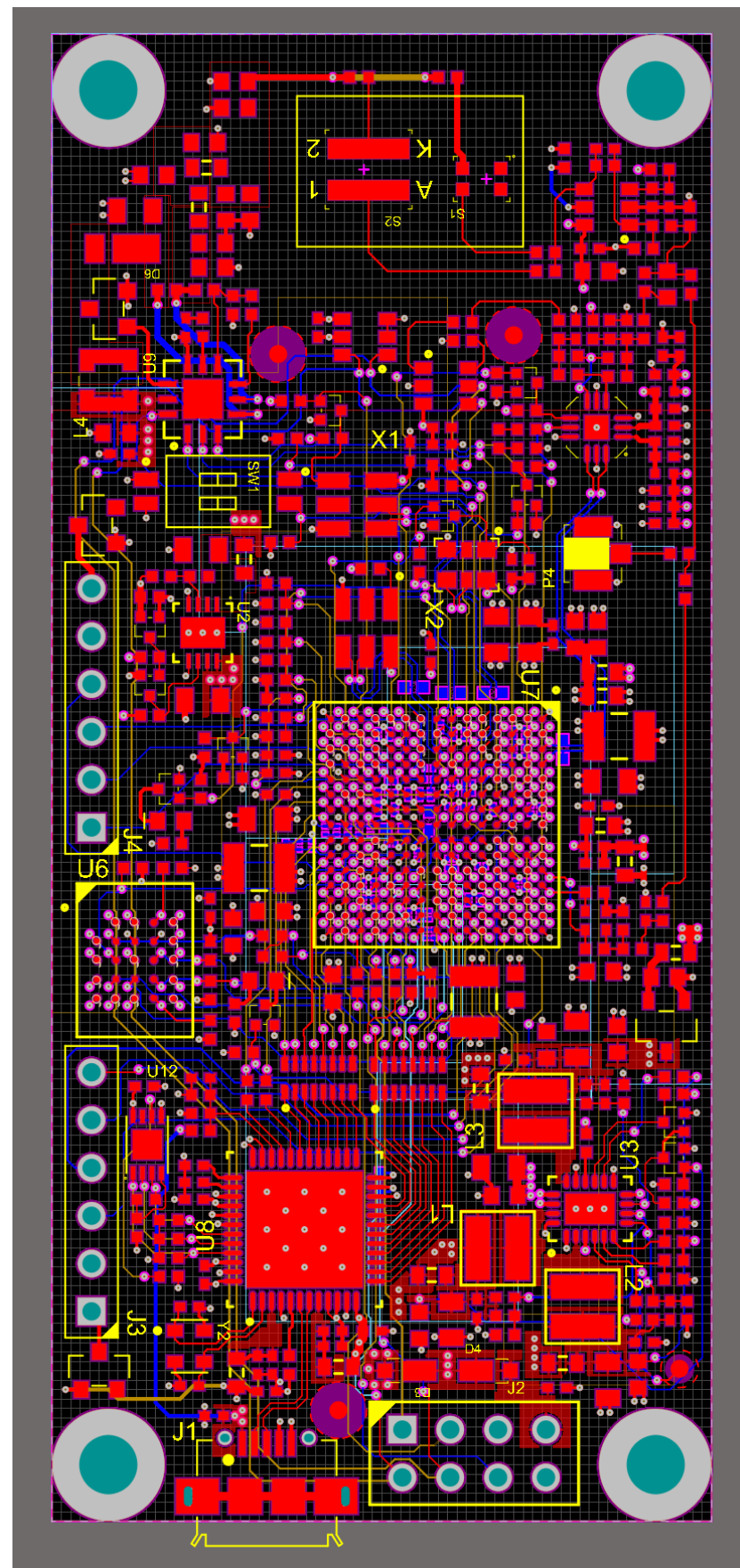


18 man-years dedicated to the project



4 . s t a t e - o f - p l a y :

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:	<ul style="list-style-type: none"> • Firmware implemented Real-Time sanity checks (MONOBIT and RUNS) • Auxiliary post-processing through a SHA256 function
State of development:	<ul style="list-style-type: none"> • Completed • Full qualification of 2 Tb through the NIST and TESTU01 protocols • Single board control through a GUI or mini-farm control implementing also the NIST DRBG procedure (SP800-90 A,B,C)

THE SINGLE GENERATOR BOARD



8 cm

3.5 cm

Upon request, bits can be routed on pins

FTDI chip for data routing on the USB

FPGA embedding a proprietary TDC and implementing the bit extraction + real-time sanity checks (MONOBIT&RUNS) + conditioning function (SHA-256)

Amplification & discrimination

Single generator (either 1x1 mm² or 3x3 mm² - Bit rate for the smaller area device: O(100 kbps) - operated with overvoltage stabilisation against Temperature variations

4 . s t a t e - o f - p l a y :

```

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 69 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.

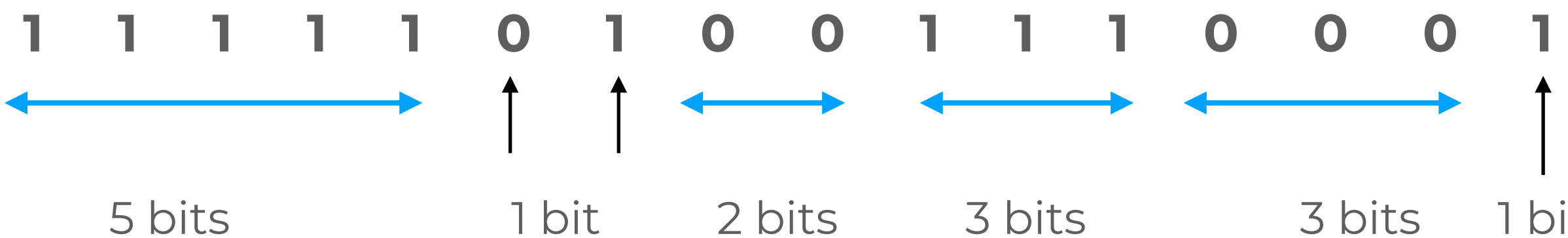
▶ A SHA256 vetted conditioning function firmware implemented

▶ 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:

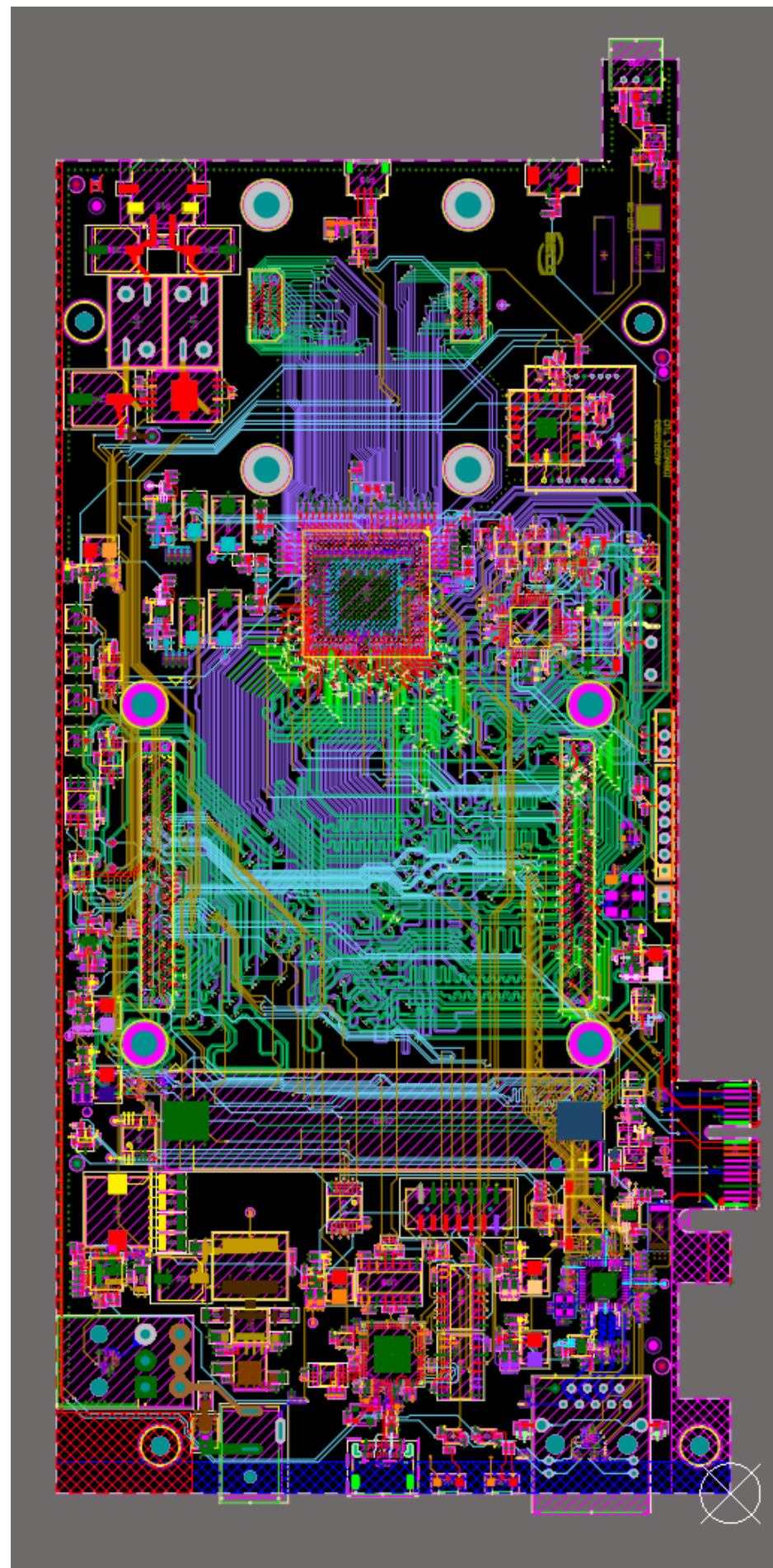
1 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1

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

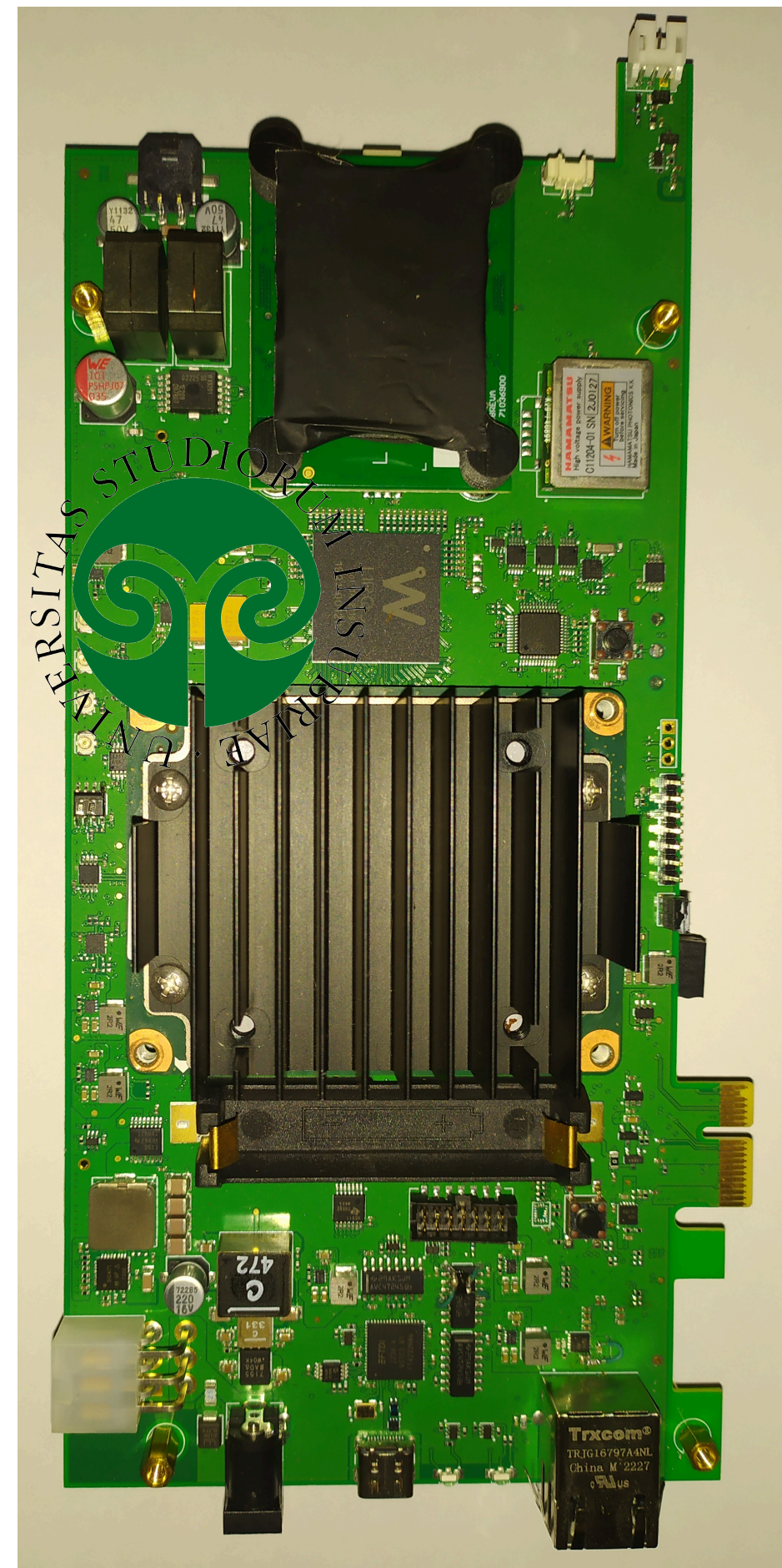


4 . s t a t e - o f - p l a y :

THE 64 GENERATORS BOARD



31 cm



11 cm

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 **(O(12W))**

I/O:

Eth or PCI-Express

Power supply:

12V, 8A

Power consumption:

< 100 W **(dominated by the Peltier cooler)**

Encryption

Yes (AES-256)

Specific Features:

- Firmware implemented Real-Time sanity checks (MONOBIT, RUNS, Adaptive proportion test, Repetition Count Test)
- Auxiliary post-processing through a SHA256 function
- Interface through the Trusted Execution Environment
- Temperature control through a Peltier cooler
- FIPS-140-3 compliant by design
- Prototype under test
- Product grade design expected by June 2024

State of development:

Goal of the



Phase 2 project (May 2022-Fall.2023)

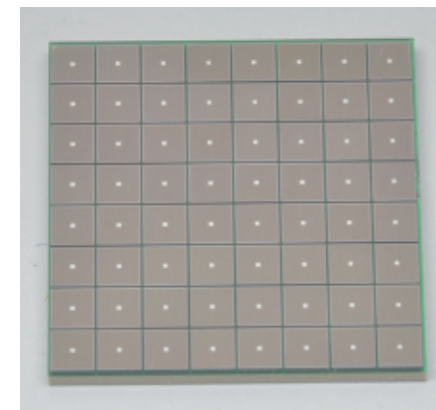
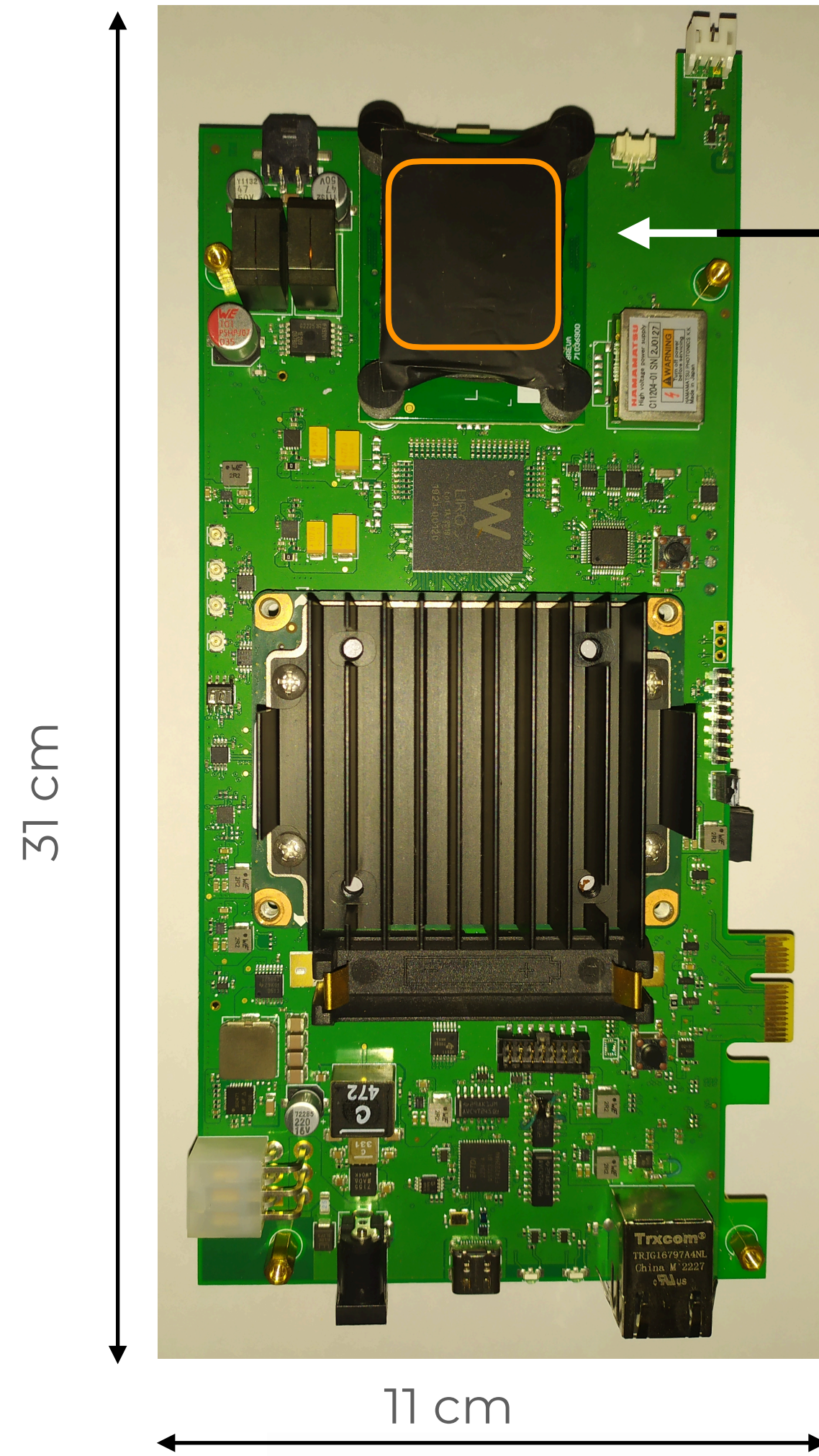
▶ **v1.0 delivered in July 2023, qualified**

▶ **v2.0, product grade, expected in May 2024**



4 . s t a t e - o f - p l a y :

THE 64 GENERATORS BOARD



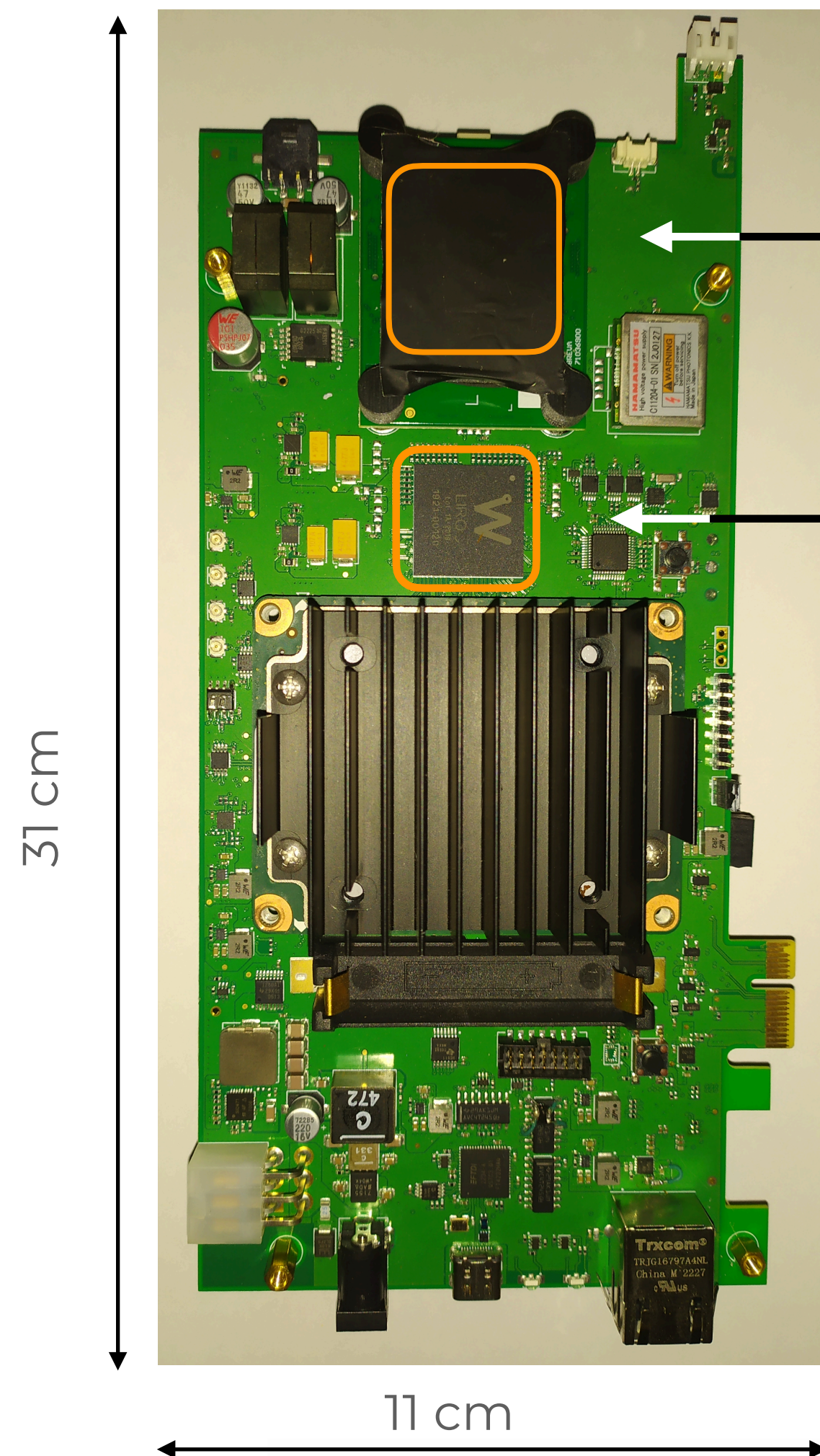
S13361-2050AE-08 by HAMAMATSU
8x8 sensors on each unit

Electrical and optical characteristics (Typ. Ta=25 °C, Vover=3 V, unless otherwise noted)

Parameter	Symbol	Value	Unit
Spectral response range	λ	320 to 900	nm
Peak sensitivity wavelength	λ_p	450	nm
Photon detection efficiency $(\lambda - \lambda_p)^{-1}$	PDE	40	%
Dark count*5	Typ.	300	kcps
	Max.	900	
Terminal capacitance	Ct	140	pF
Gain	M	1.7×10^6	-
Breakdown voltage	VBR	53 ± 5	V
Recommended operating voltage	Vop	VBR + 3	V
Vop variation between channels in one product	Typ.	0.1	V
	Max.	0.3	
Temperature coefficient of recommended operating voltage	ΔTV_{op}	54	mV/°C

Expected bit rate: $0.45 * 300 * 64 = 9$ Mbps (I believe it can be pushed to 32 Mbps)

THE 64 GENERATORS BOARD



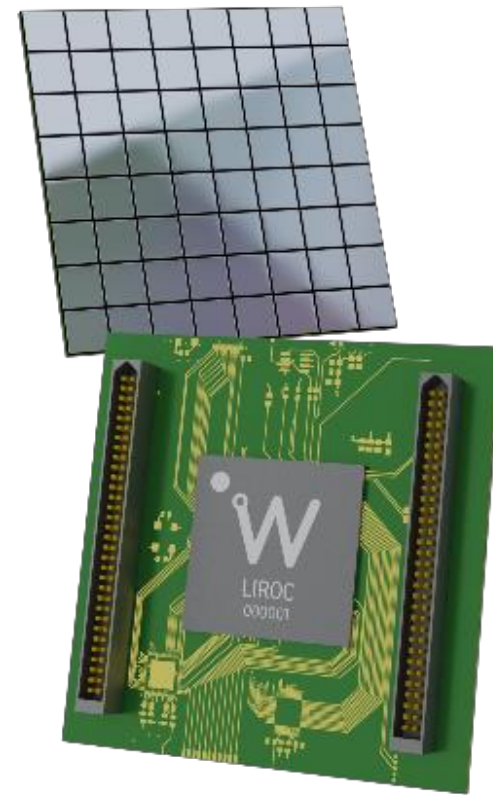
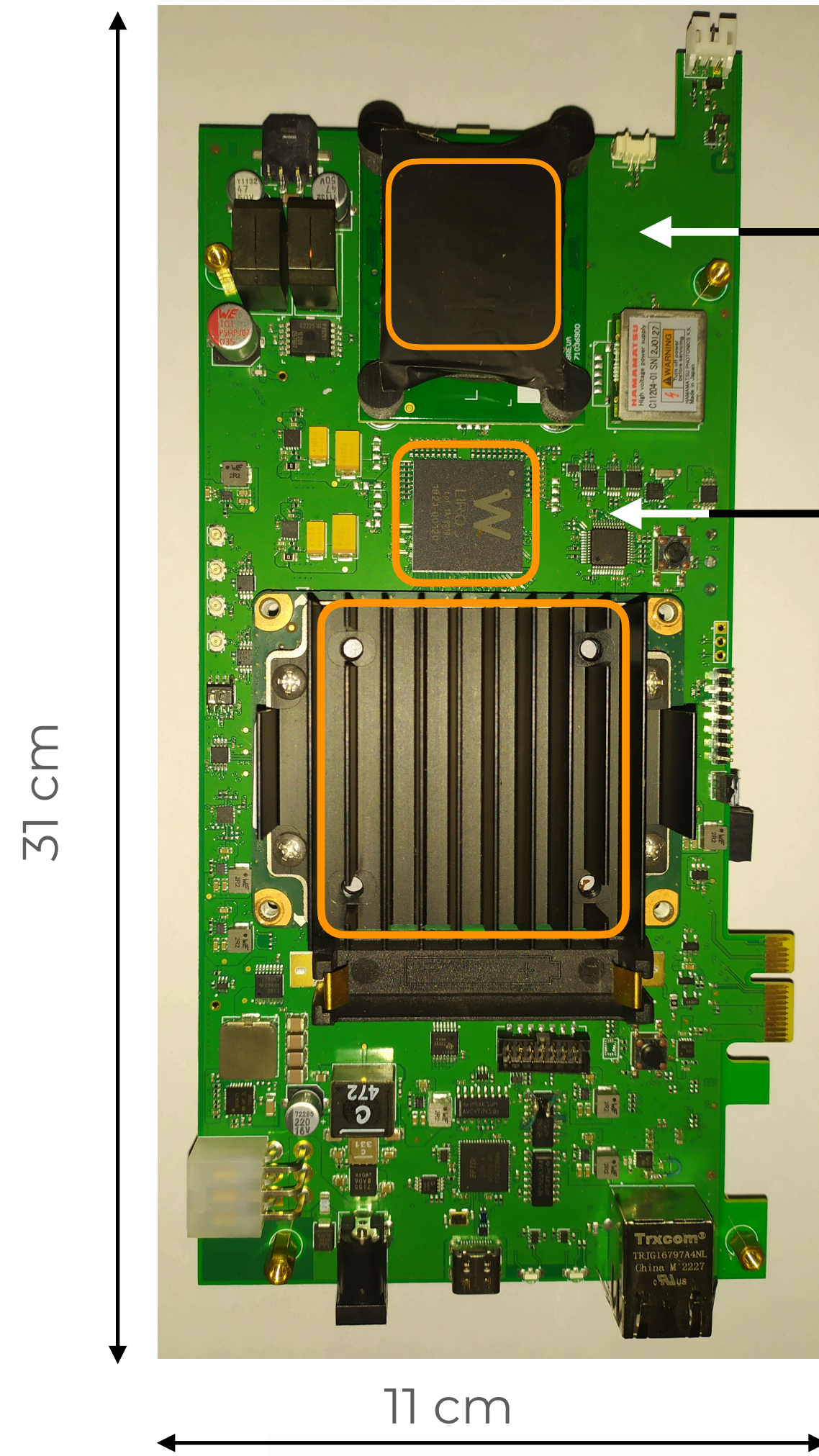
S13361-2050AE-08 by HAMAMATSU
8x8 sensors on each unit

the LIROC ASIC

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 mm ² Flip-Chip low inductance packaging technology

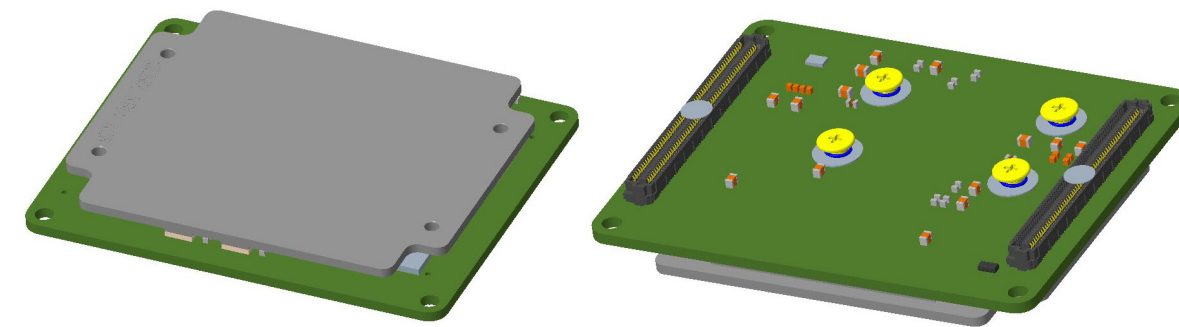
Power Consumption	210mW (TBC) – Supply voltage : 1.2 V
Inputs	64 analogue inputs with independent SiPM HV adjustments
Outputs	64 LVDS triggers
Internal Programmable Features (I2C)	64 HV adjustment for SiPM (64 x 6 bit), trigger threshold programming (10bits), 64 x 7 bit channel-wise threshold adjustment,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

THE 64 GENERATORS BOARD



S13361-2050AE-08 by HAMAMATSU
8x8 sensors on each unit

the LIROC ASIC



AMD
XILINX

Kria K26 SOM

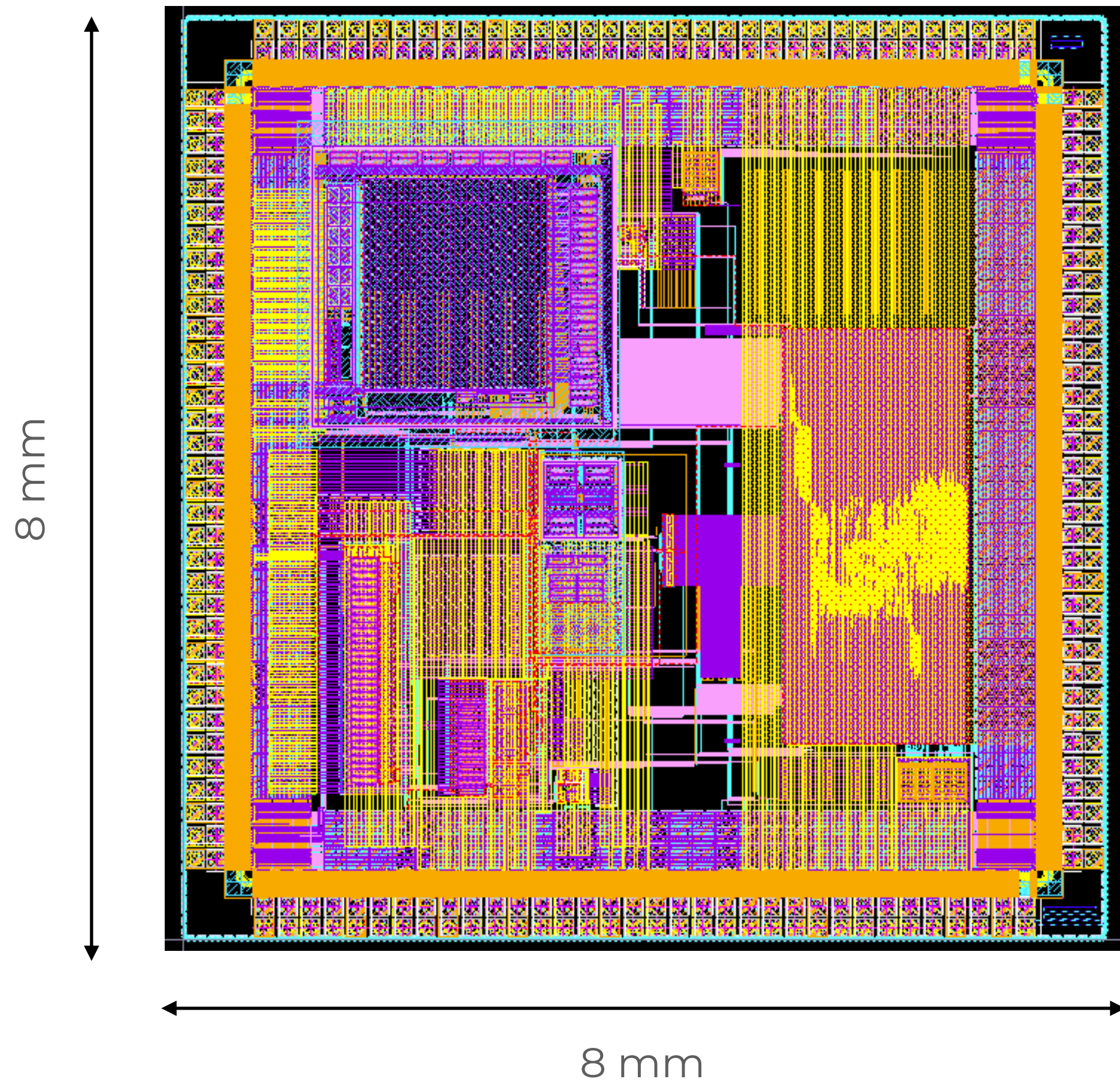
Zynq UltraScale+ MPSoC (XCK26)

- **APU:** Arm® Cortex®-A53 based application processing unit (APU) consisting of quad-core Cortex-A53 processors with an $F_{MAX} = 1333$ MHz, L2 cache, SIMD, VFP4 floating point, and cryptography extensions.
- **RPU:** Arm Cortex-R5F based real-time processing unit (RPU) consisting of dual-core Cortex-R5F processors with floating point unit support with an $F_{MAX} = 533$ MHz, able to operate in stand-alone and lock-step functions.

12W power consumption

4 . s t a t e - o f - p l a y :

THE CUSTOM ASIC

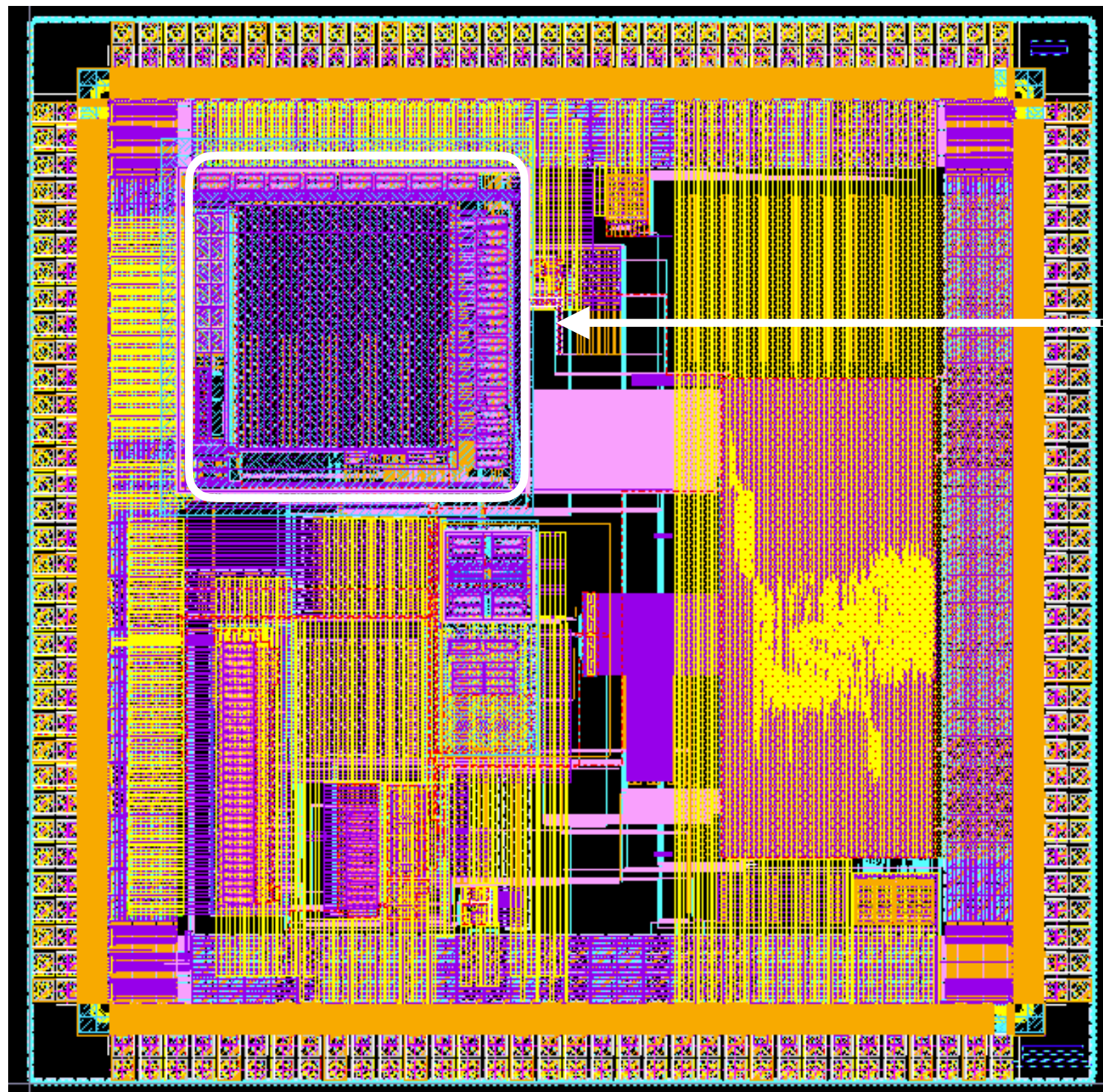


Dimensions [cm²]	1x1
No. generators	1 array
Raw bit stream:	1 Mbps
NIST DRBG output (SP800-90 A,B,C)	32 Mbps
Control:	SPI at 24 MHz (system clock: 66 MHz)
I/O:	SPI at 24 MHz
Power supply:	5V, 1.8V
Power consumption:	100 mW
Encryption of the bit stream:	Yes (AES-256)
Specific Features:	<ul style="list-style-type: none"> • On Silicon implementation of the NIST Real-Time sanity checks (Adaptive Proportion Test and Repetition Count Test) • On Silicon implementation of the NIST DRBG protocol • Package: QFN100 • FIPS 140-3 compliancy by design; • CAVP (Cryptographic Algorithm Validation Program) in progress
State of development:	<ul style="list-style-type: none"> • Design Completed • Production on going • Delivery expected by April 2024

▶ **out of the foundry in April 2024**



THE CUSTOM ASIC: a focus on elements of interest for the PP community



The SPAD array:

- * 32 x 32 cells, **indexed** (!), 50 μm pitch
- * 400 μm^2 SPAD area **[O(45%) FF in Tower's structure with no DTI]**
- * active quenching
- * 2bits/cell to tag whether "screamers" and "disabled"
- * expected $V_{\text{breakdown}}$: O(12.5V)
- * expected DCR density @roomT: 20 Hz/ μm^2 (all in all 8.2 Mcps in the array; mind the screamers!); note that other processes have a DCR lower by a factor 15
- * Deep trench isolation for X-talk reduction (O(1%) at +4V)

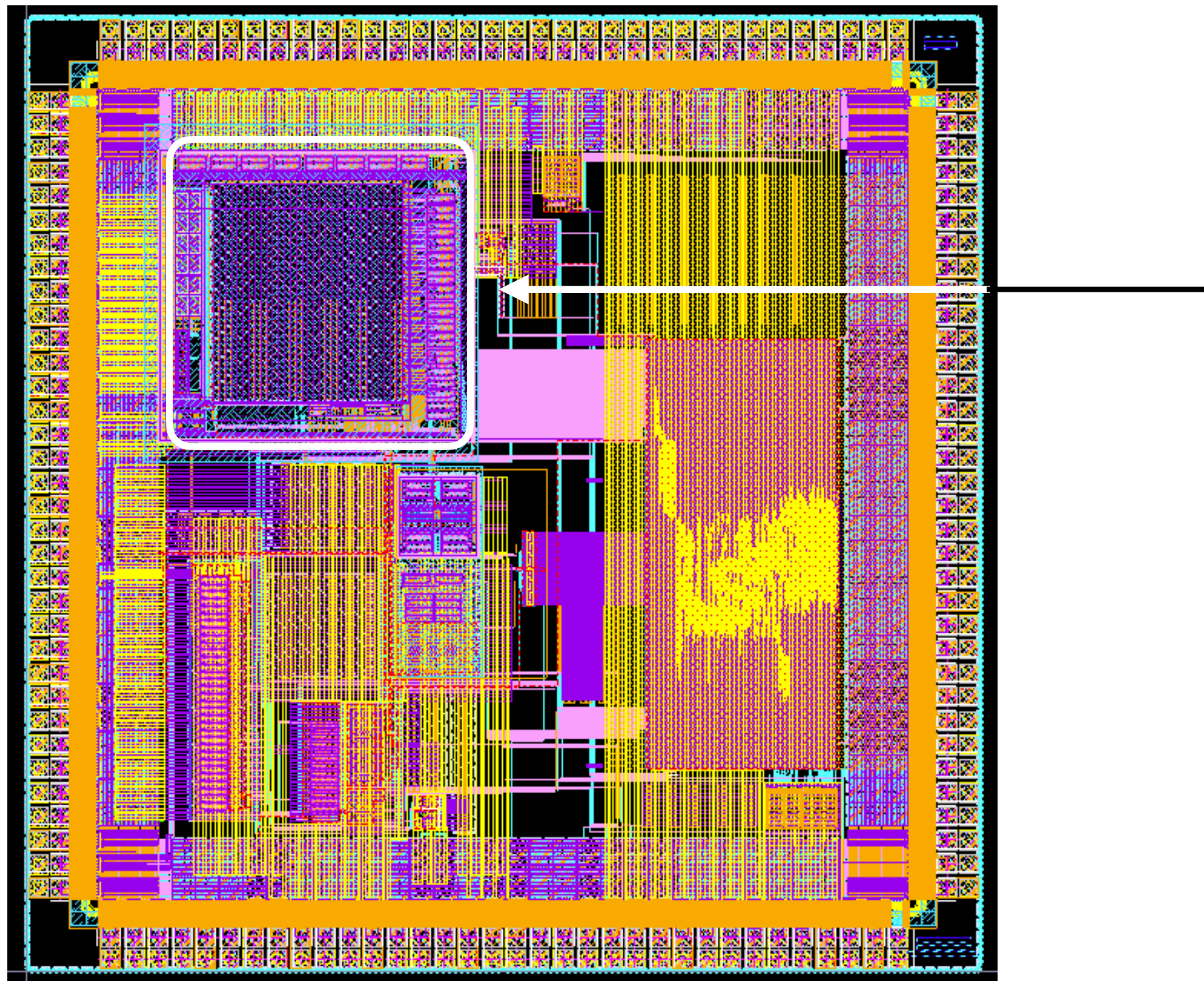
- * **FBK-IP: circuit for**
 - ➔ **auto- V_{Br} detection**
 - ➔ **High-V generation through a charge pump**
 - ➔ **auto excess voltage stabilisation against T & process variations**

1

2

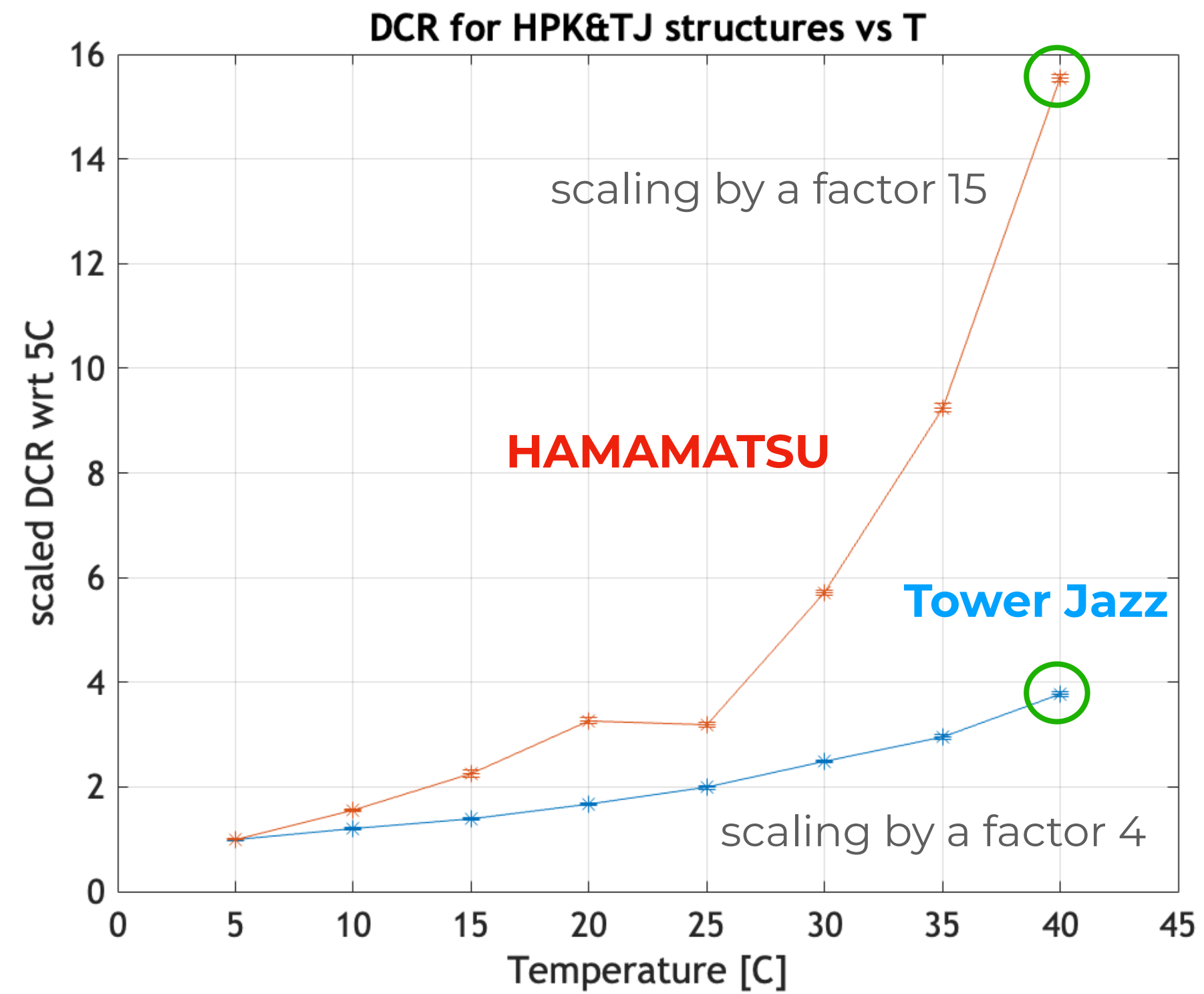
4 . s t a t e - o f - p l a y :

THE CUSTOM ASIC: a focus on elements of interest for the PP community



The SPAD array:

* Very interesting behaviour against Temperature:



Random Power IP: process variation to further reduce the T dependence

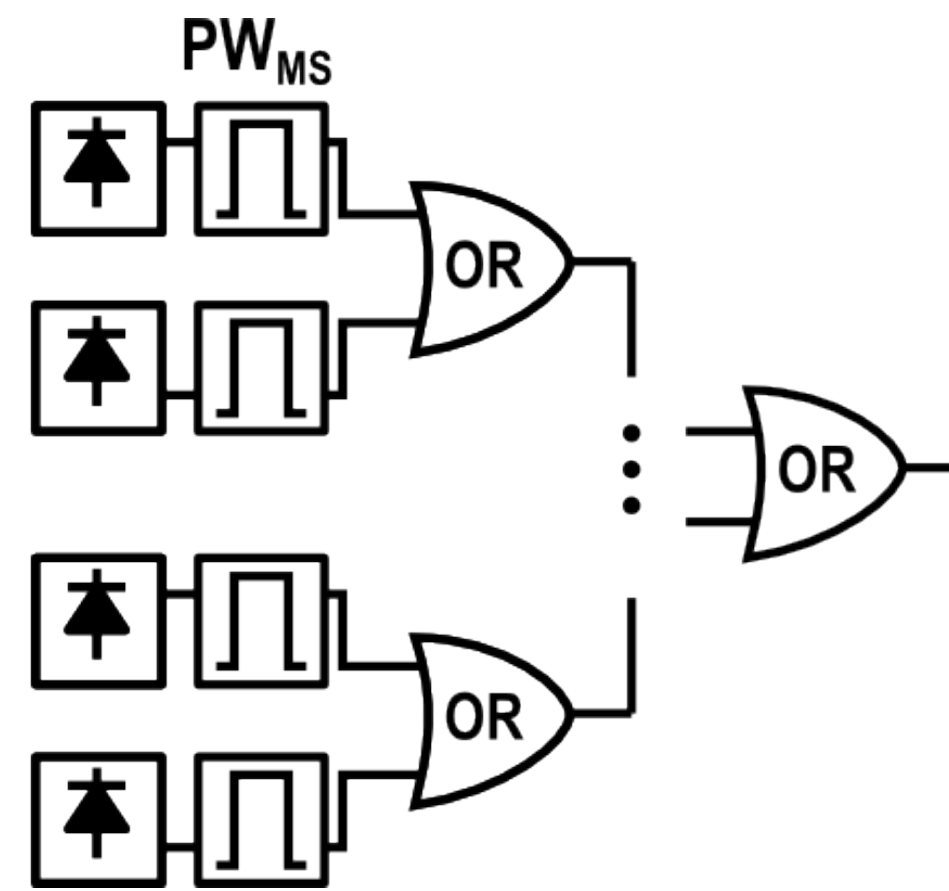
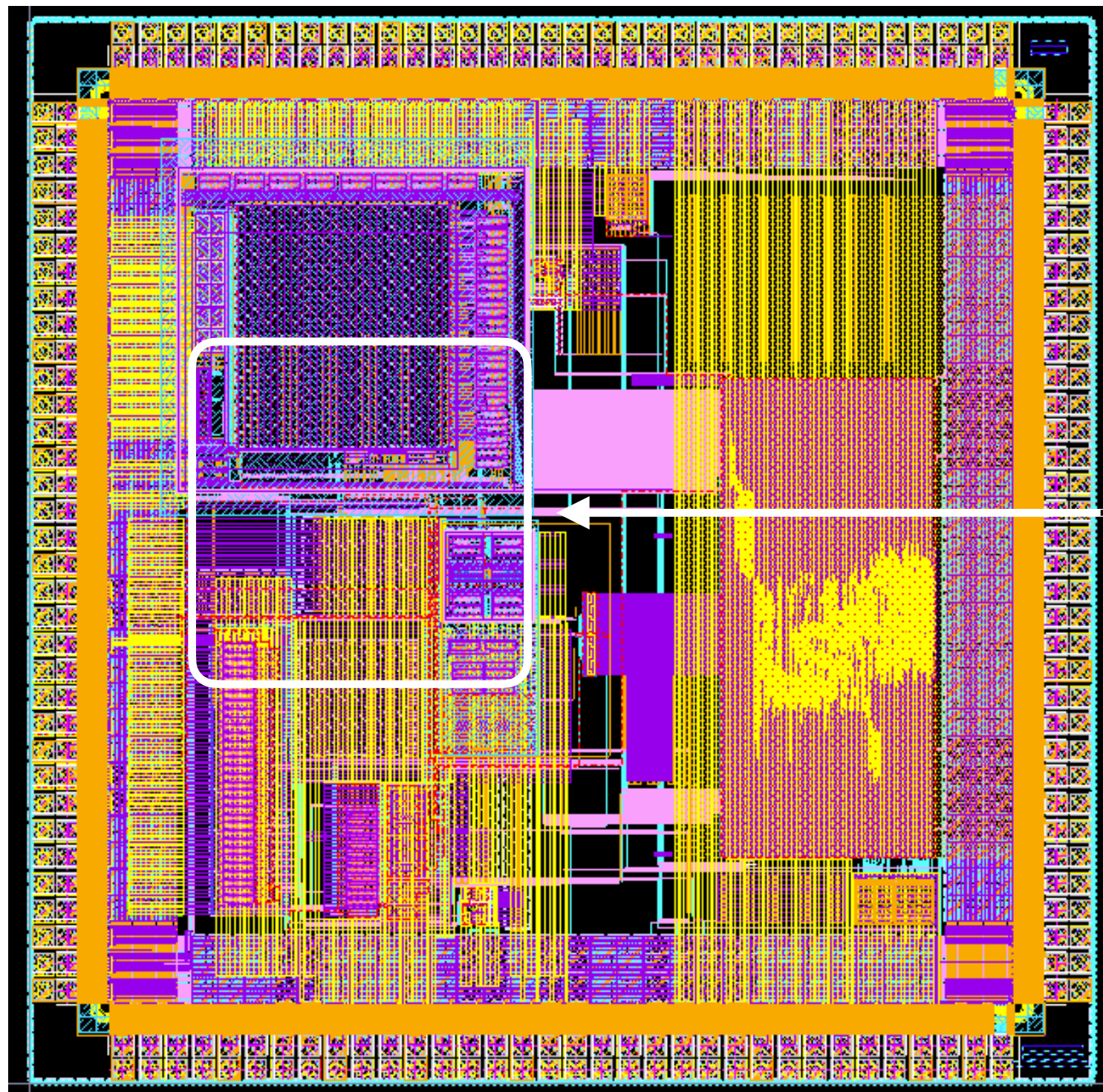
3

experimental results by test structures in one of the Tower processes

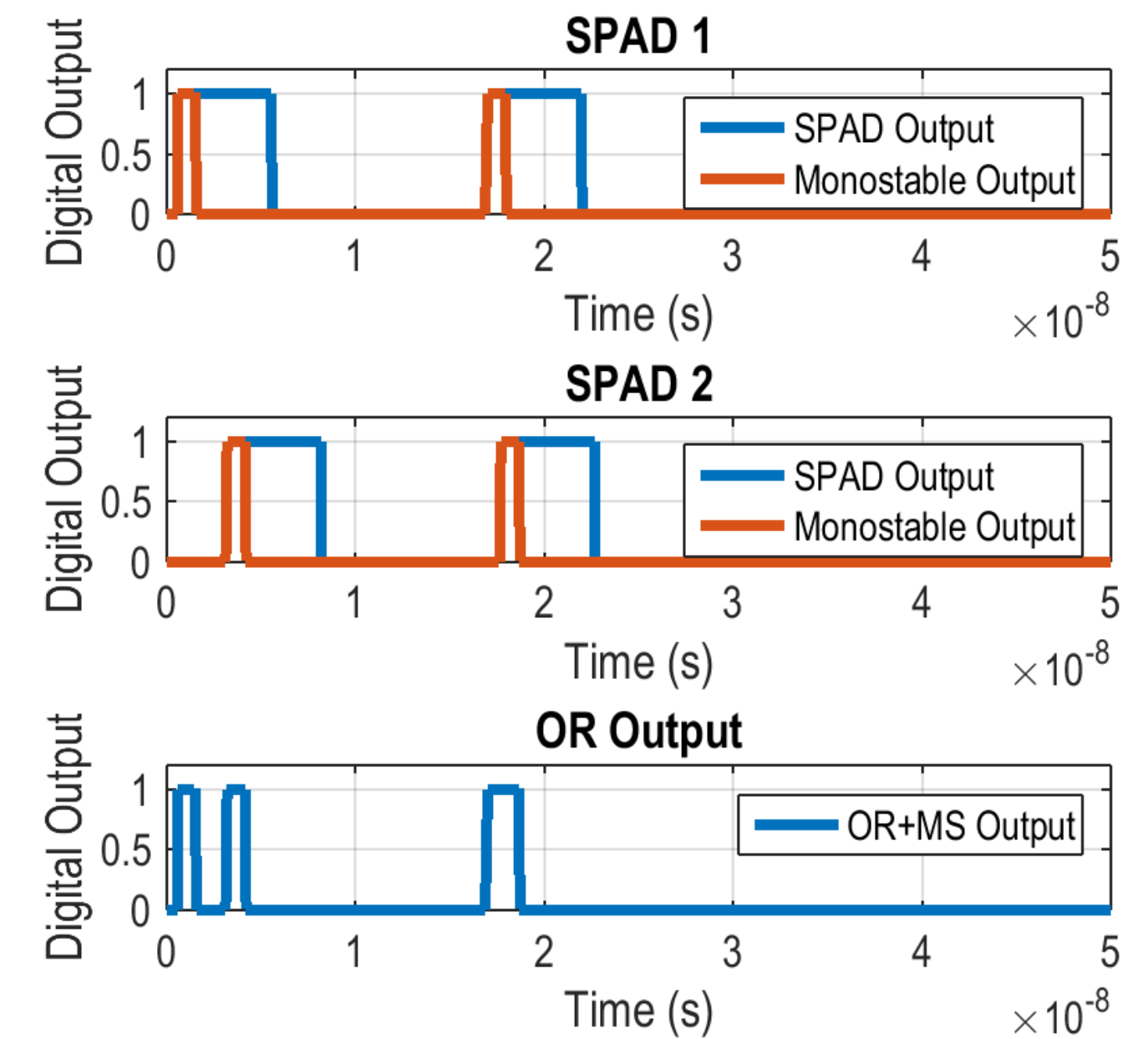
THE CUSTOM ASIC: a focus on elements of interest for the PP community



Data “draining”: pulse combination through an on-cell monostable driven OR tree:



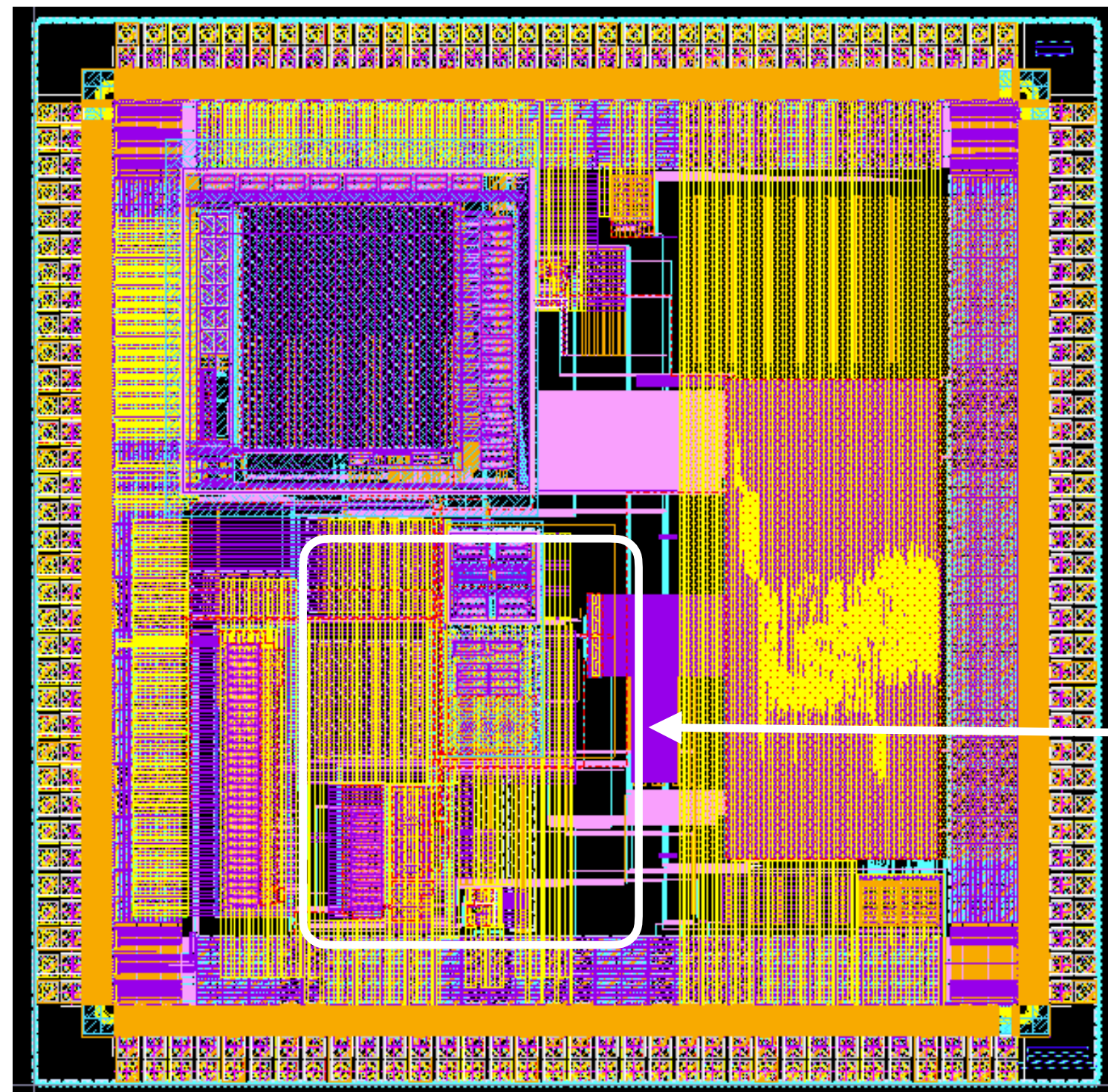
- OR tree fed by pulses from a monostable circuit
- width of the pulse $PW_{MS} < \tau_d$ (≈ 100 ps quoted in the ref. paper. 3 ns in pur implementation vs τ_d about 30 ns)



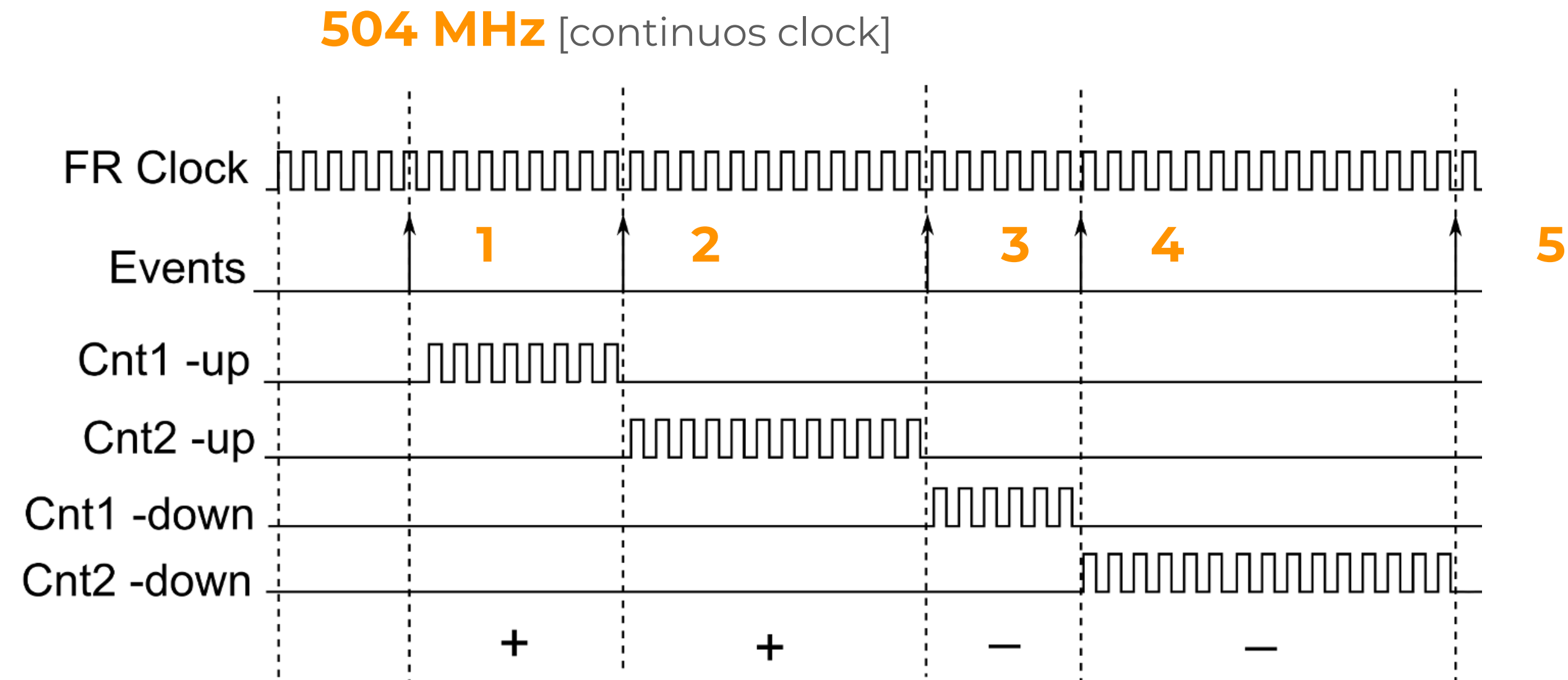
circuitry: FBK-IP (partially patented)

* “Digital Silicon Photomultipliers with OR/XOR Pulse Combining Techniques’, *IEEE Transactions on Electron Devices*, vol. 63, no. 3, pp. 1105-1110. <https://doi.org/10.1109/TED.2016.2518301>, by S. Gnechi et al., 2016

THE CUSTOM ASIC: a focus on elements of interest for the PP community



* TDC-A [FBK IP]; the ping-pong architecture:



5

1. starts counter 1 up
2. stops counter 1 & starts counter 2 up
3. stops counter 2 & starts counter 1 down
4. stops counter 1 down & starts counter 2 down
5. stops counter 2 down and re-start counter 1 up

- the sign of each counter (15+1 bits) determines the status of one random bit
- dead time of each up-down counting 20 ns
- cascade of 4 counters

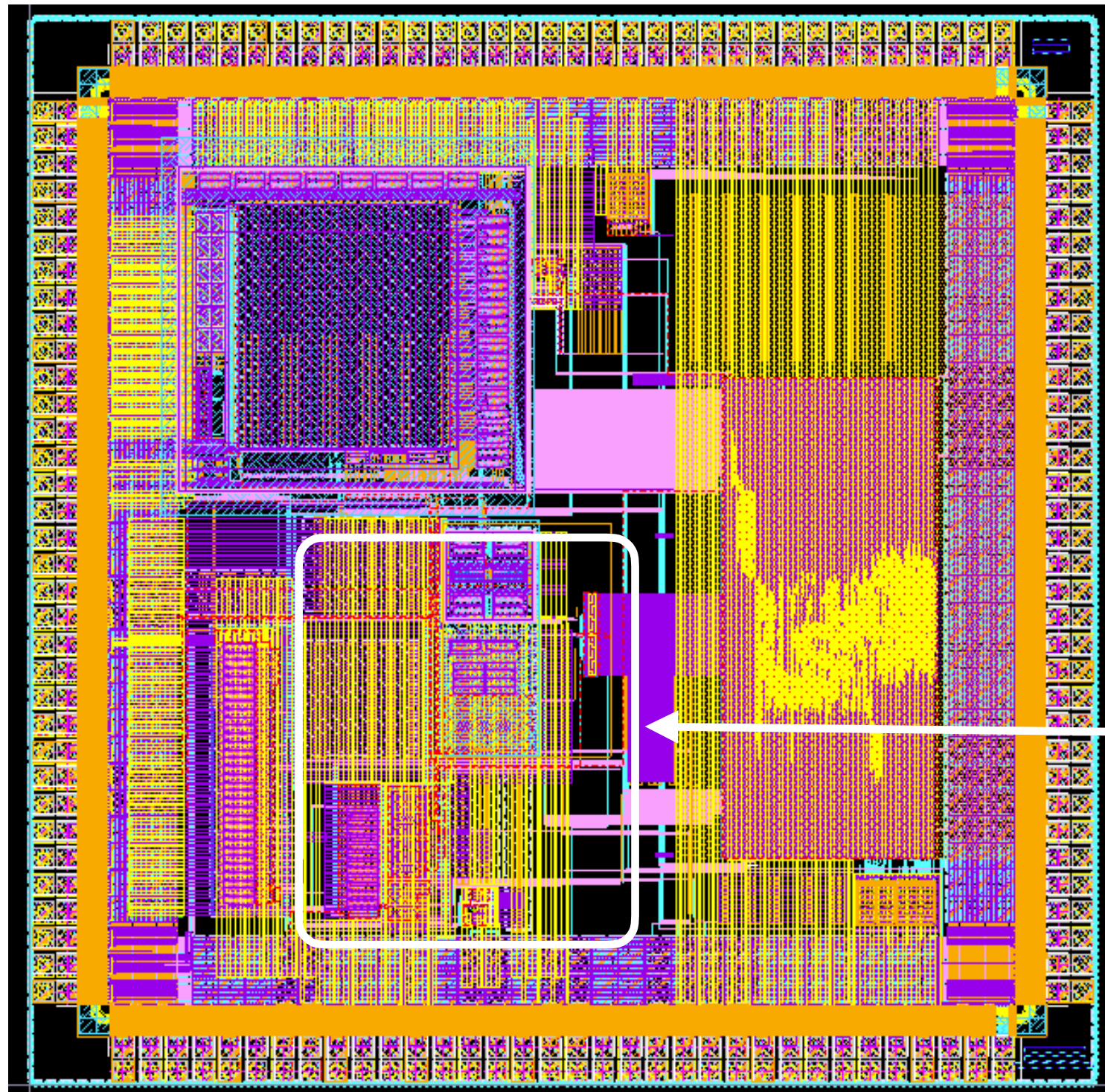
- A Fully Digital 8 16 SiPM Array for PET Applications With Per-Pixel TDCs and Real-Time Energy Output, L. Braga et al. IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 49, NO. 1, JANUARY 2014

- A High-Throughput Time-Resolved Mini-Silicon Photomultiplier With Embedded Fluorescence Lifetime Estimation in 0.13 μm CMOS, D. Tyndall et al. IEEE TRANSACTIONS ON BIOMEDICAL CIRCUITS AND SYSTEMS, VOL. 6, NO. 6, DECEMBER 2012

THE CUSTOM ASIC: a focus on elements of interest for the PP community

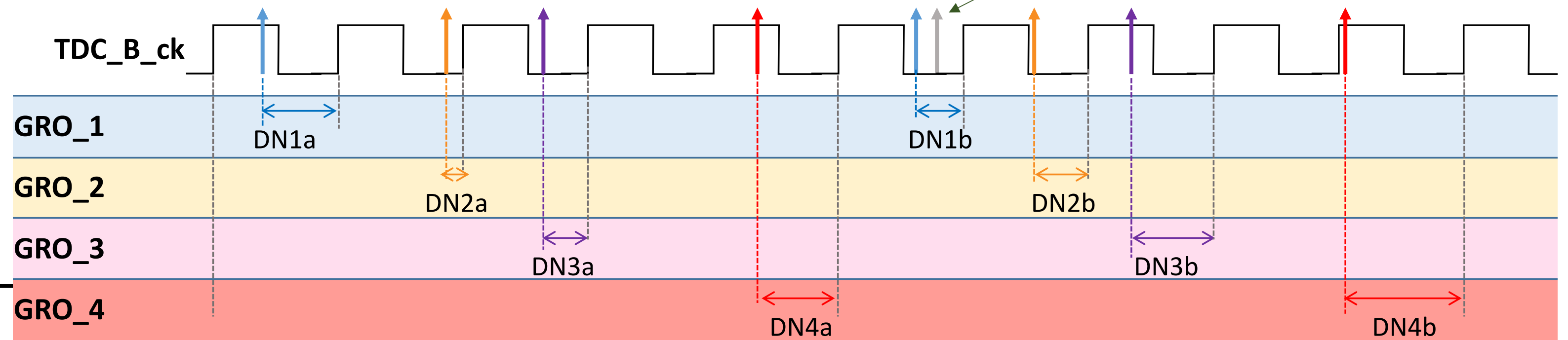
* **TDC-B [IMASENIC IP]: a fourfold cascade of high-res resettable counters**

6



Tunable coarse clock [default: 66 MHz]

Event ignored: only 1st arrival in each clock cycle is detected



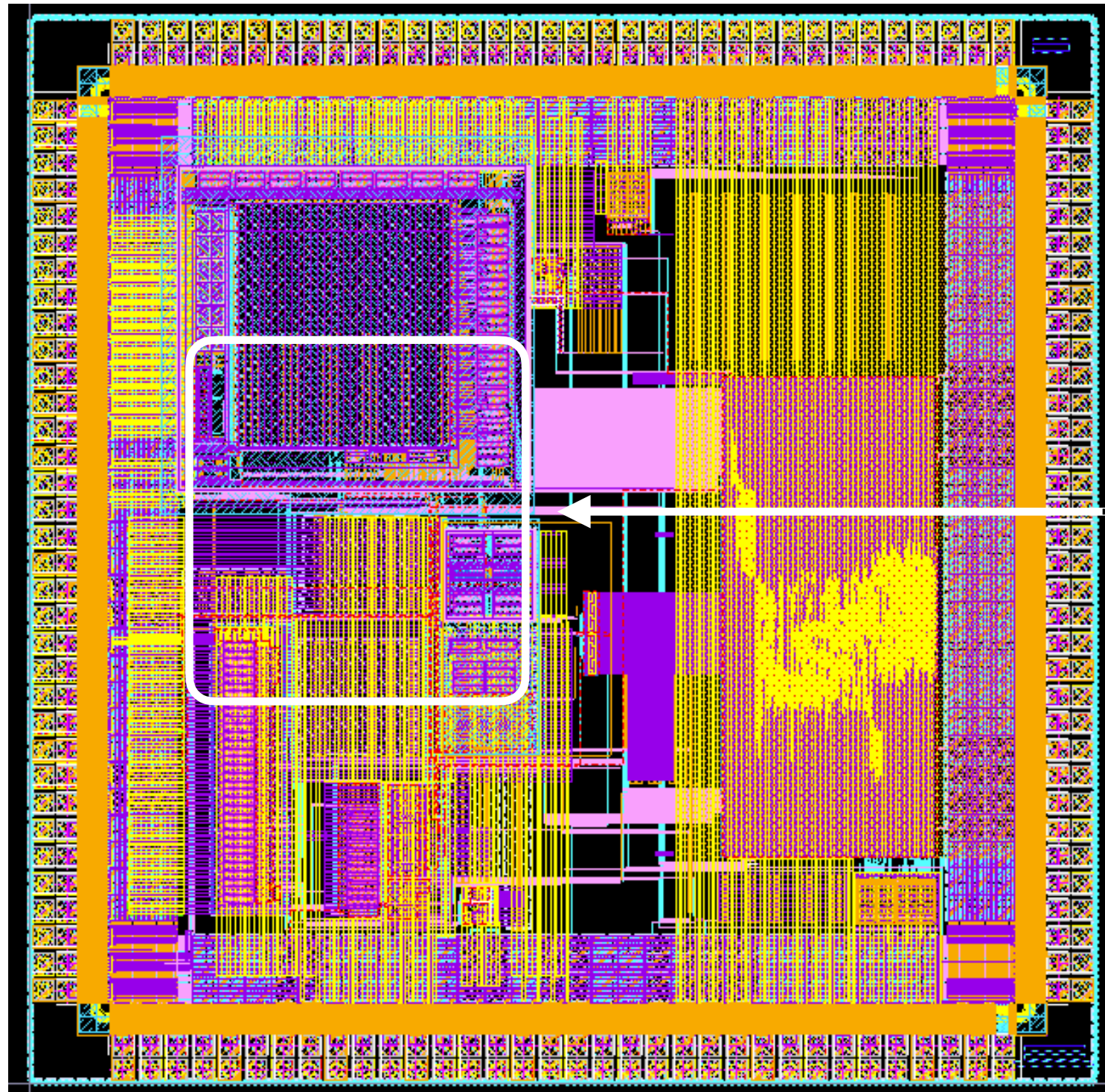
↑ Gated Ring Oscillators with 248 ps cycle

Time stamping by the time of the arrival to the next leading edge of the coarse clock

Optimisation:

- **efficiency**, taking into account advantages & disadvantages linked to the coarse clock frequency
- **systematics**, comparing “time of arrivals” originating by the same GRO

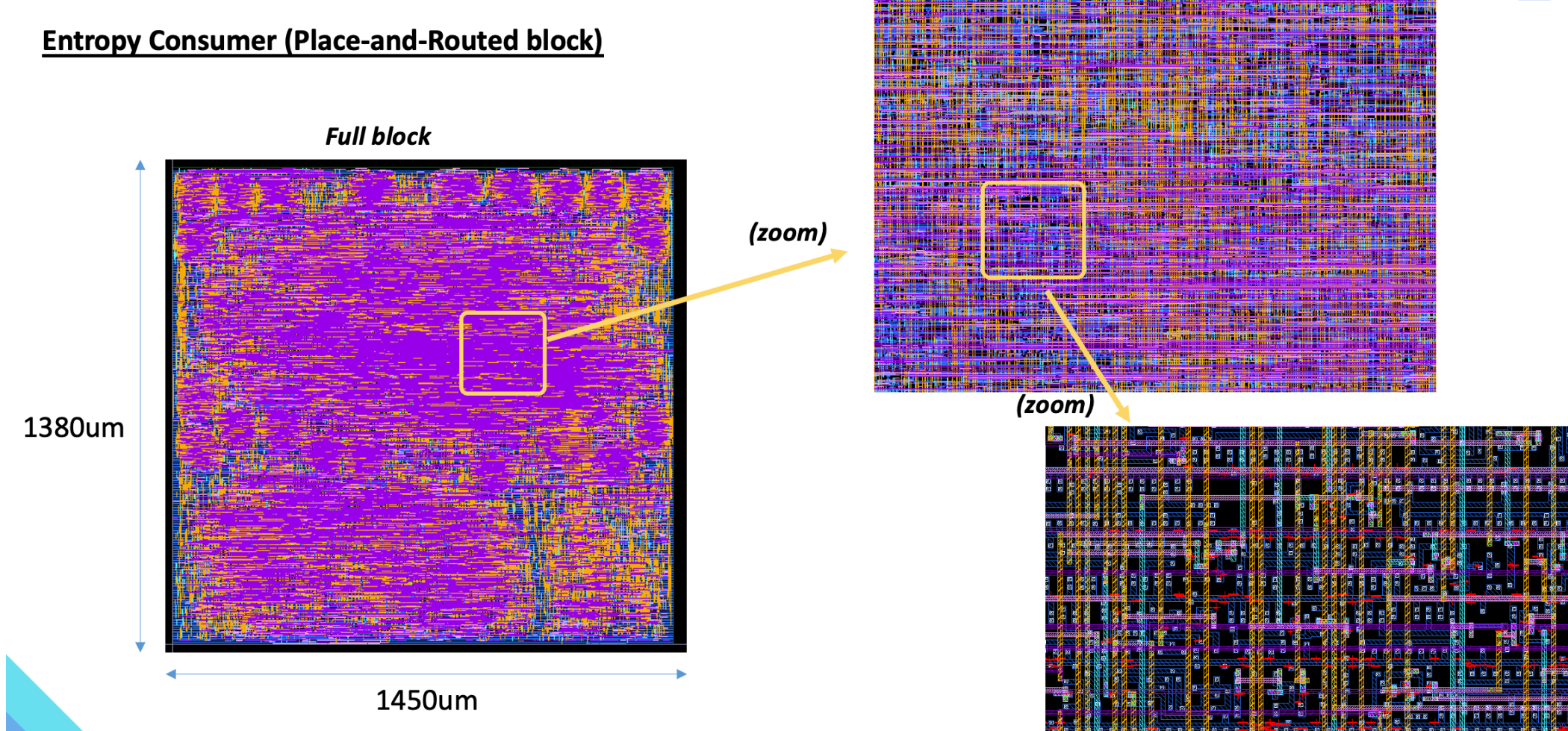
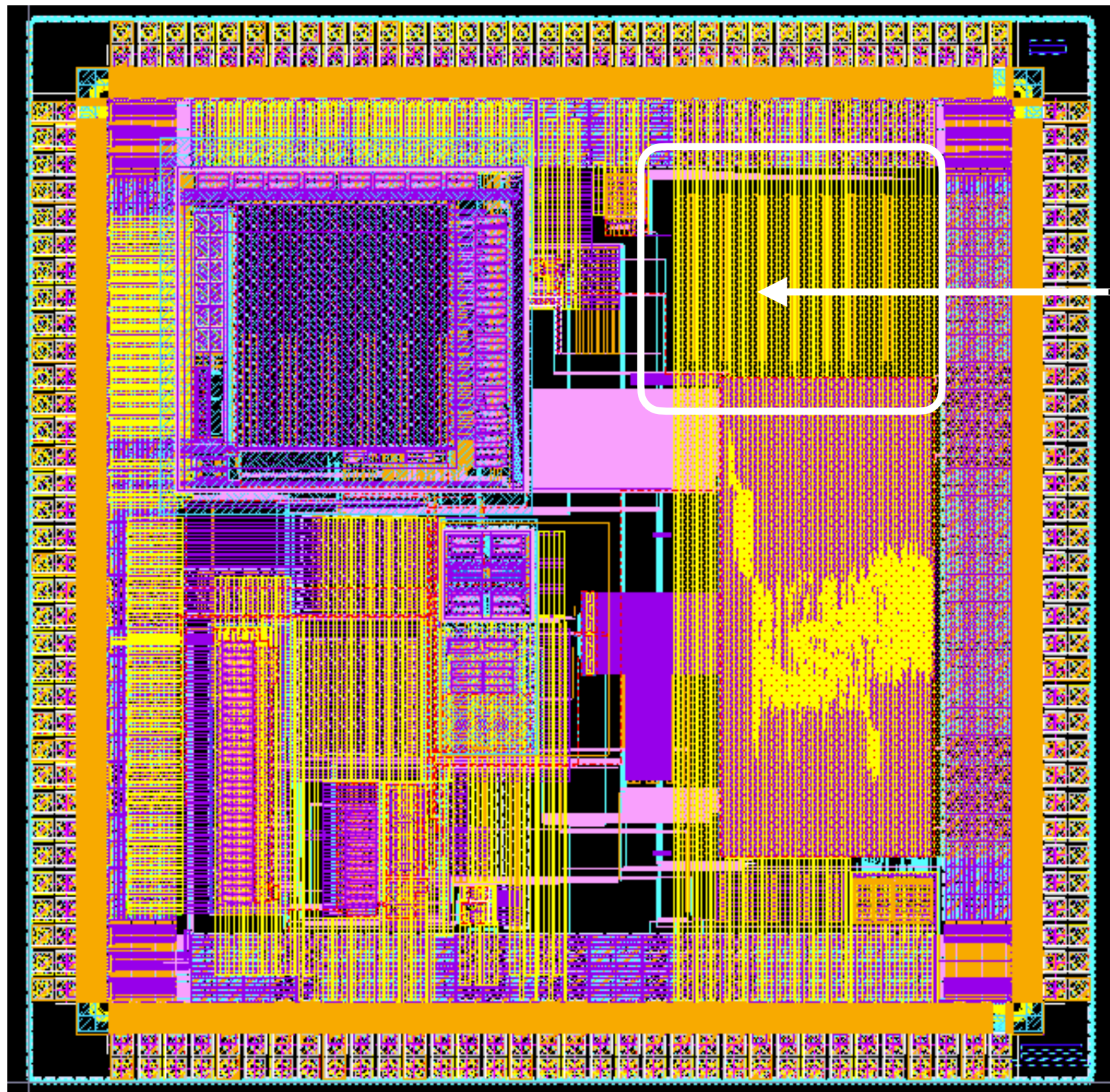
THE CUSTOM ASIC: beside potential interest for the PP community



DCR level control (joint property of Random Power and FBK)
through bias variation and cell enabling/disabling

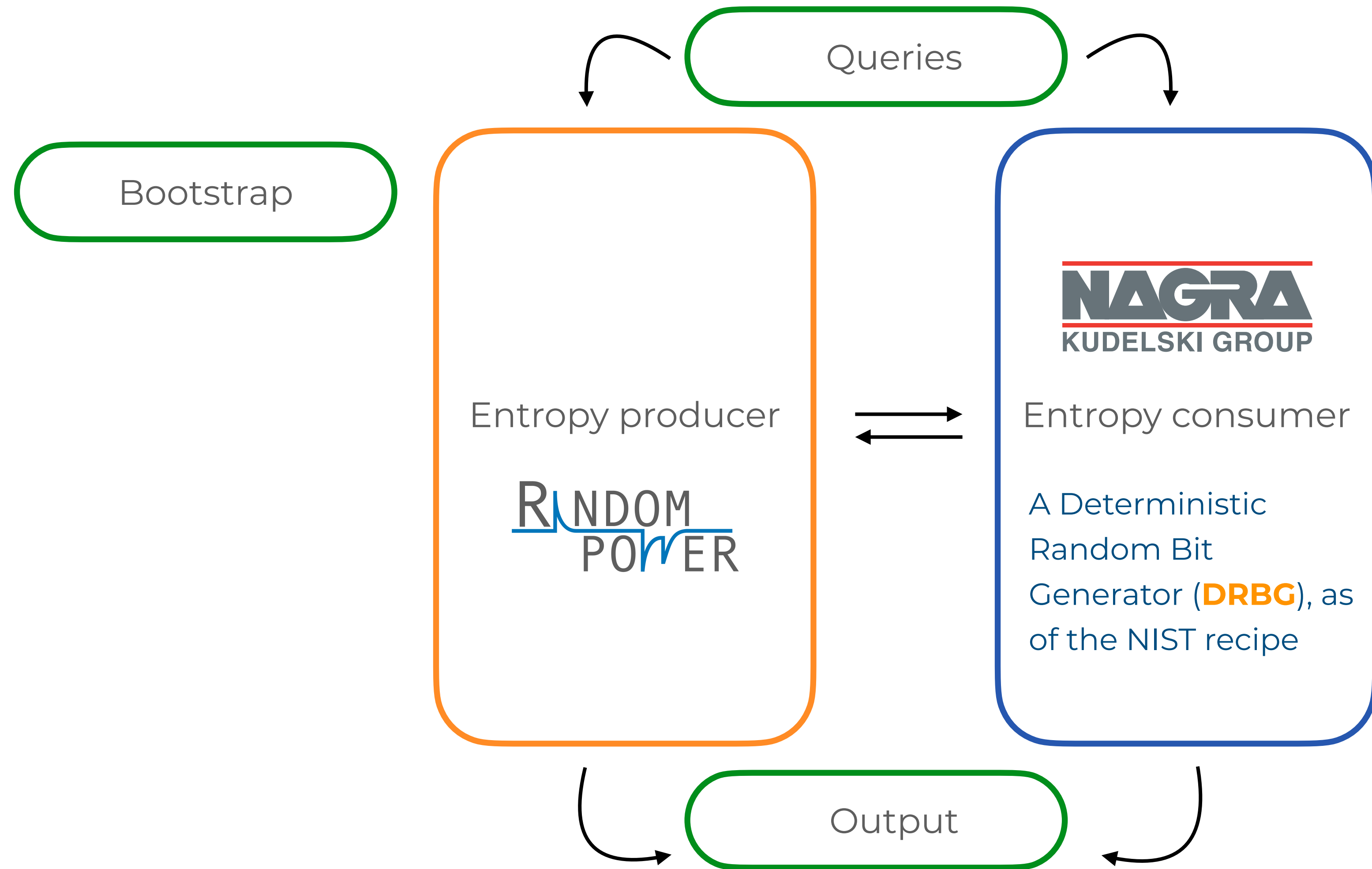
THE CUSTOM ASIC: beside potential interest for the PP community

- * Implementation of the NIST DRBG (Deterministic Random Bit Generation) machine (NAGRA-KUDELSKI IP)



- * AES-256 encryption of the bit stream (NAGRA-KUDELSKI IP)
- * Chip access control via a silicon encoded key (NAGRA-KUDELSKI IP)

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)

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 Deterministic Random Bit Generators (DRBG)

NIST Special Publication 800-90A
Revision 1

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Approved DRBG mechanisms

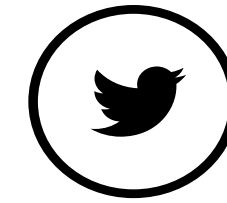
1 (Second Draft) NIST Special Publication 800-90C

2
3
4
5
6
7

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”



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



2020 Winner - ICT

2020 Winner of 2 "special prizes"

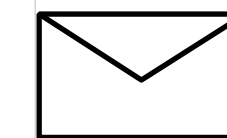


2021 PoC investment by LifTT, a VC located in Torino (ITALY)

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



CONTACT US at:



▶ massimo.caccia@randompower.eu

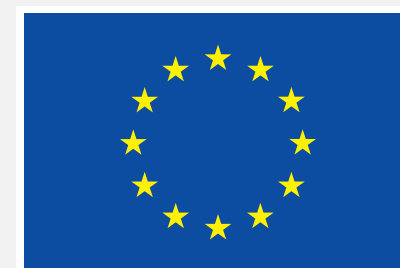
● marcello.esposito@randompower.eu

* lorenza.paolucci@randompower.eu

RANDOM POWER

www.randompower.eu

Established in June 2021



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