# SPAD-based QRNGs

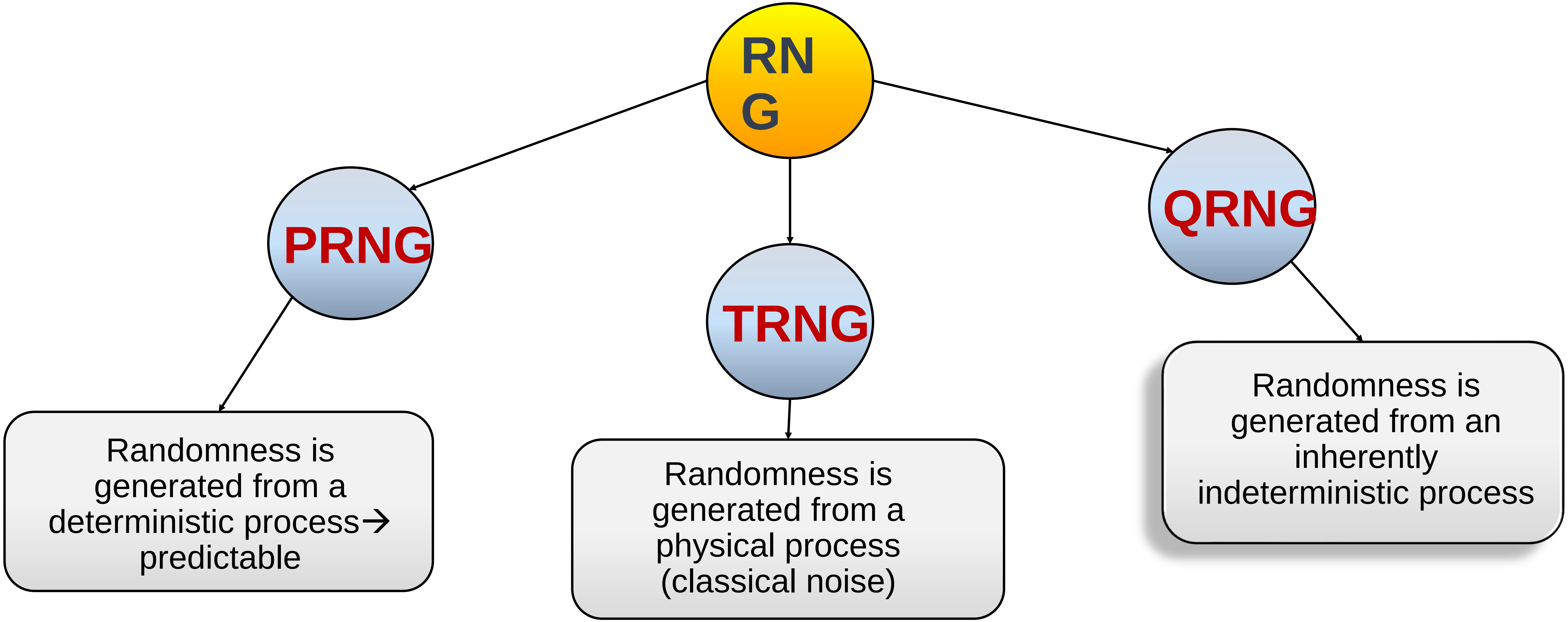
Nicola Massari

Fondazione Bruno Kessler - Italy

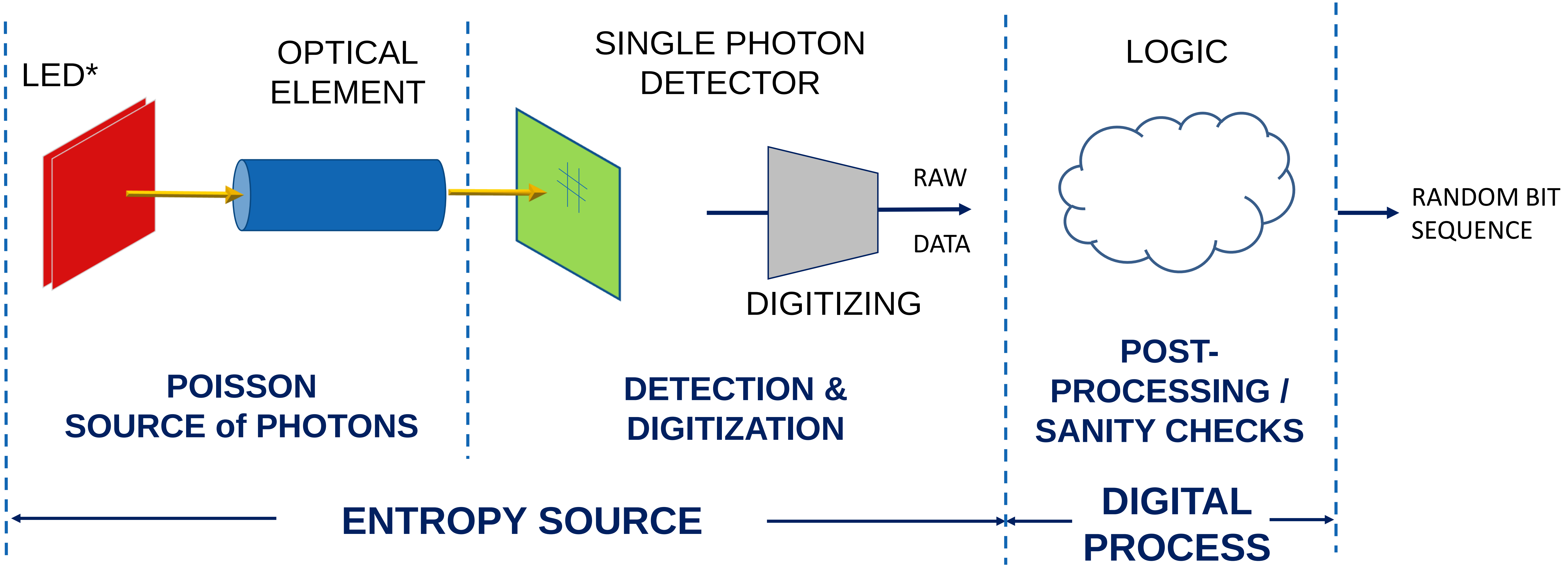
# QRNG based on SPAD
## Outline

- Introduction to QRNG based on SPAD
- Different QRNG approaches:
  - Based on photon counting
  - Based on the arrival time: single and multi-bit
  - Random FF
- QRNGs trend:
  - Monolithic SPAD
- Conclusion

# Context and motivation
## Quantum Random Number Generator



# SPAD-based QRNG
## Typical scheme

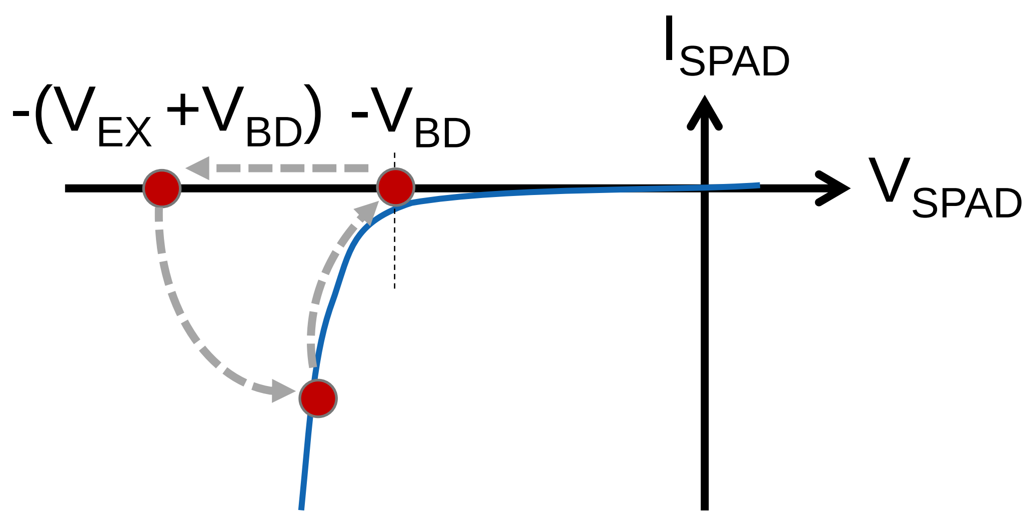



*An LED produces incoherent light by spontaneous emission which is essentially a random process. If operated at sufficiently low power, a LED emits photons which are virtually independent of each other

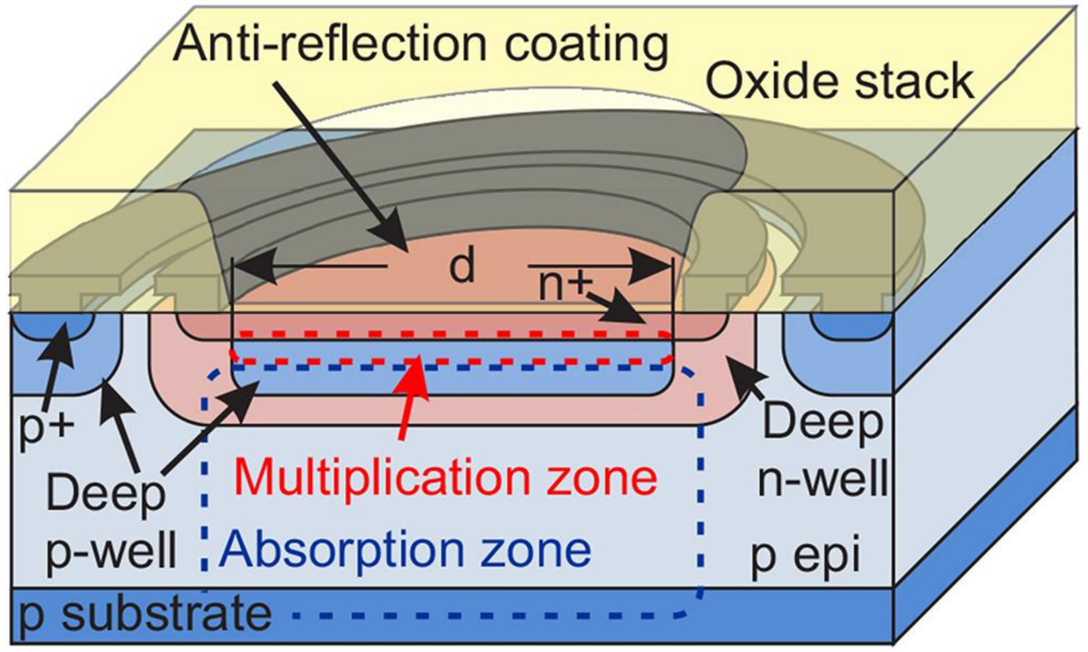
# SPAD-based QRNG
## Single Photon Avalanche Diode (SPAD)

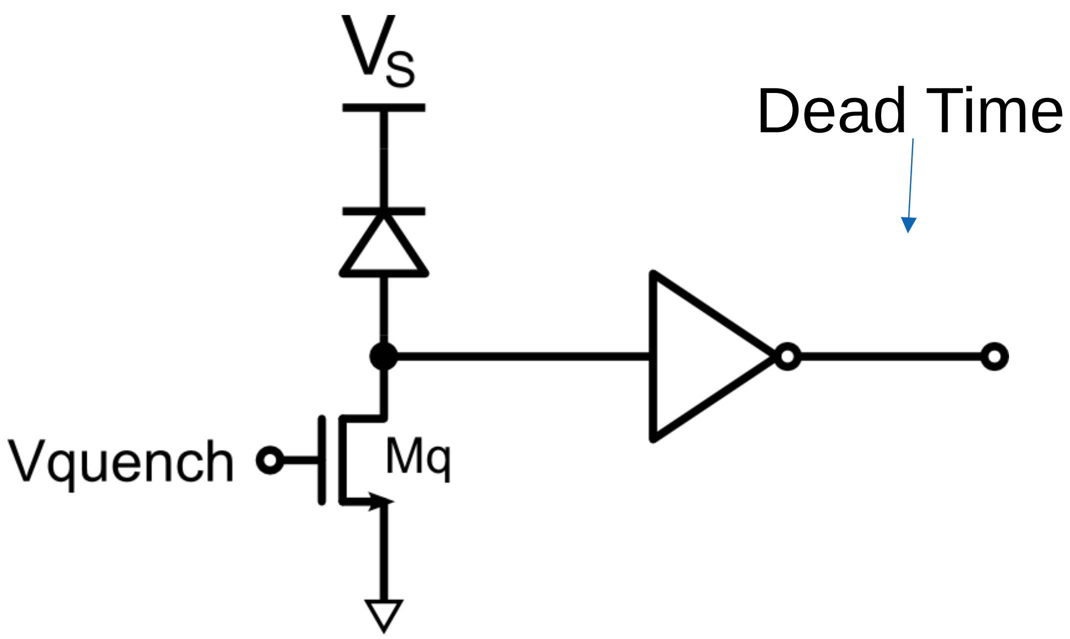
**SPAD (biased in Geiger mode) operation**

Avalanche
Quenching
Recharge

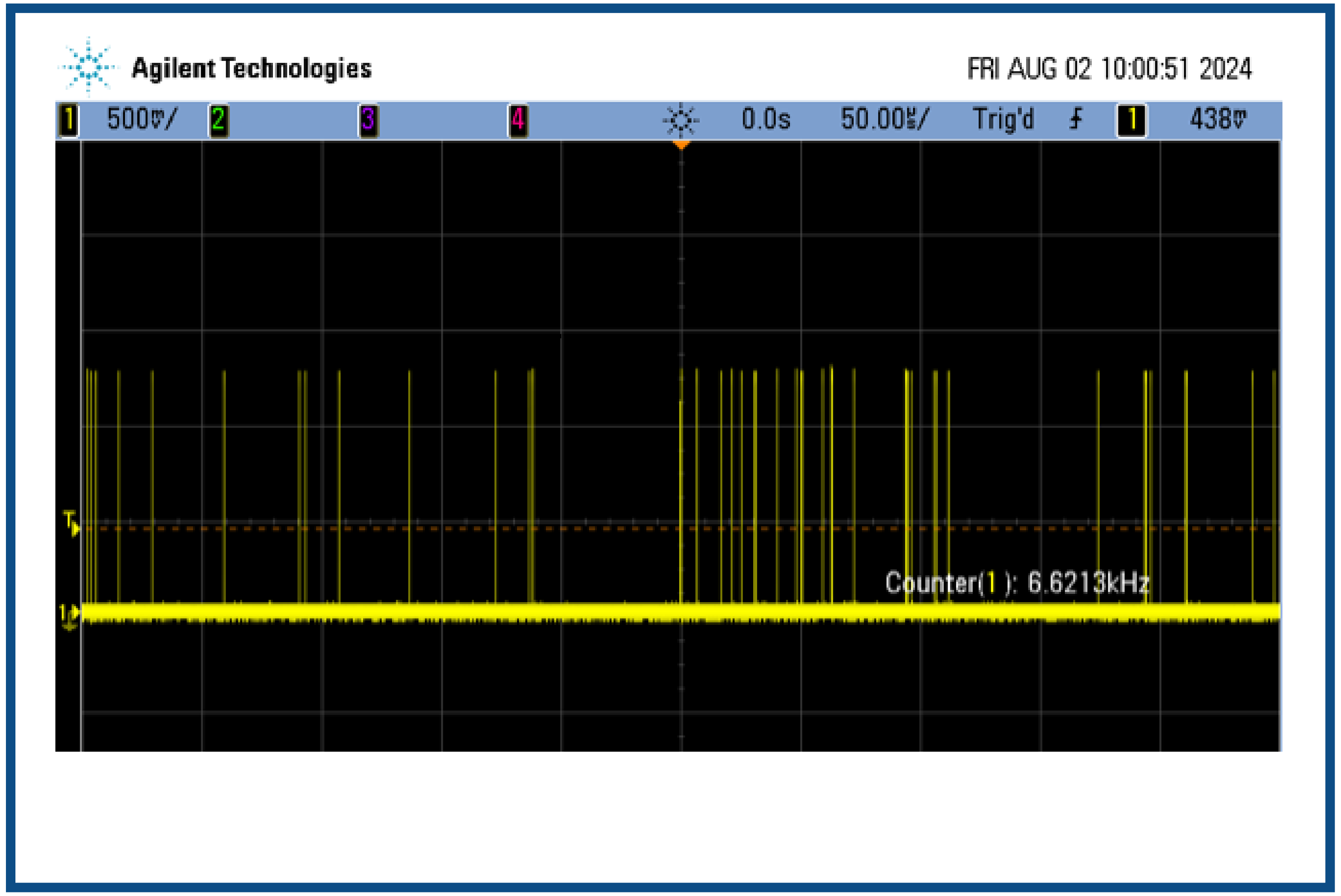


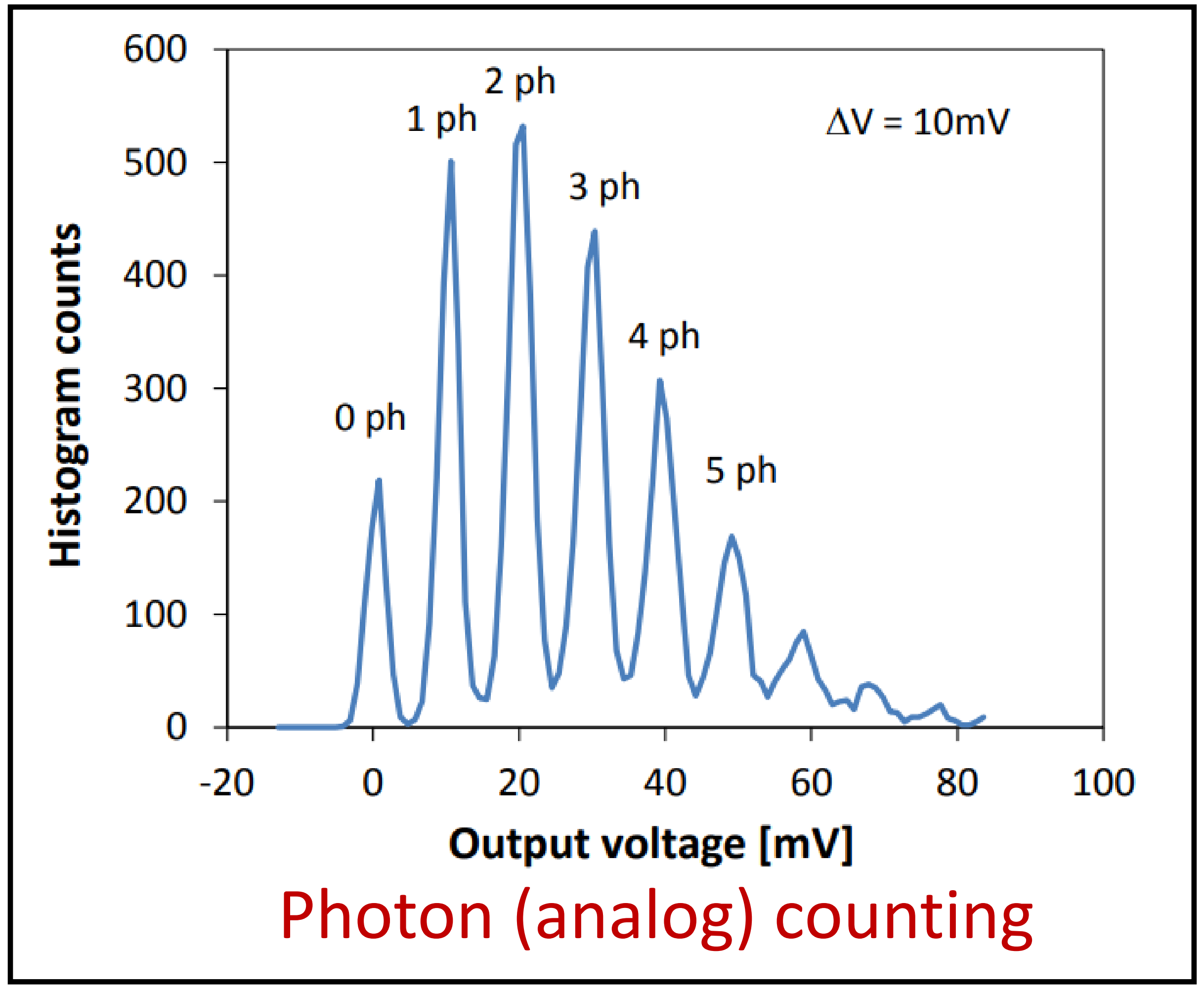

**Integration in a CMOS process**

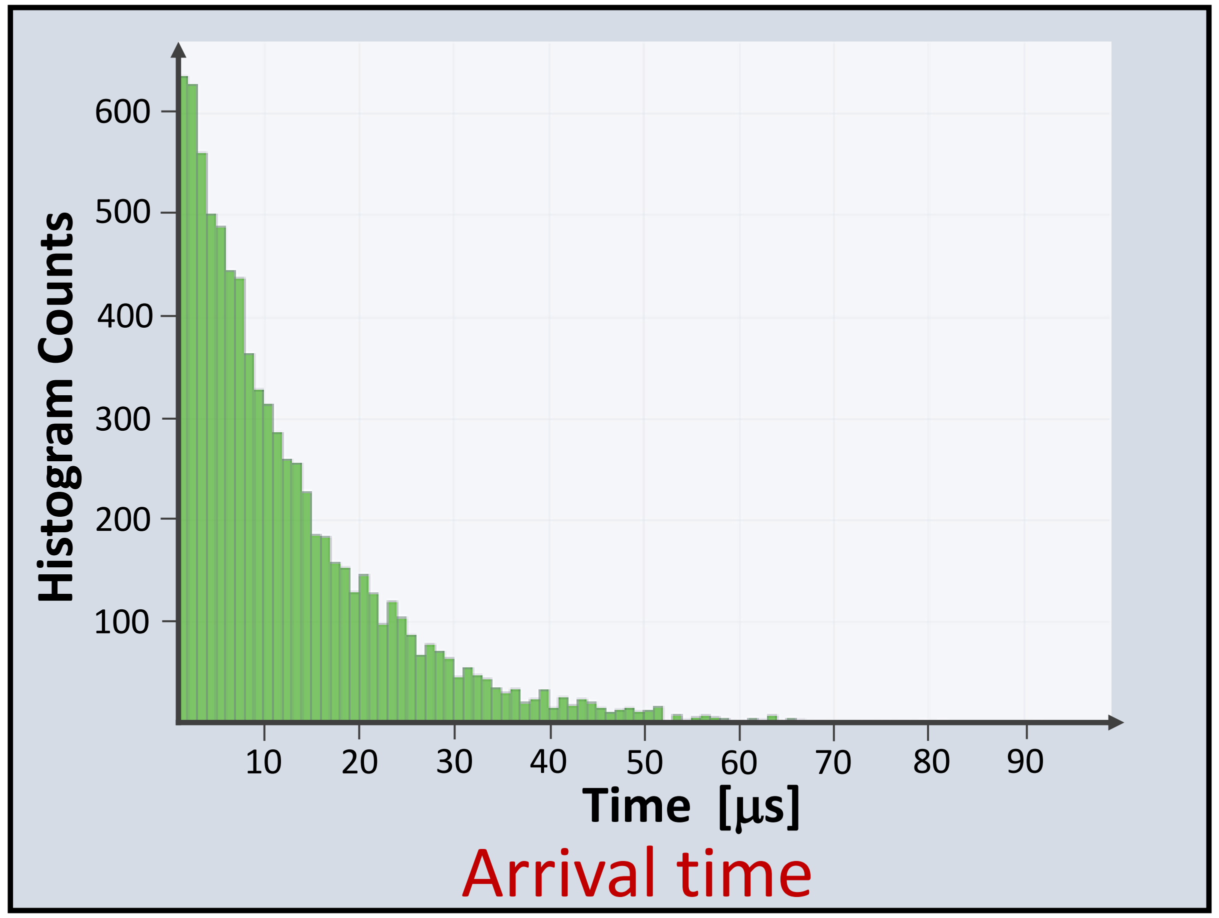


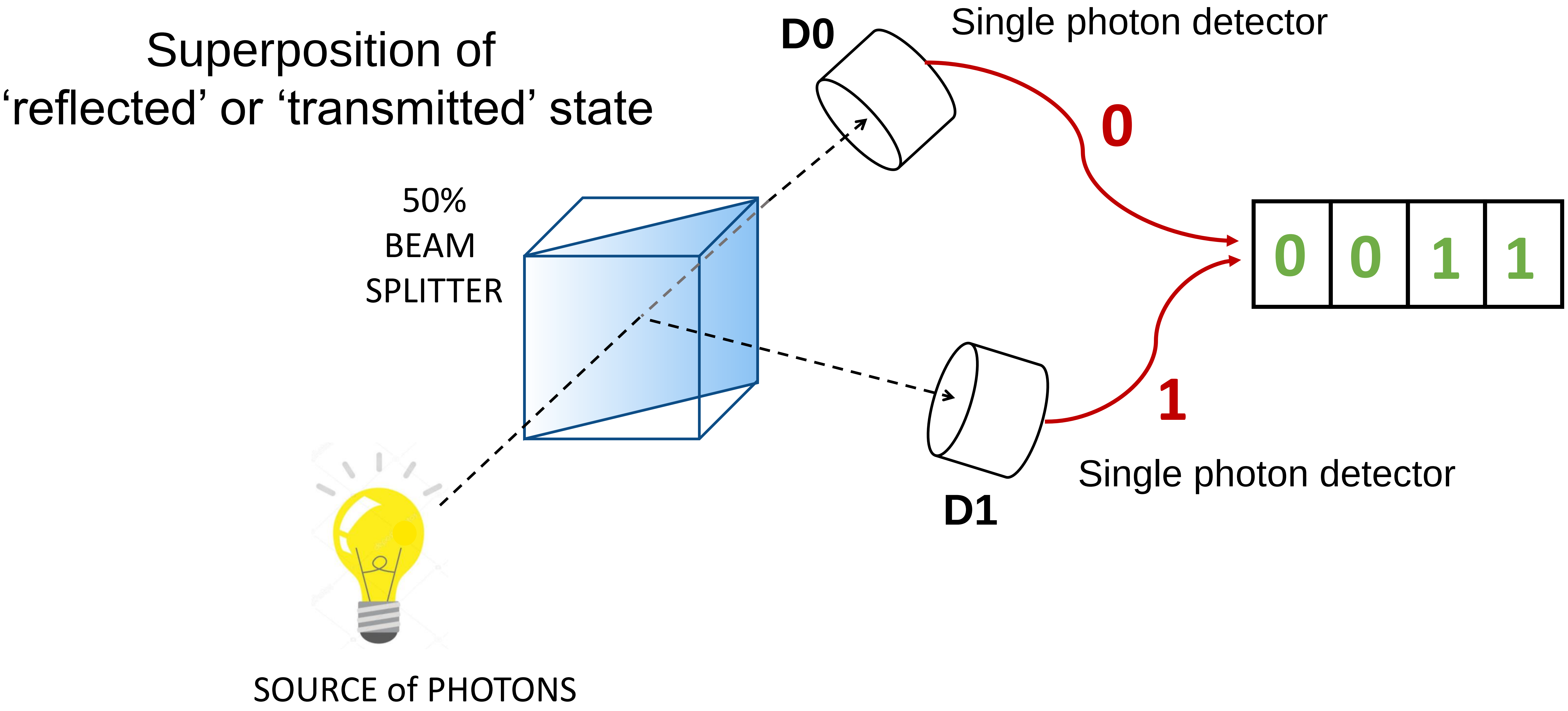
# SPAD-based QRNG
## SPAD output



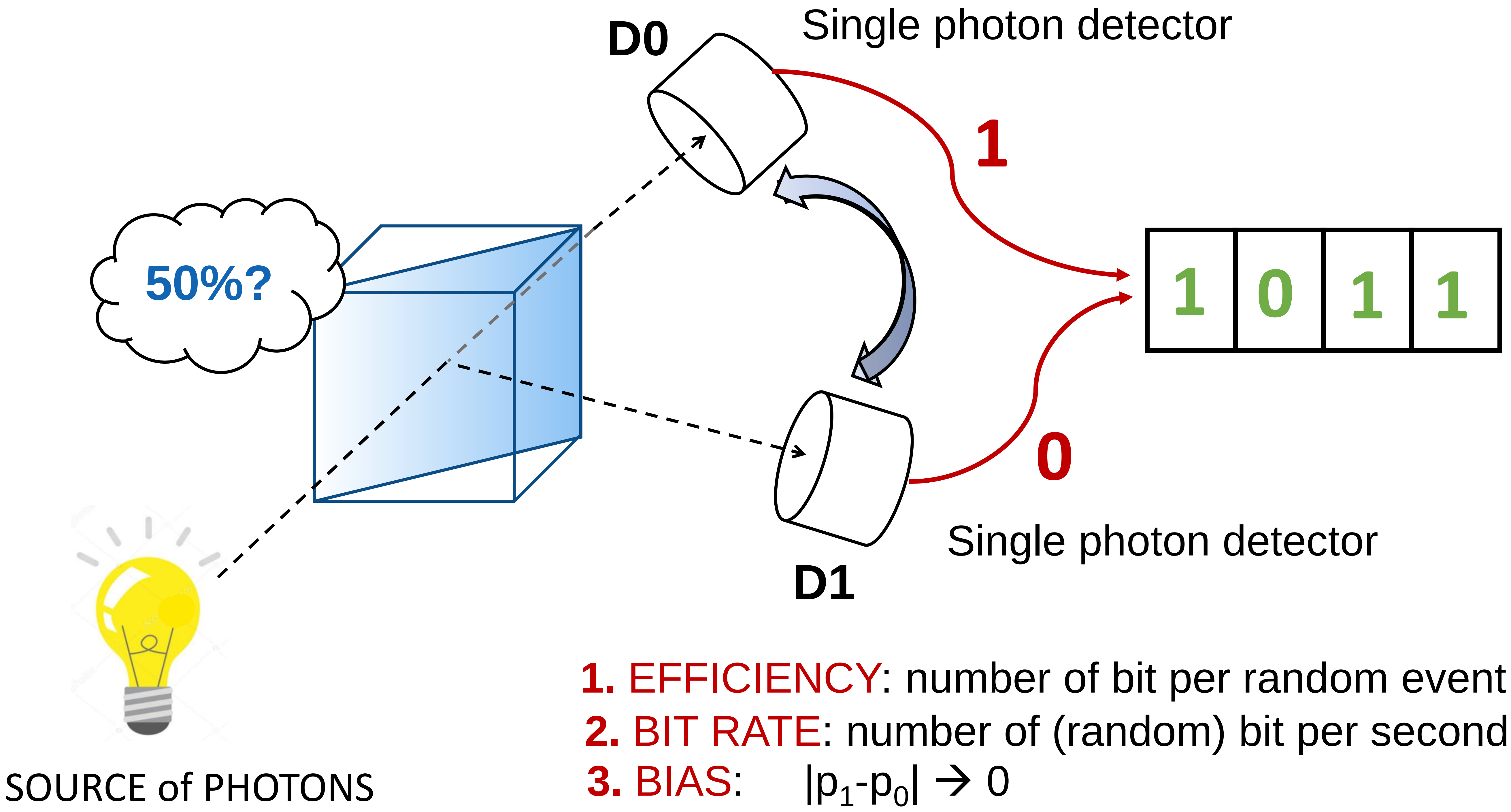



# Quantum Random Number Generator
## A prototypical QRNG

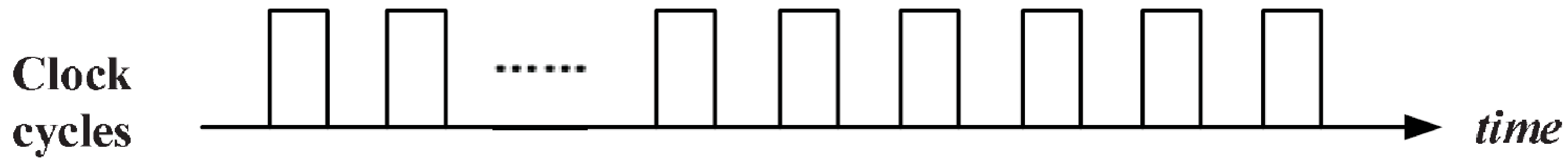


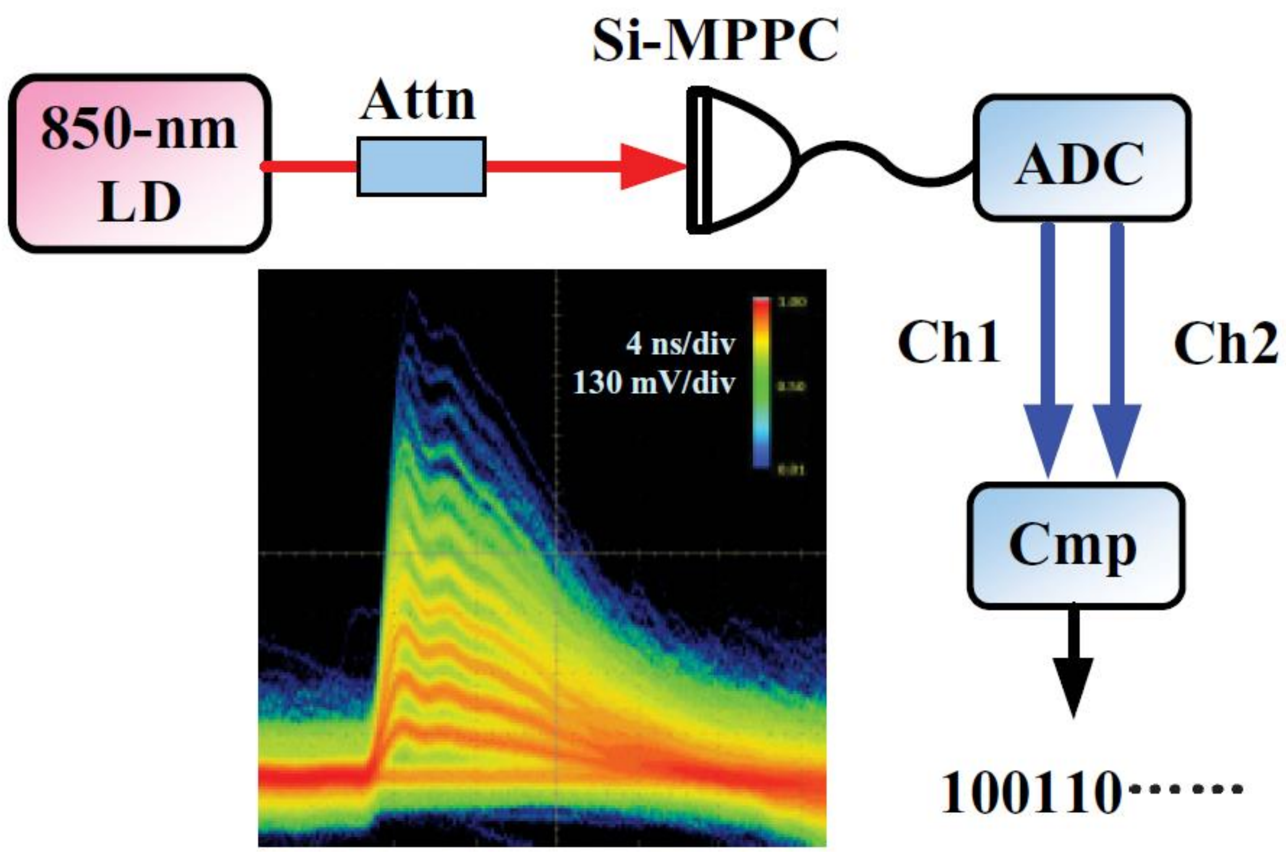
# Quantum Random Number Generator
## Main parameters




1. EFFICIENCY: number of bit per random event (detected ph)
2. BIT RATE: number of (random) bit per second
3. BIAS: $|p_1 - p_0| \rightarrow 0$
4. ENTROPY: $H(X) = -\sum_i p_i \log(p_i)$

# QRNG based on photon counting
## Single SPAD with external laser




$$P(N) = \frac{(\lambda T)^N e^{-\lambda T}}{N!}$$

The efficiency η of random bit generation is equal to

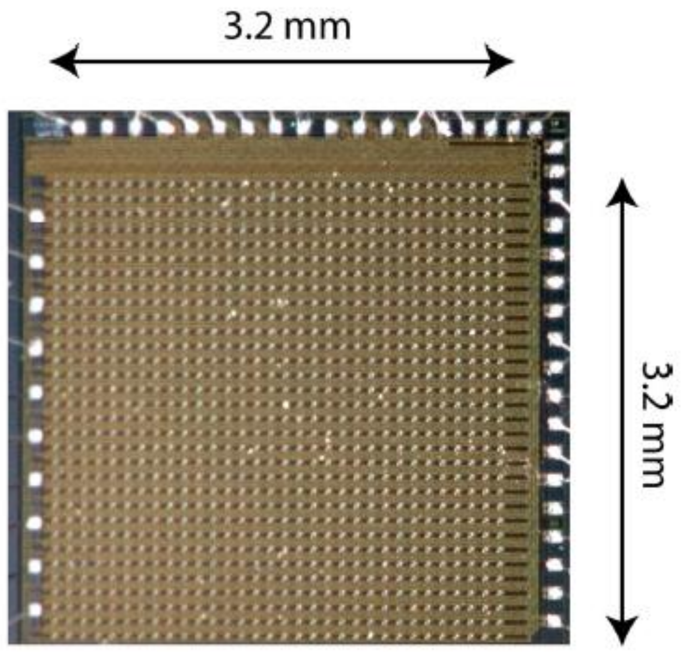
→ maximum 50% if a counter with N → ∞

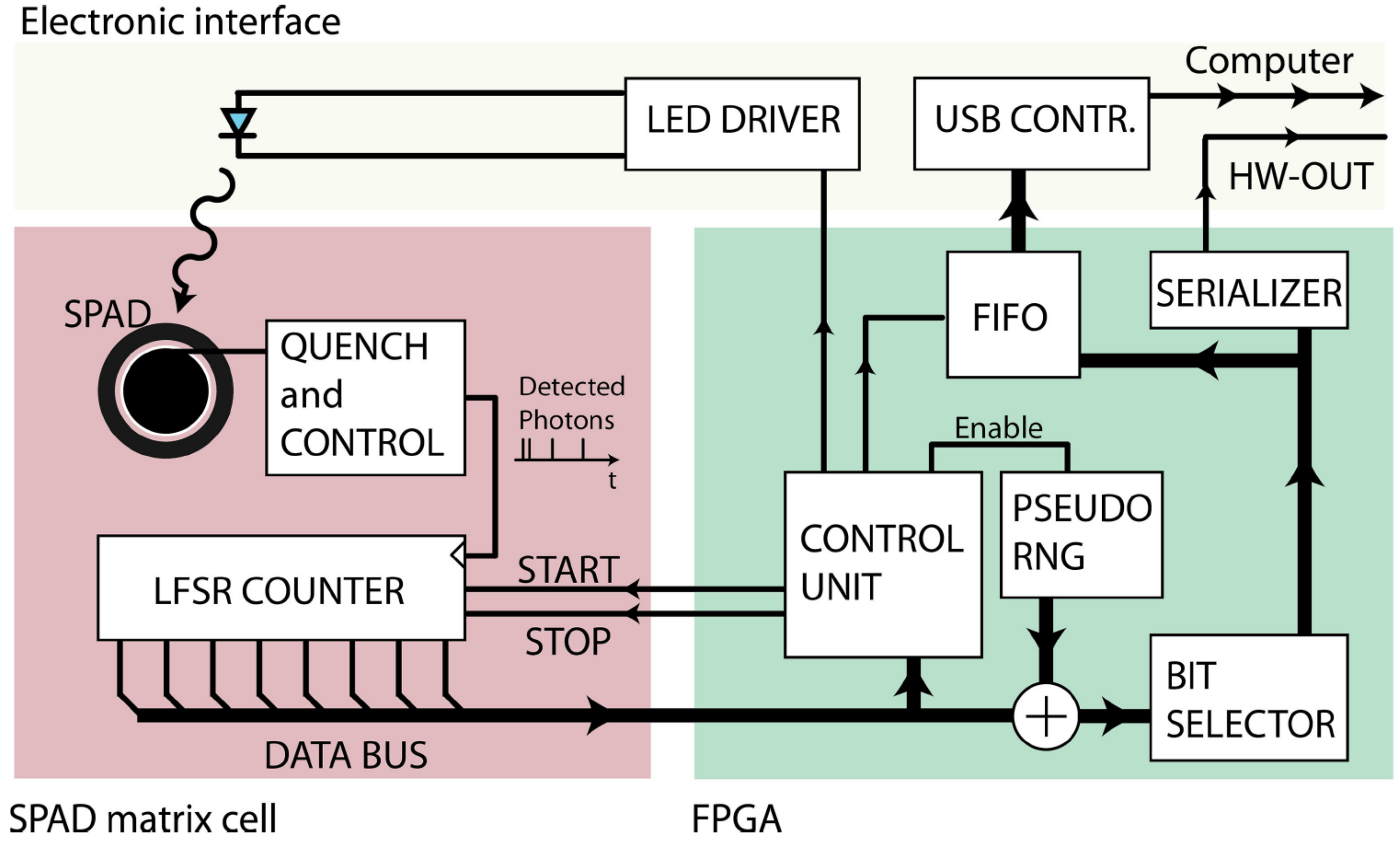
$$\eta = \frac{P(1) + P(0)}{2}$$

η is reduced because of the probability of $n_{i+1} = n_i$ → no random bit generation

*[Ren11]*

# QRNG based on Photon Counting
## QRNG by MPD


*[Tisa15]*

Up to 200 Mbps

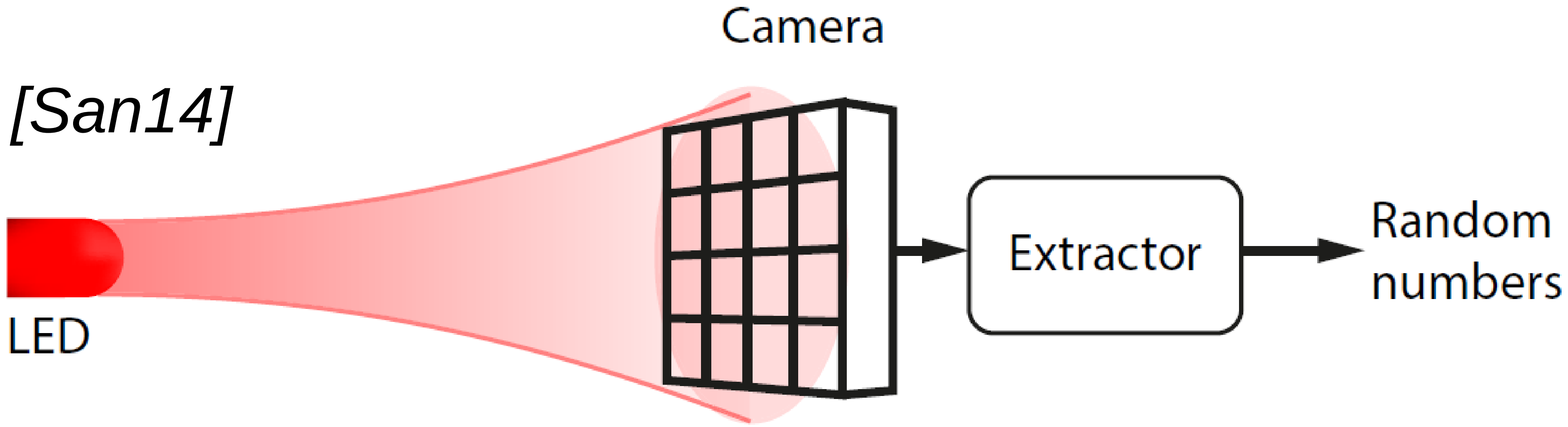
QRNG produced by MPD is based on an array of 32x32 SPAD cells connected to a photon counter. For high counts ($\lambda$>>10), the Poisson is ~ a Gaussian distribution with std equal to $\sqrt{\lambda}$. Choosing the LSB (parity bit) whitens the distribution. We can extend to more LSBs always guaranteeing a min entropy ~ $1/2\log_2(2\pi\lambda)$

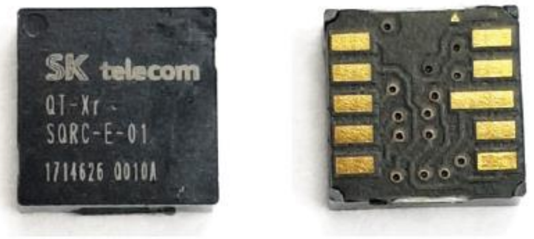
# QRNG based on Photon Counting
## IdQ product

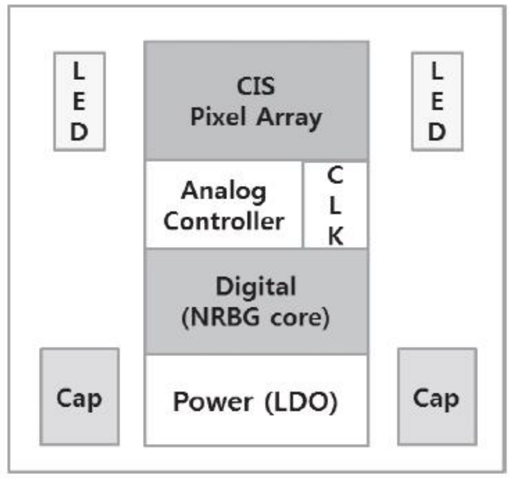
QRNG based on a standard digital camera.
The pixel value is dominated by shot noise and approximates well a Poission distribution

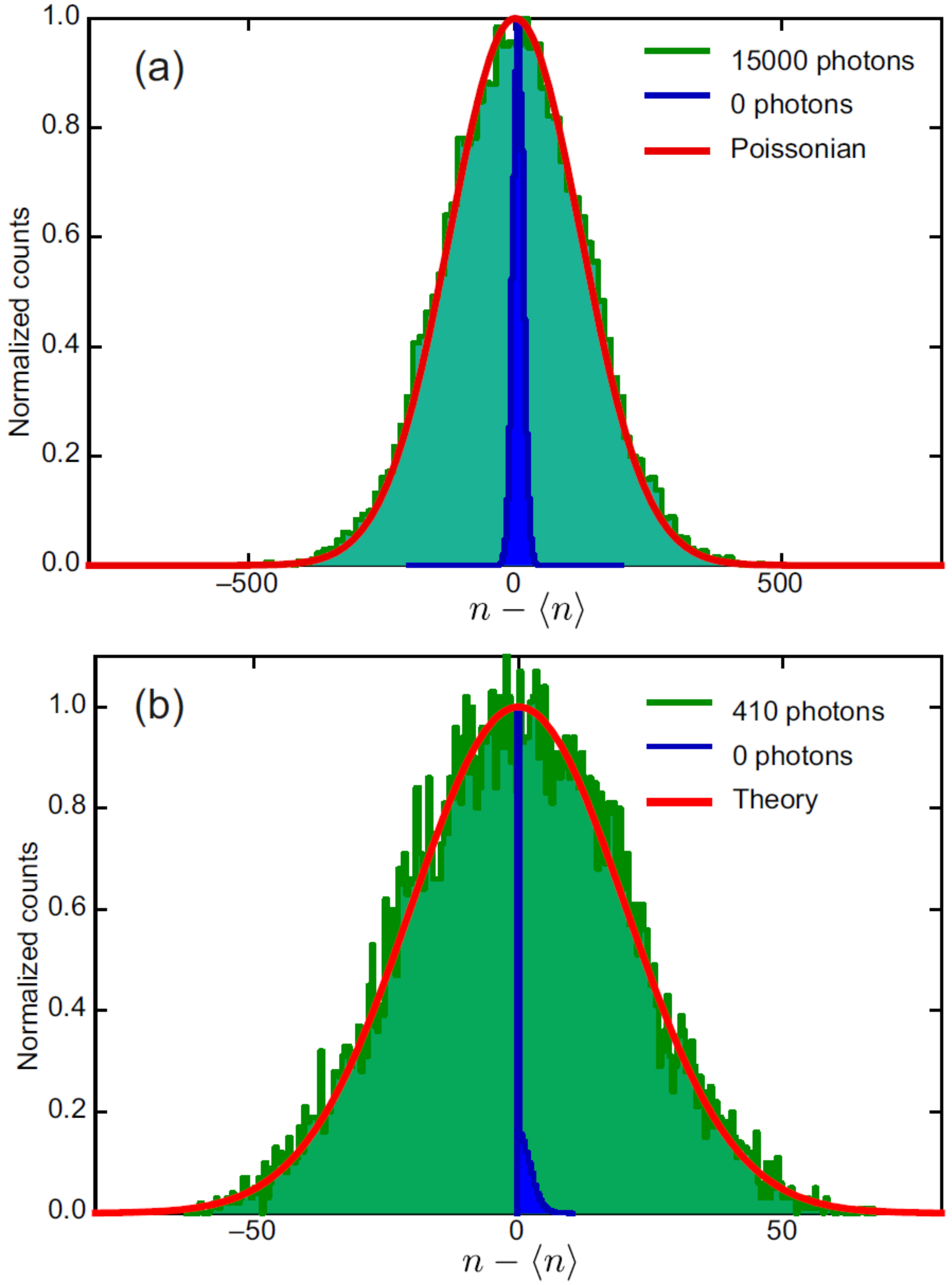
100 Mpixel → 3 bits per pixel → 0.3 up to 3 Gbps

*[San14]*

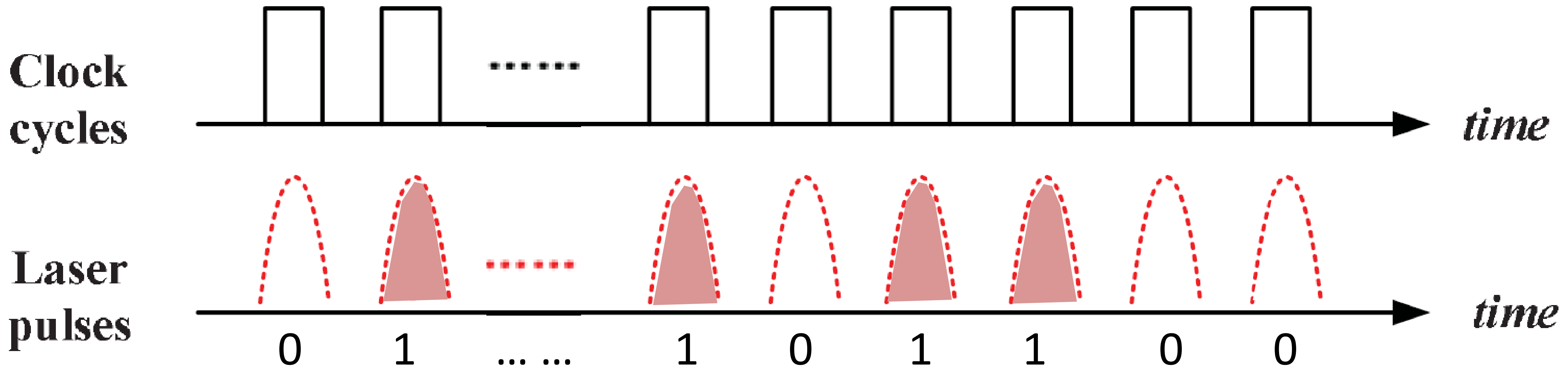


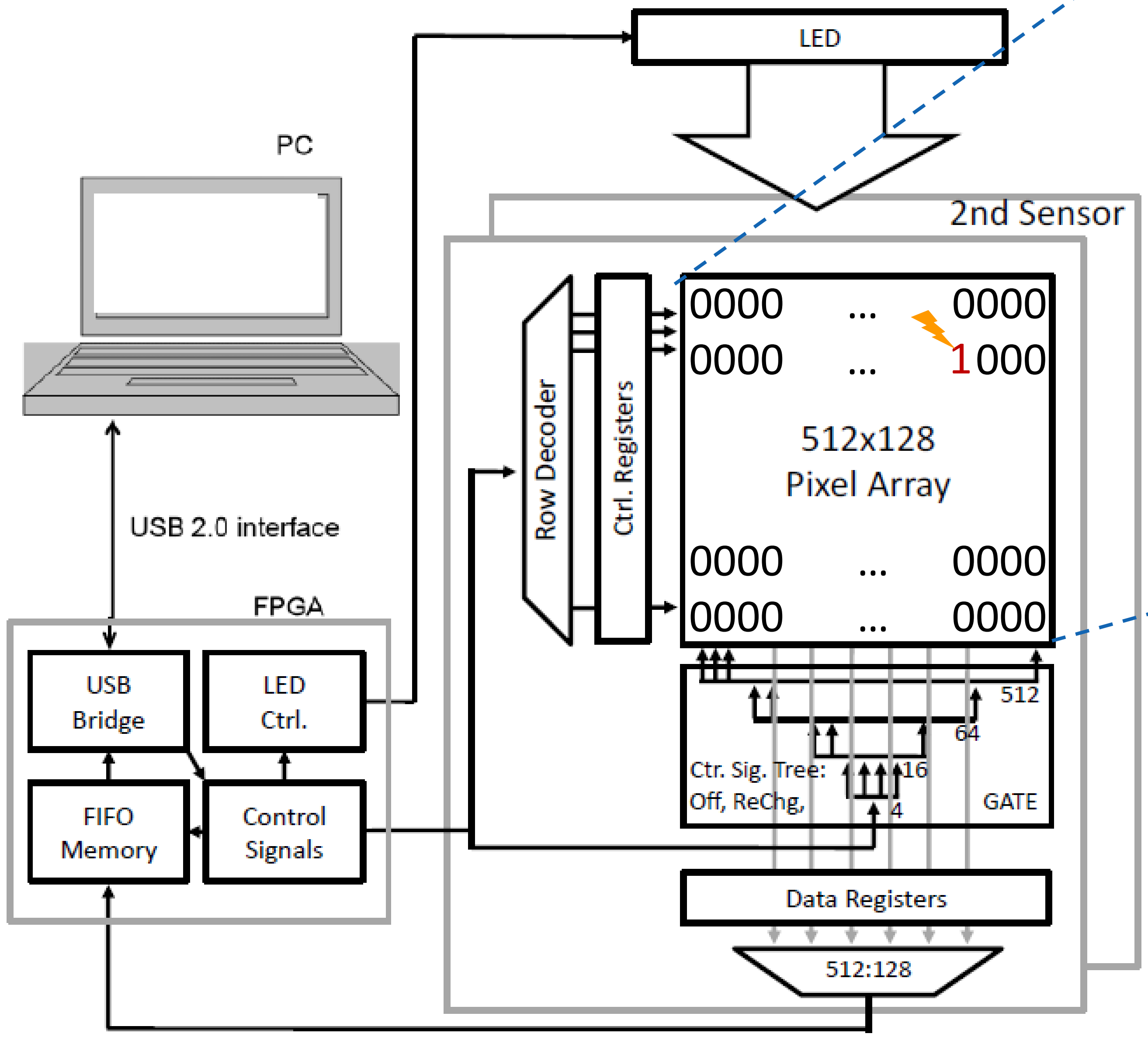



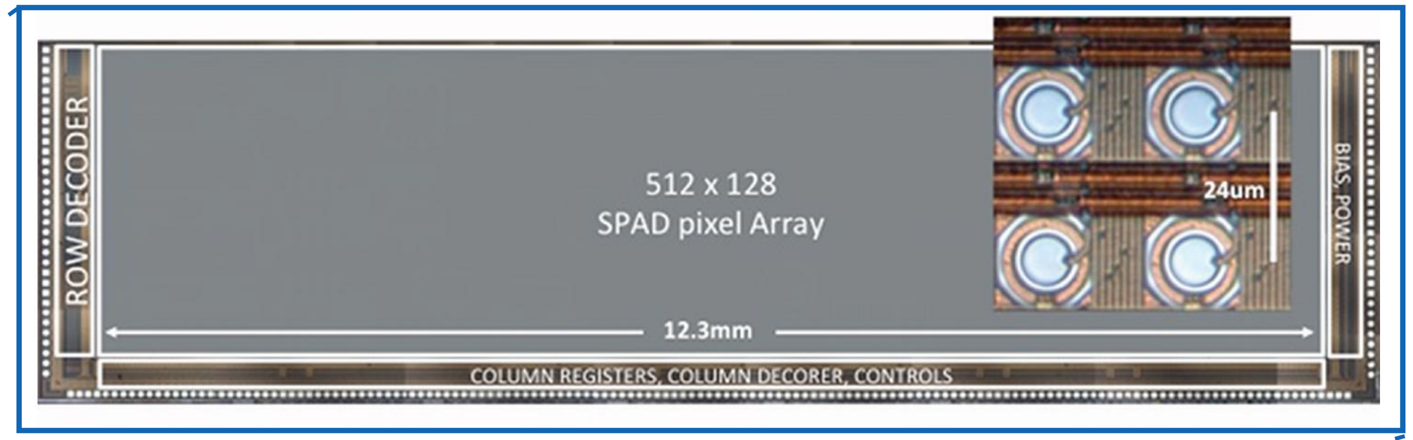
# QRNG based on photon counting
## Particular case when N=1

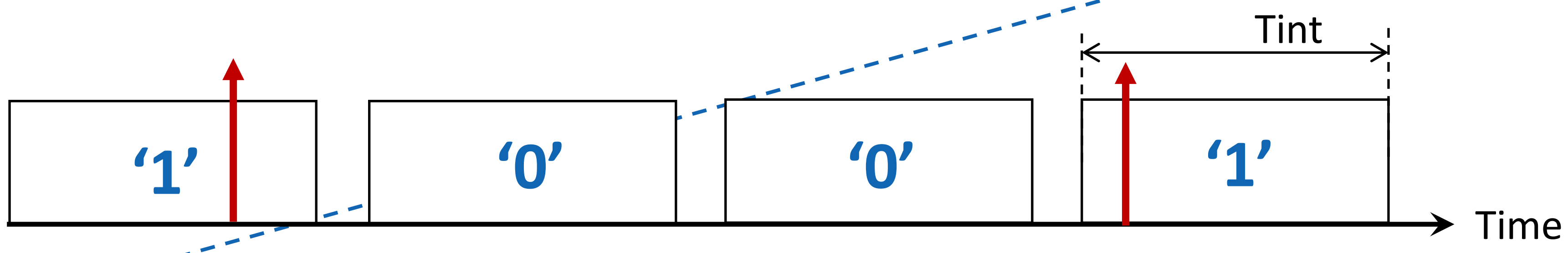



*[Wei18]*

# QRNG based on photon counting
## Fast (Gbps) binary single photon imager



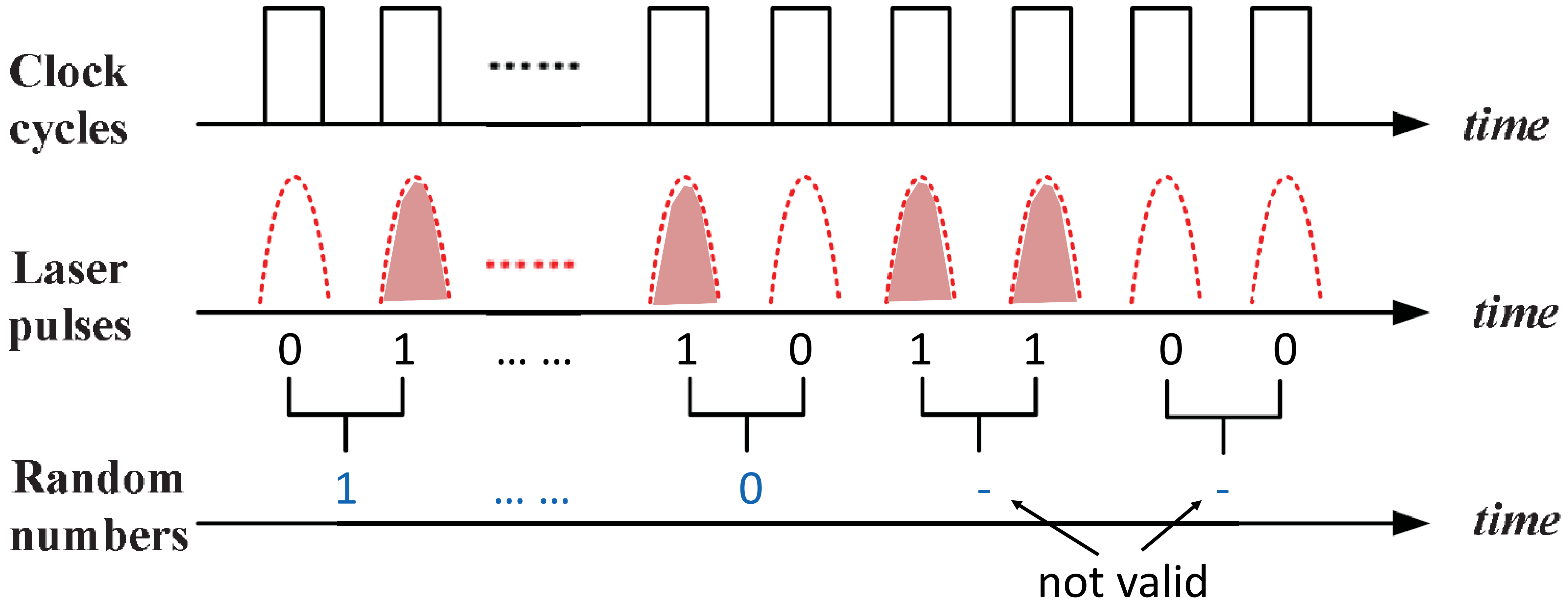




- Array of 512x128 pixels each having a SPAD
- Every cell of the array is reset to '0' and when it detects an event changes state ('0' → '1')

**5 Gb/s** maximum speed

*[Burri13]*

# QRNG based on photon counting
## Particular case when N=1 --> Von Neumann filter

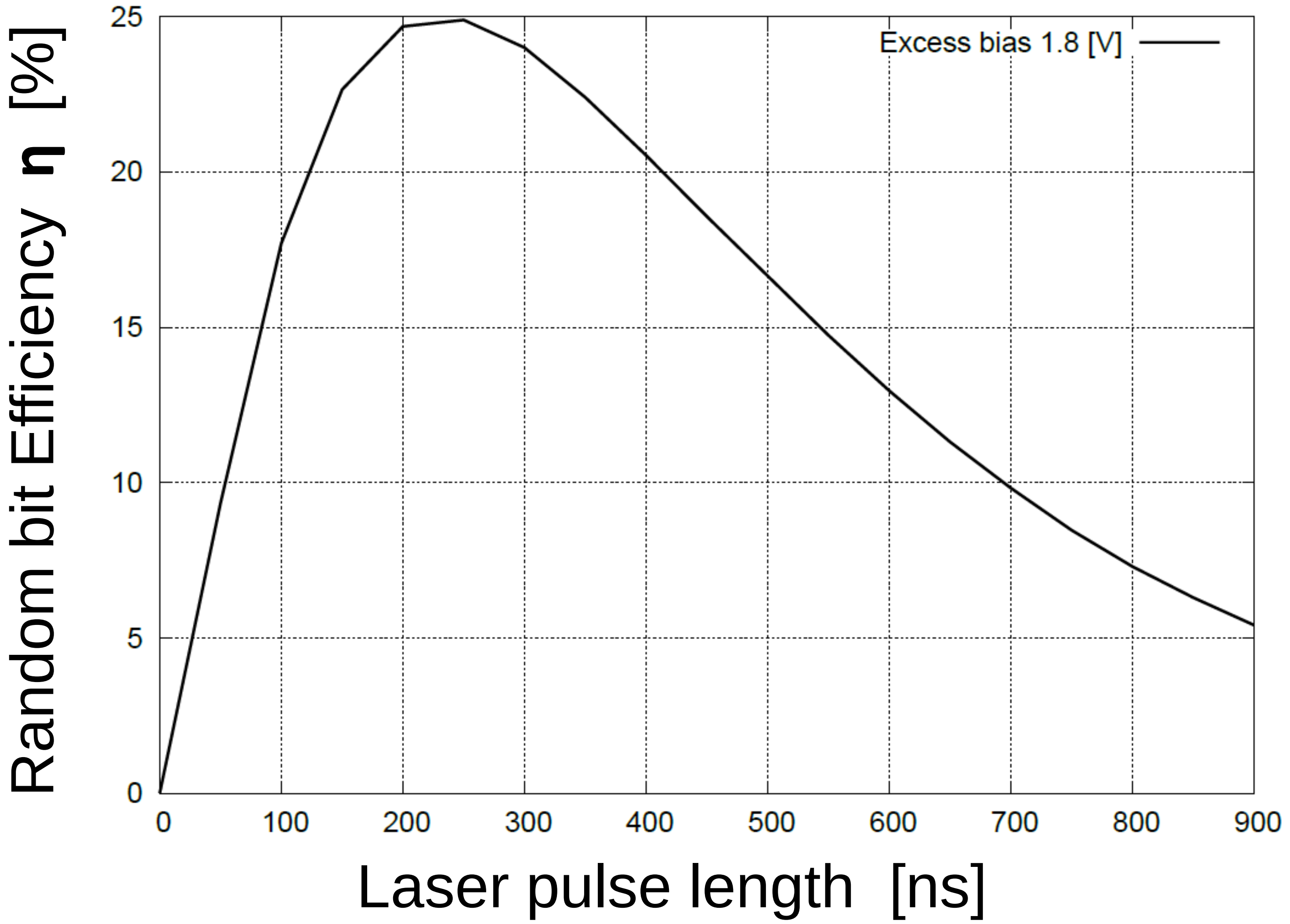



$$\eta = \frac{P('1') + P('0')}{2} = e^{-\lambda T} \cdot \left(1 - e^{-\lambda T}\right)$$

*[Wei18]*

Apply the Von Neumann filter to raw data: the maximum efficiency η=0.25 is reached at λT=ln2 ≈0.693 representing the value where probability of zeros and ones are equal

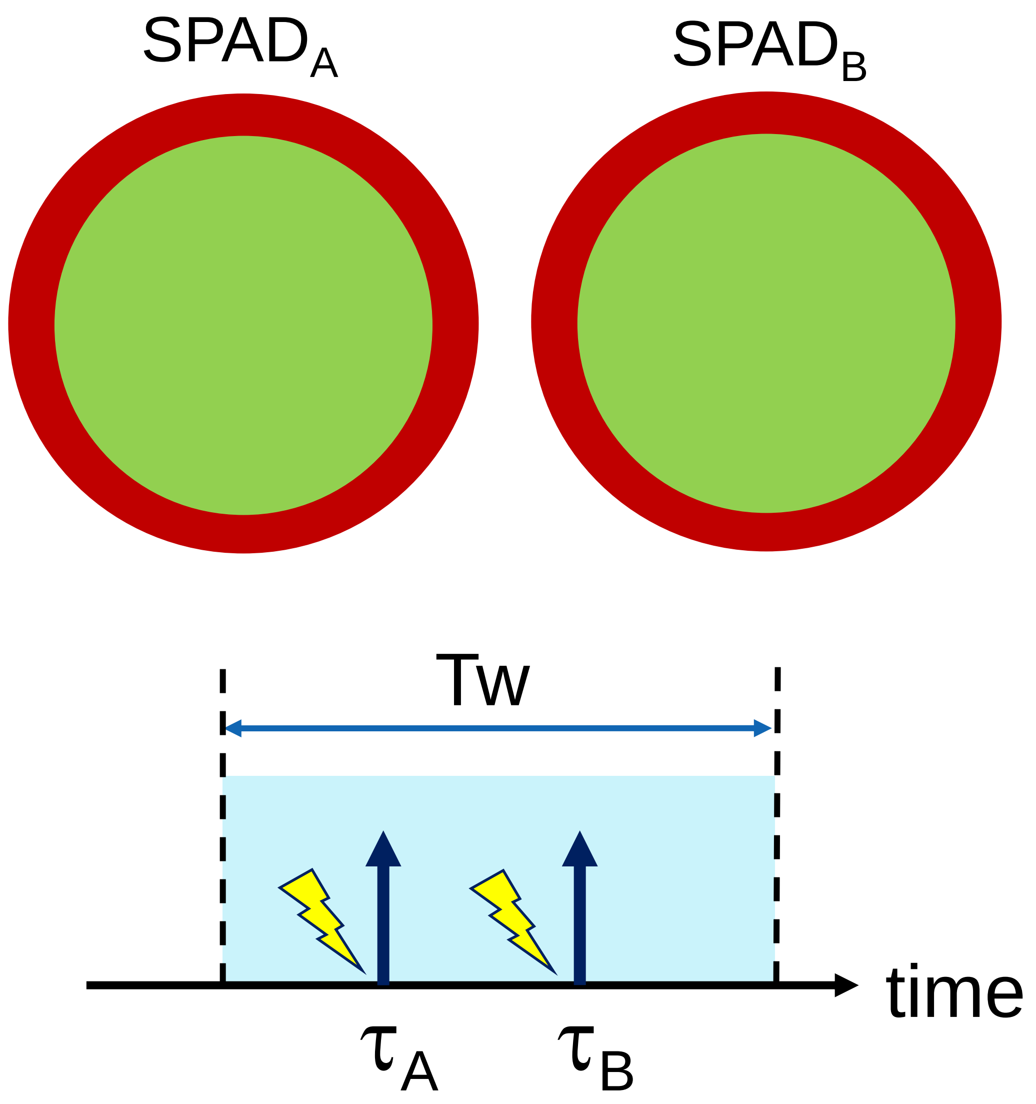
# QRNG based on photon counting
## Performance variation

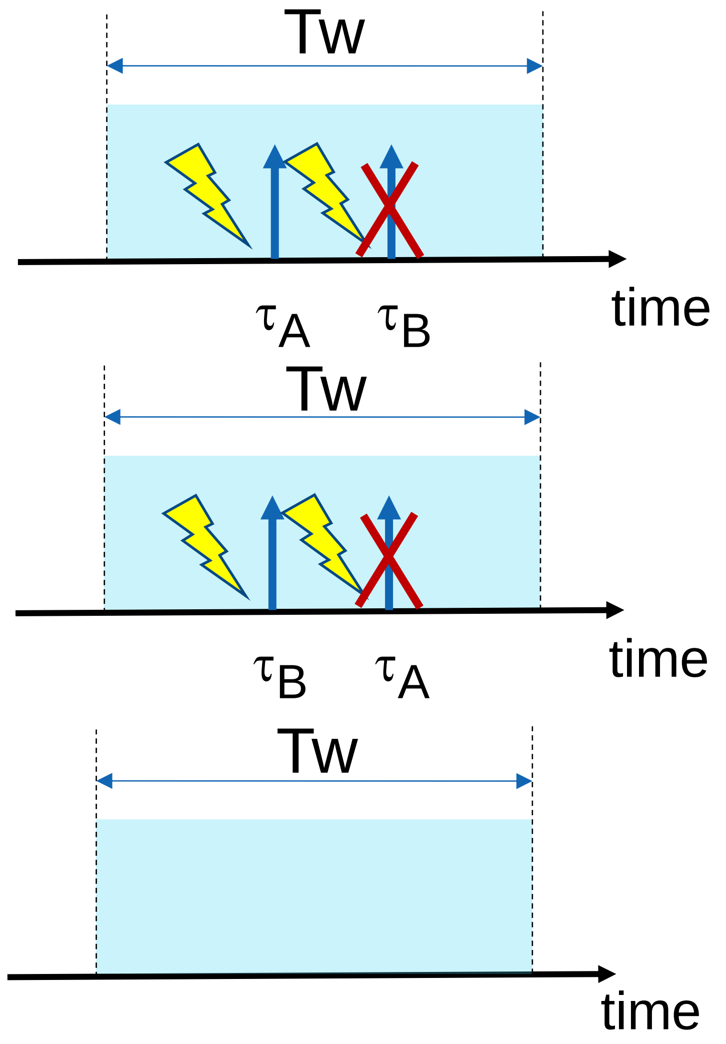



- The QRNG efficiency strongly depends on the flux of photons detected by every cell
- Difficult to guarantee a uniform behavior across the array
- May depends on aging or drift of the source of light

# QRNG based on the arrival time
## First detected photon

Let's consider a couple of SPAD with same size one close to the other

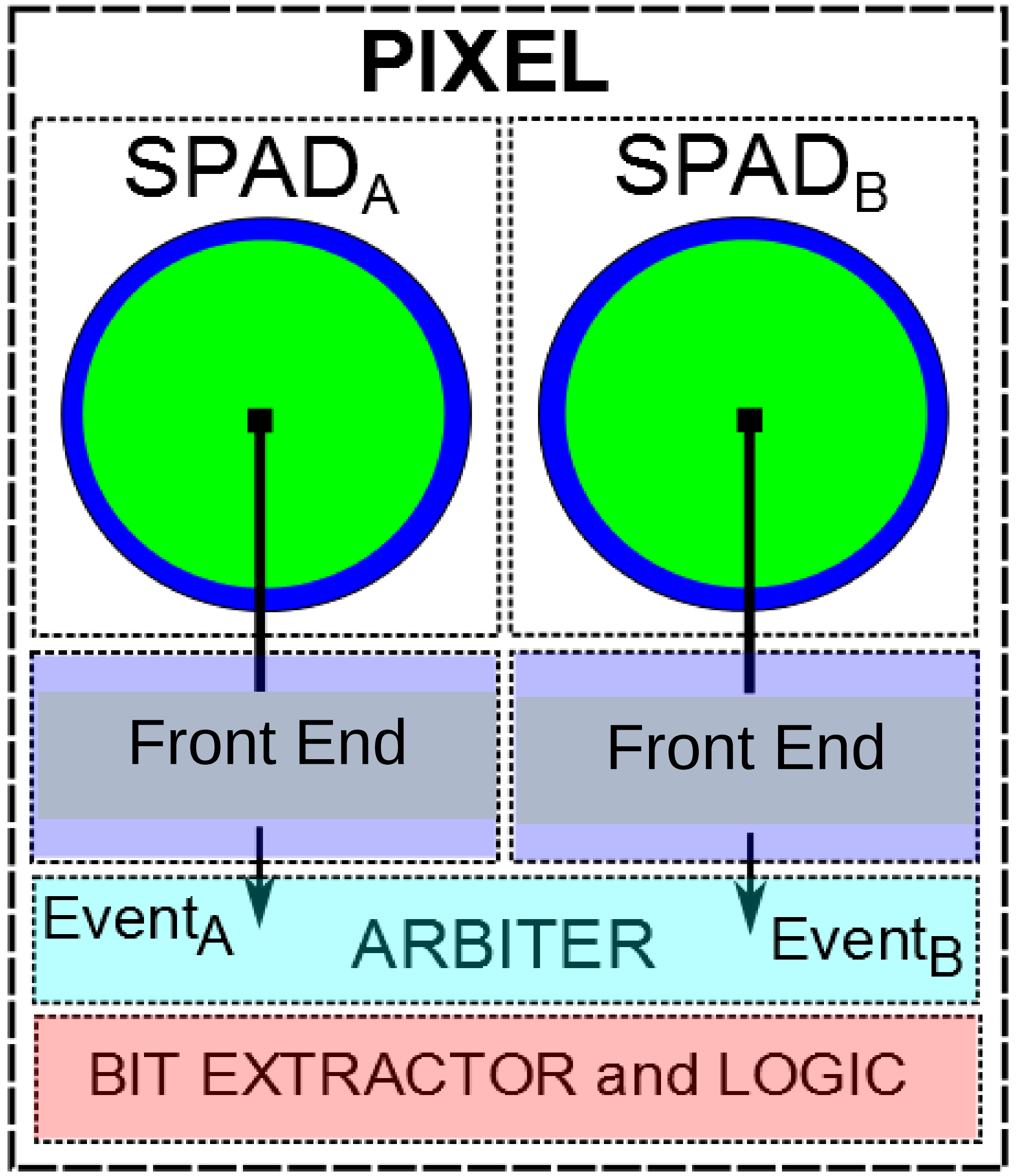



| **Output** | **When** |
|---|---|
| Bit '**1**' | $\tau_A < \tau_B$ |
| Bit '**0**' | $\tau_B < \tau_A$ |
| **No out** | **no event detection** |

*[Mas16]*
*[Xu18]*

# QRNG based on the arrival time
## First detected photon




- Competition between $SPAD_A$ and $SPAD_B$
- An arbiter has to identify the winner: $r_b = \begin{cases} '0' & if\ \tau_A > \tau_B \\ '1' & if\ \tau_A < \tau_B \end{cases}$

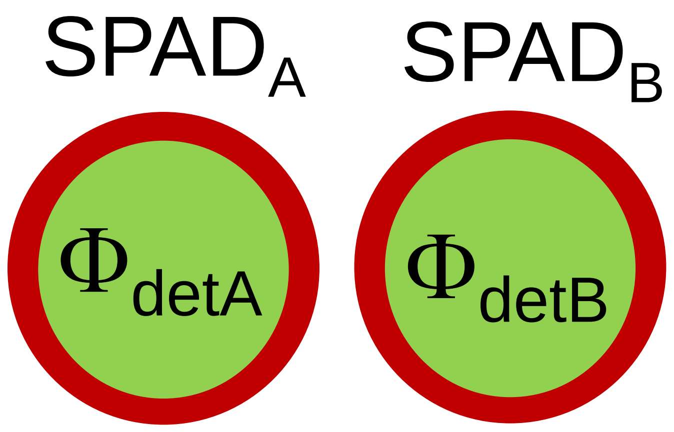
$$\begin{cases} P(\tau_A \leq t) = 1 - e^{-\Phi_{detA} t} \\ P(\tau_B \leq t) = 1 - e^{-\Phi_{detB} t} \end{cases}$$

$$\Rightarrow \boxed{P(\tau_A \leq \tau_B) = \frac{\Phi_{detA}}{\Phi_{detA} + \Phi_{detB}}}$$

If $\Phi_{detA} = \Phi_{detB}$ $\Rightarrow$ $P(\tau_A < \tau_B) = P(\tau_B < \tau_A) = 0.5$

# QRNG based on arrival time
## Source of bias: cell behaviour

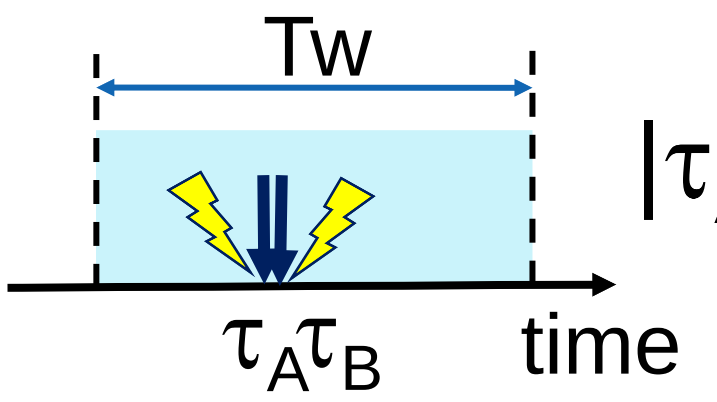
1.Mismatch between the two SPADs




- 1. Dark Count Rate (DCR
- 2. Detection Probability

$\Phi_{detA} \neq \Phi_{detB}$

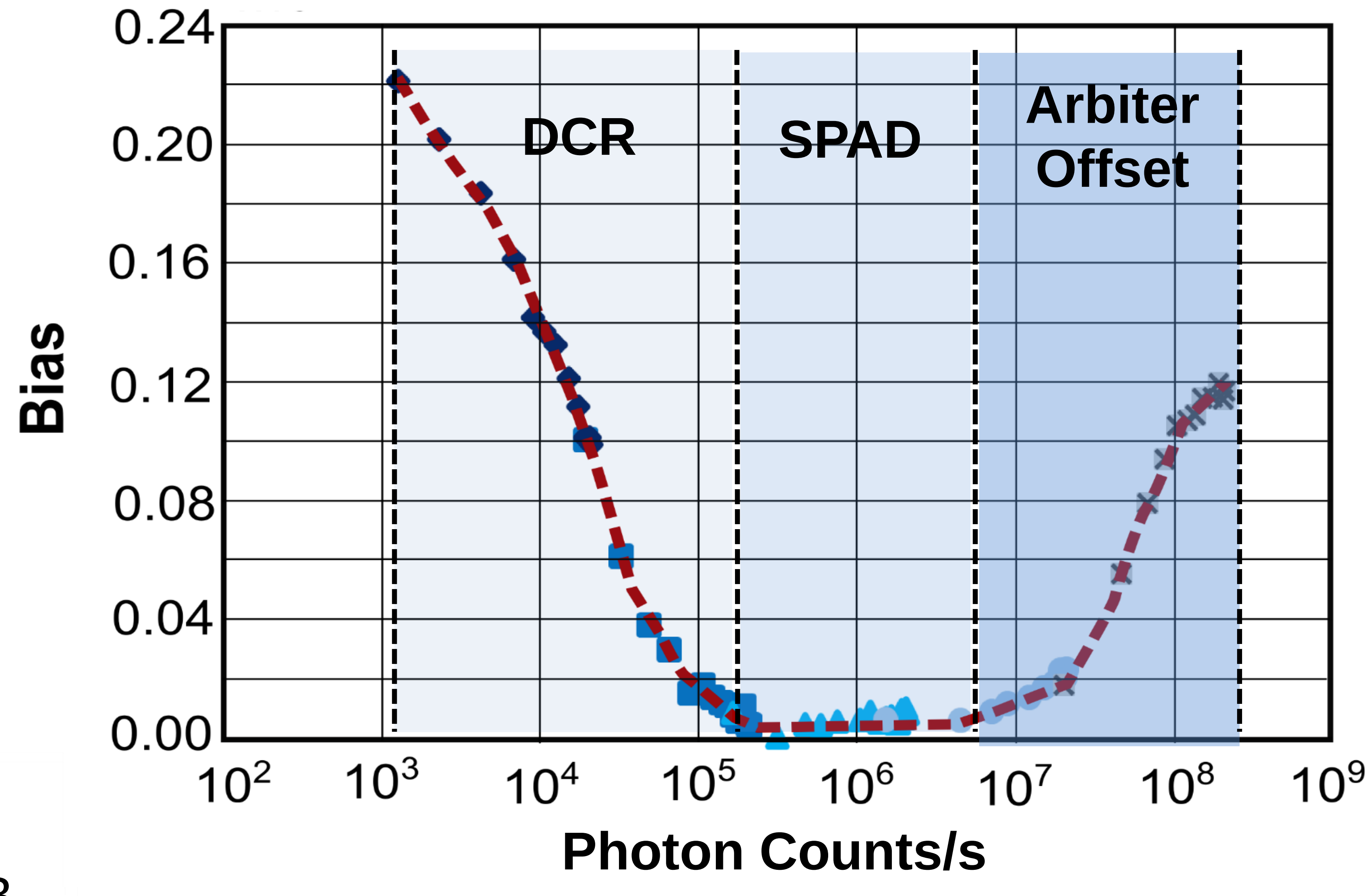
2. Circuit offset referred to the arbiter




$|\tau_A - \tau_B| < t_{OFF}$

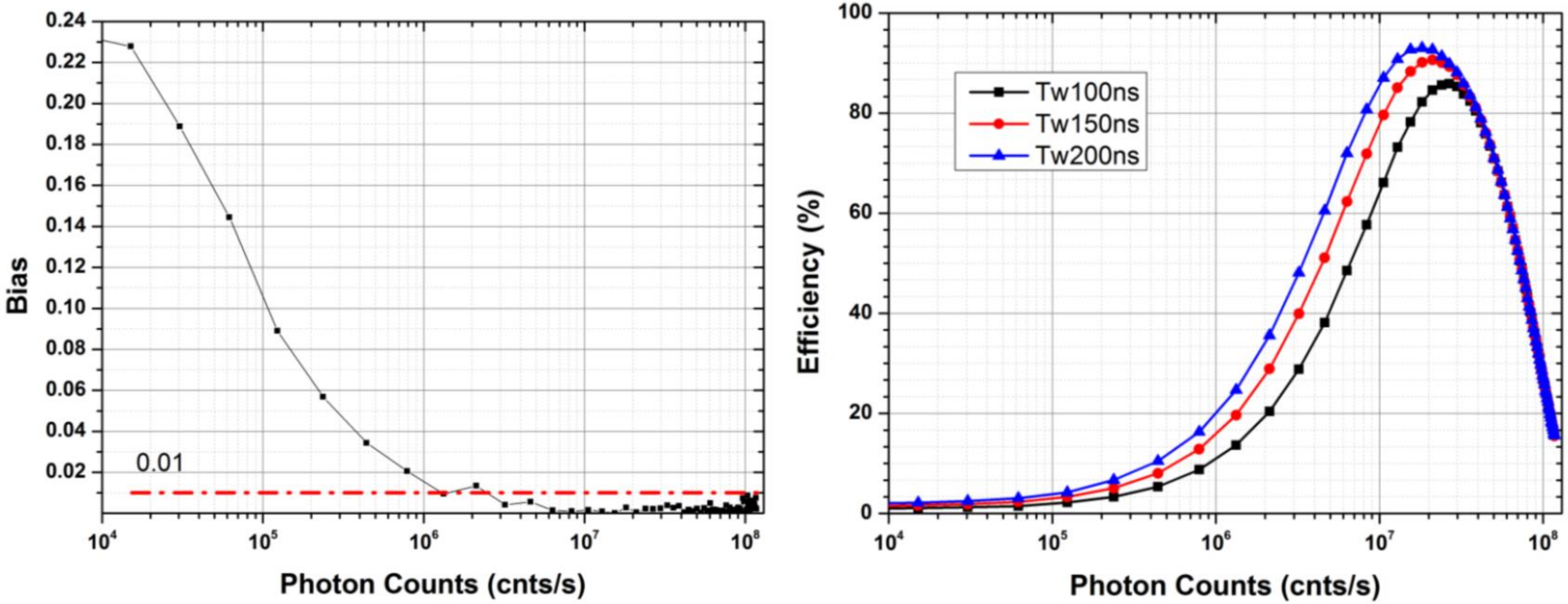
- 1.High $\Phi$
- 2. Crosstalk$_{A\leftrightarrow B}$

Mismatch due to the arbiter offset



# QRNG based on the arrival time
## Improved solution

- A circuit discards events that are too close in time:

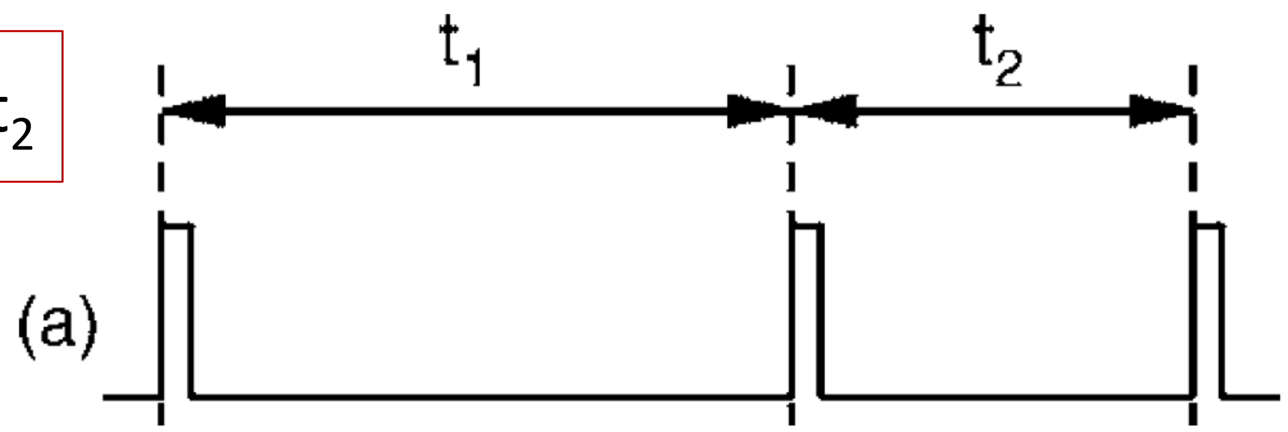



No use of TDC

Speed of 128 Mbps

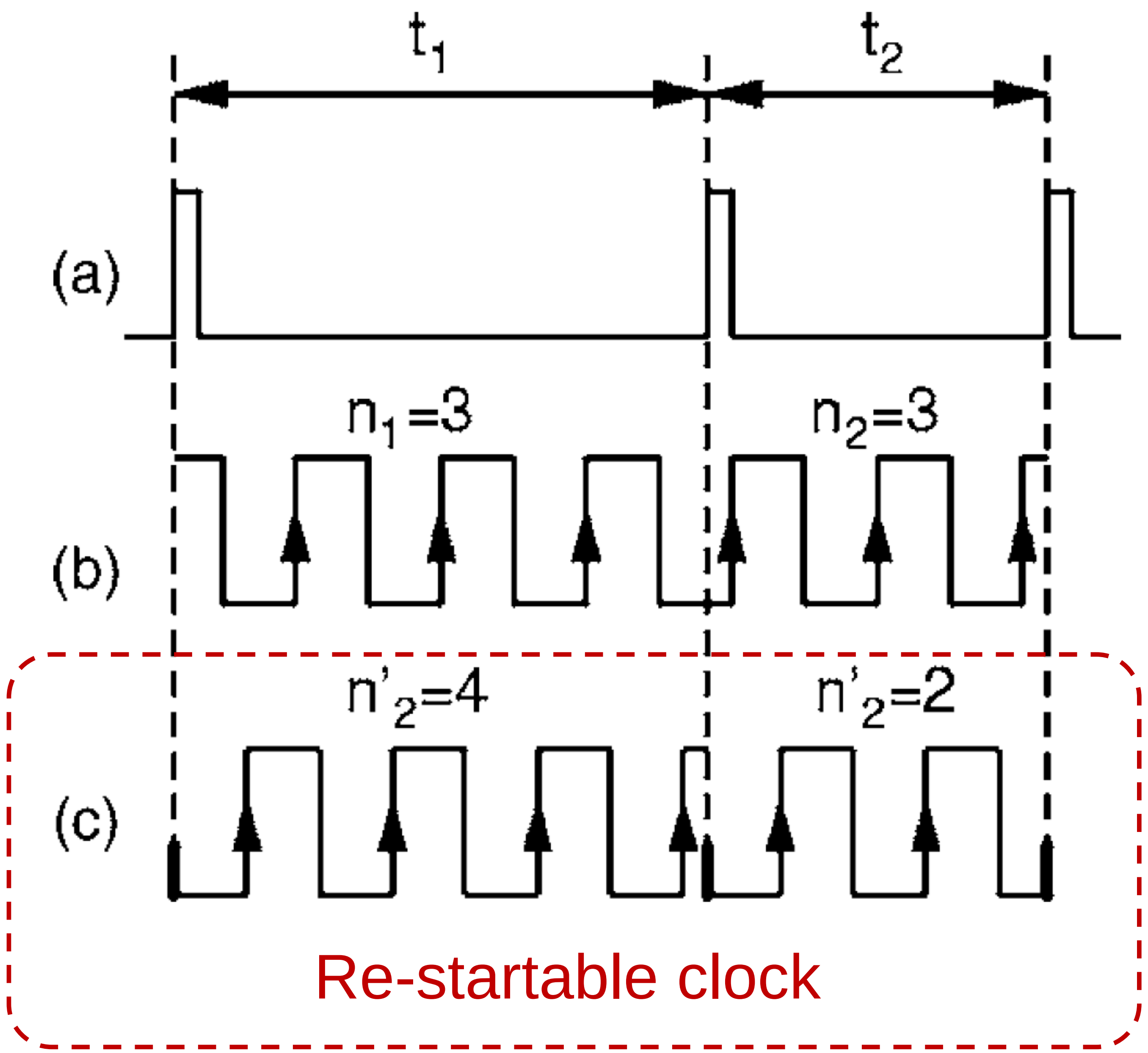
# QRNG based on the arrival time
## Time comparison

$t_1 < t_2$

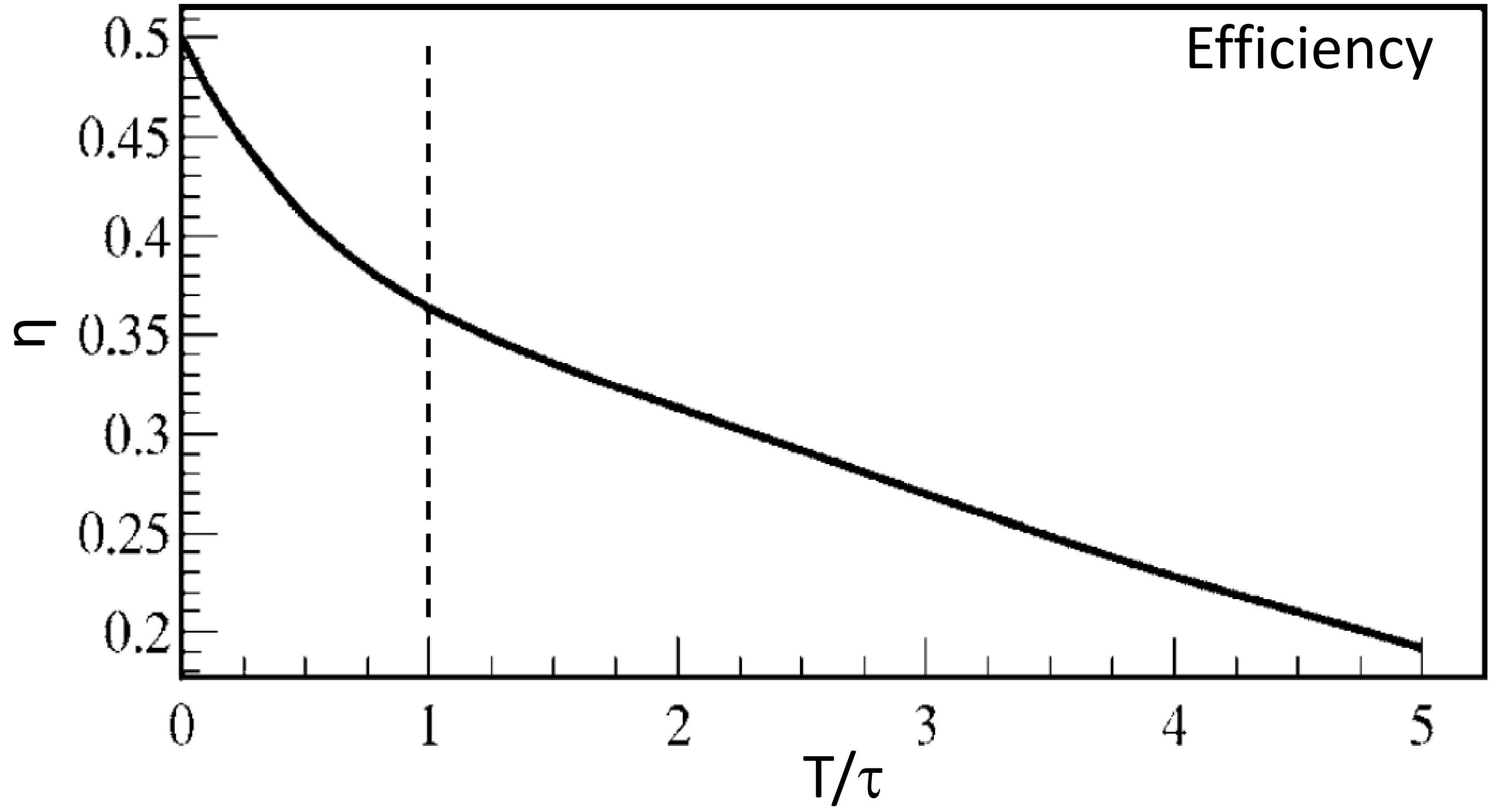



Using a frequency clock (1/T), we measure $n_1$ and $n_2$ → prob that $n_1 = n_2$ is $\neq 0$

# QRNG based on the arrival time
## Time comparison

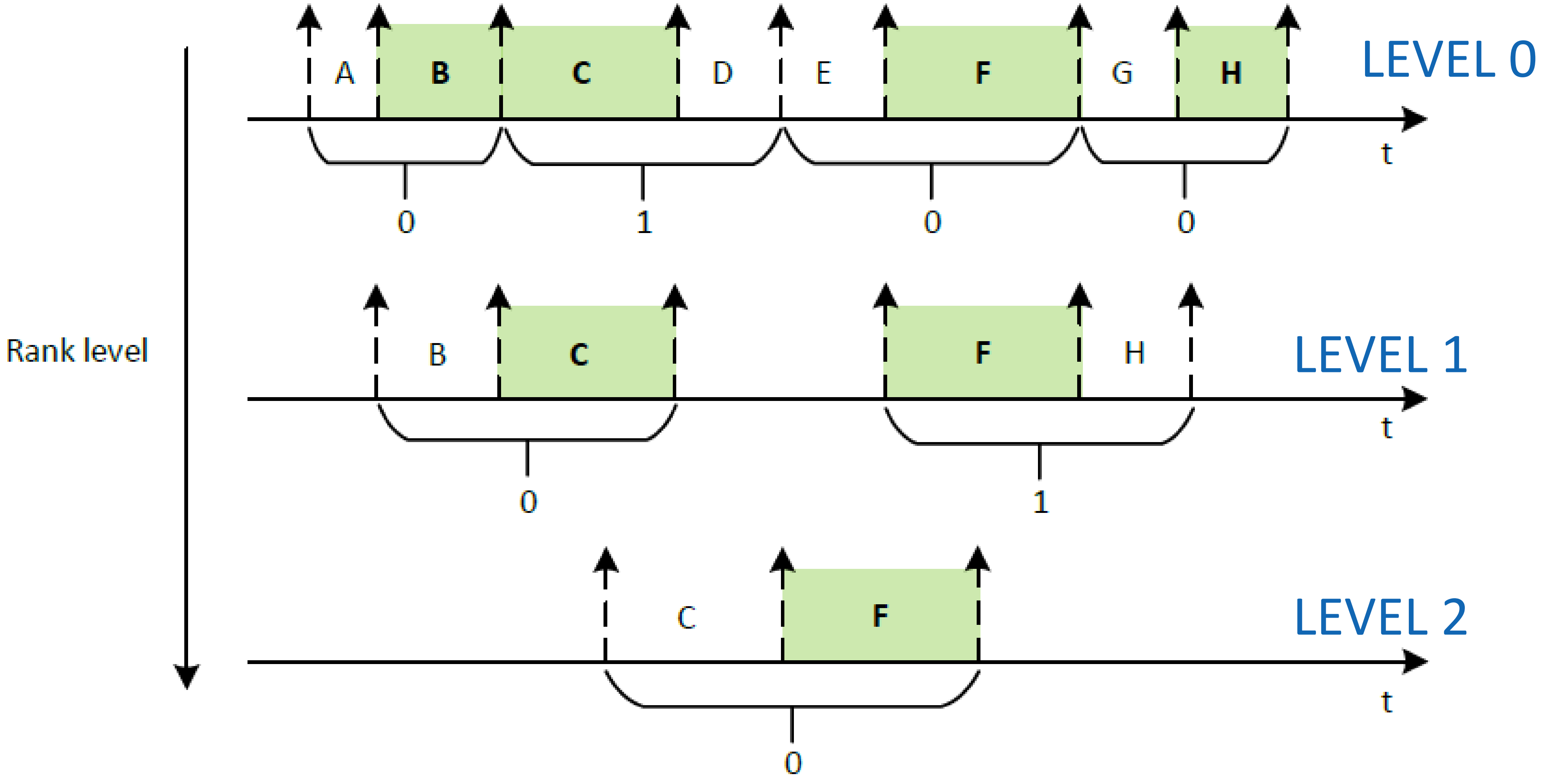



If $\tau$ is the average arrival time of events, the efficiency of the generator will be

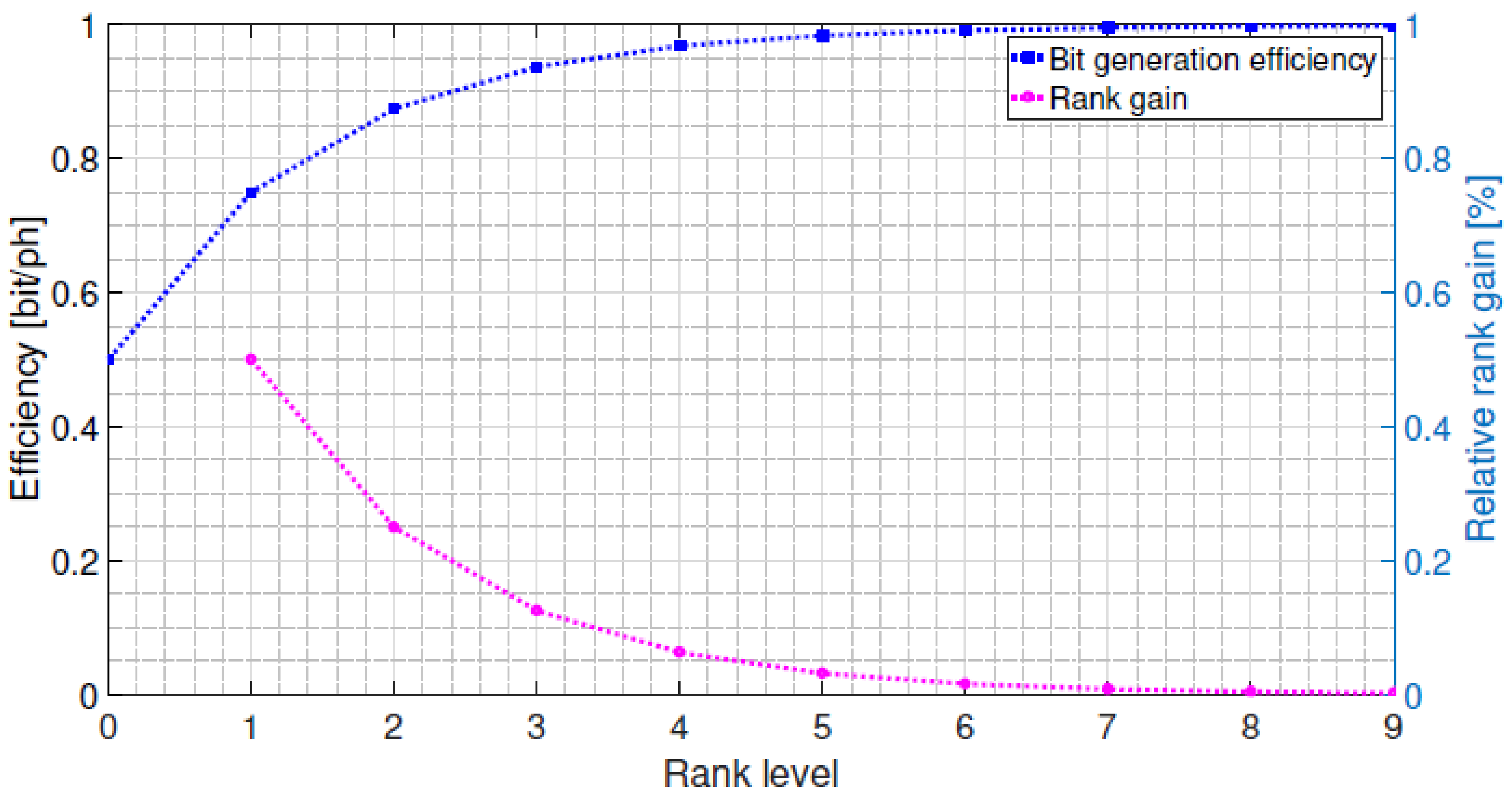


# QRNG based on arrival time
## Time comparison (extension)

Multiple ranks random number generation based on the arrival time



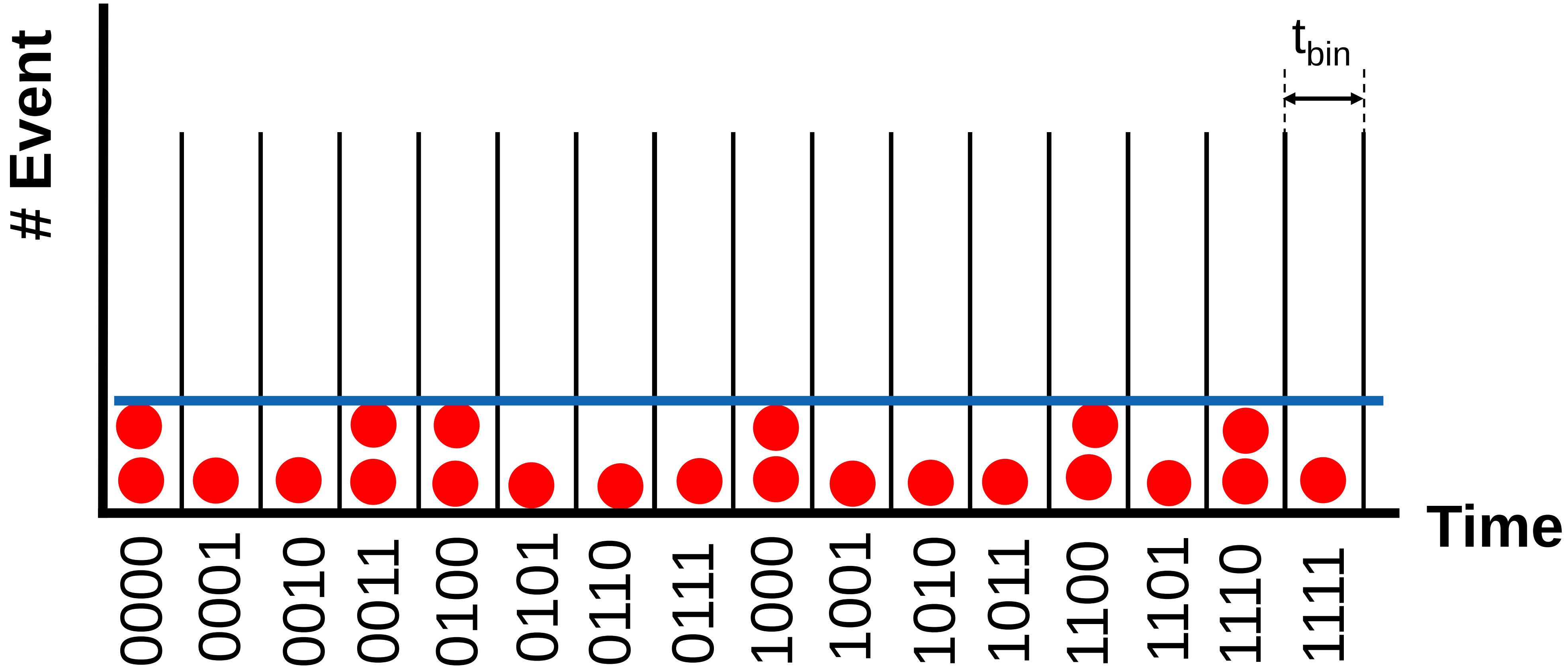

*[Ton19]*




Using 3 ranking levels we are exceeding 90% of efficiency

# QRNG based on arrival time
## Multi-bit generation

[Yan15]
[Bis17]
[Bis18]




λ = rate of events
$T_w$ = observation time window
$\lambda T_w$ = average events in Tw

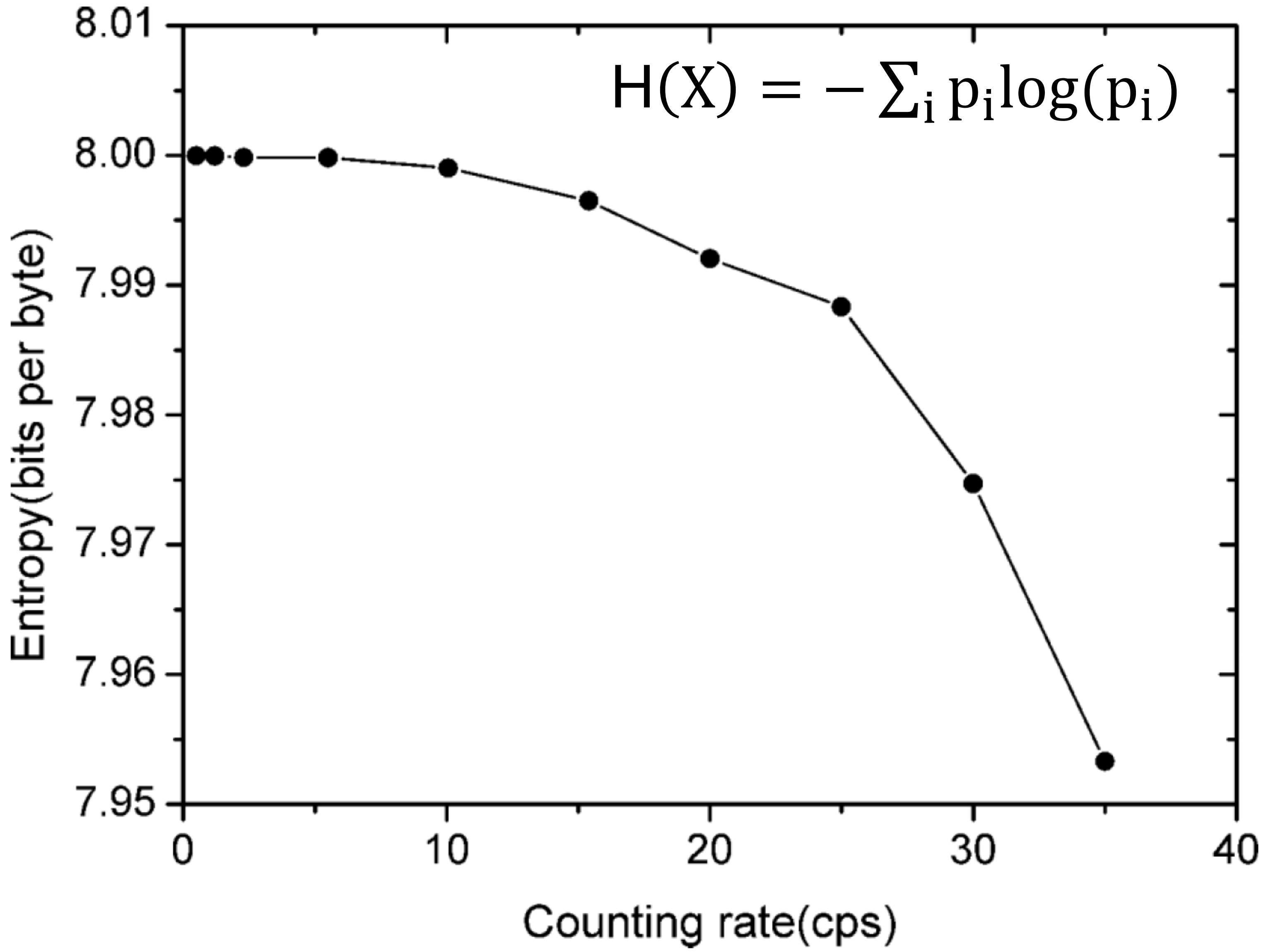
**Very low event rate**
**$\lambda T_w \ll 1$**

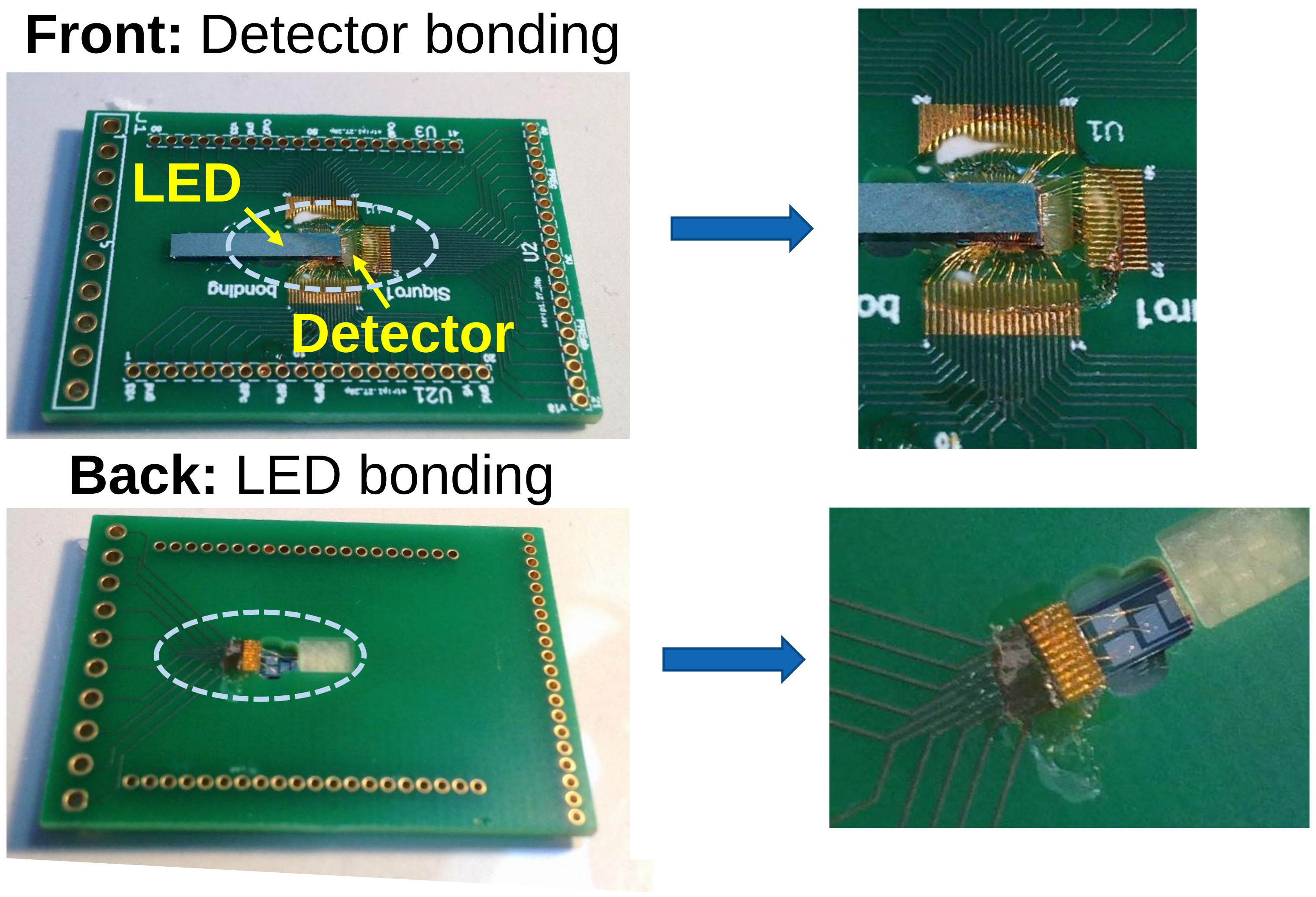
$$P\{t \le \tau |\, N(T_w) = 1\} = \frac{P\{t \le \tau, N(T_w) = 1\}}{P\{N(T_w) = 1\}} = \frac{P\{N(\tau) = 1, N(T_w) - N(\tau) = 0\}}{P\{N(T_w) = 1\}} =$$

$$= \frac{\lambda\tau \cdot e^{-\lambda\tau} \cdot e^{-\lambda(T_w - \tau)}}{\lambda T_w \cdot e^{-\lambda T_w}} = \frac{\tau}{T_w}$$

→If the flux is so low to ensure up to 1 detection per $T_w$, the arrival time is uniformly distributed in $T_w$

# QRNG based on arrival time
## Multi-bit generation



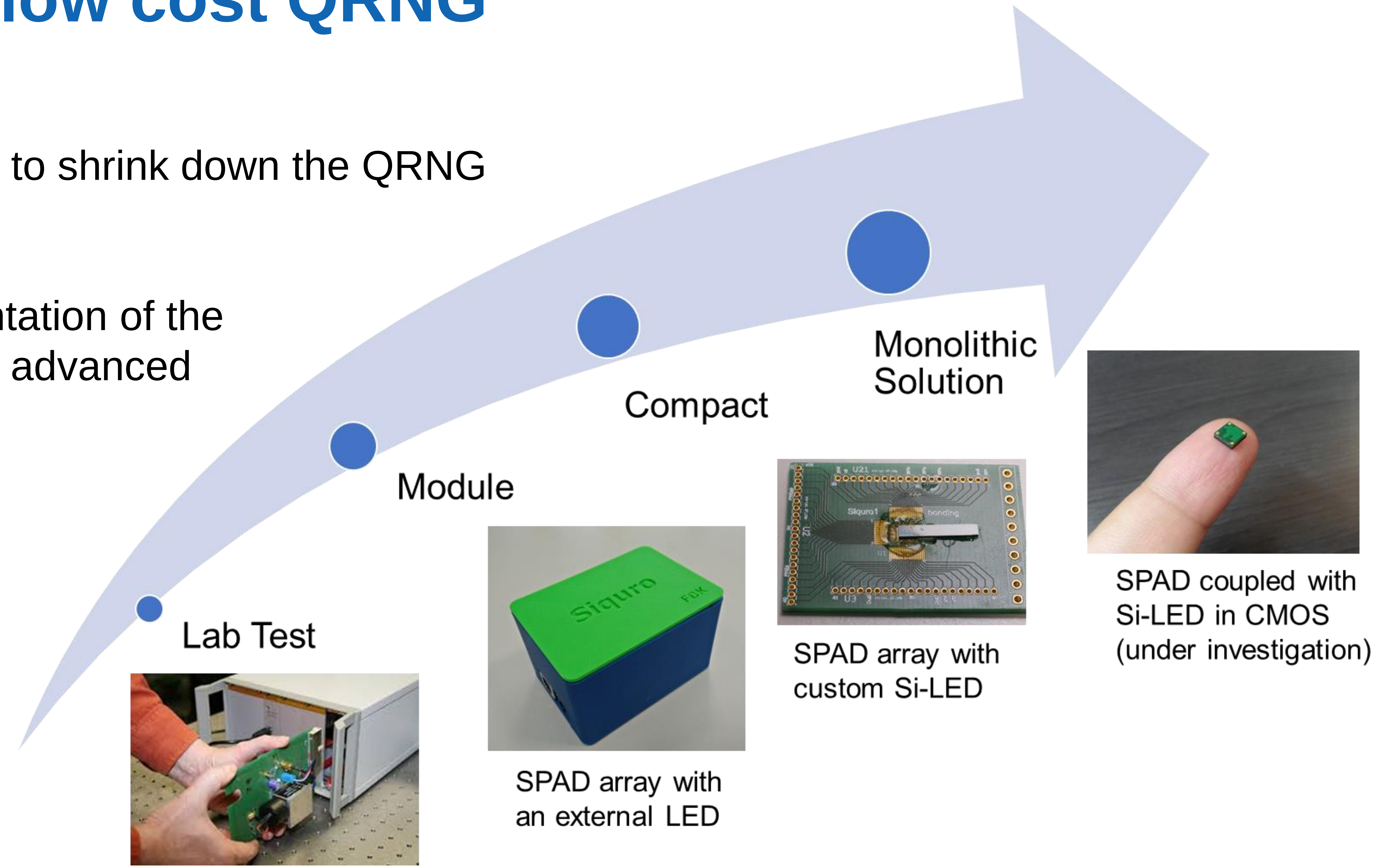

Use of an external Si-nc LED to design a compact design

*[Mas19]*

# Monolithic QRNG
## Towards a low cost QRNG

- Integration allows to shrink down the QRNG dimension and cost

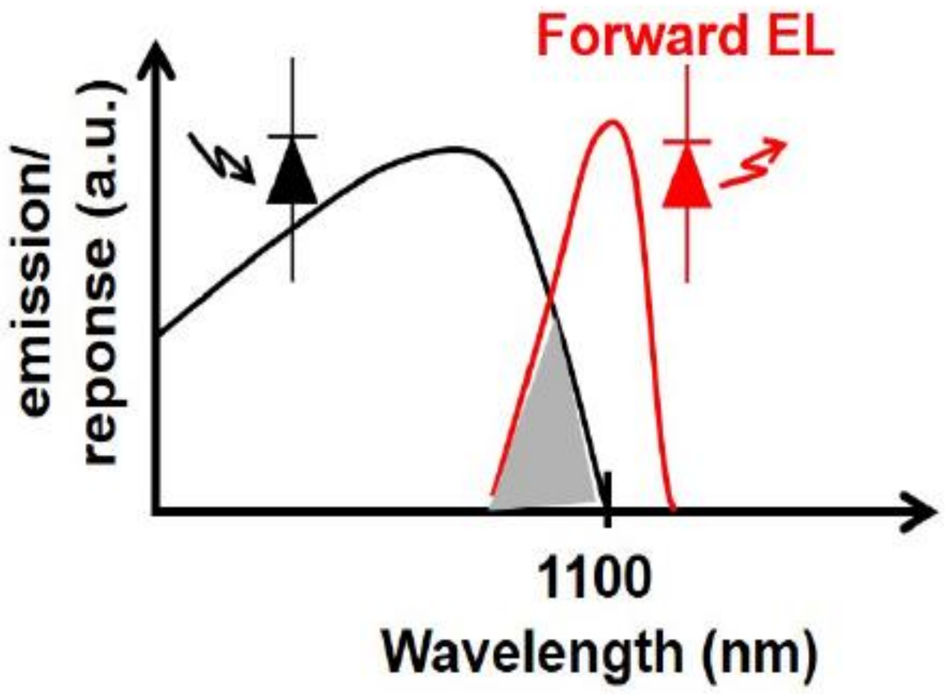
- **Target:** implementation of the QRNG in a standard advanced technology node

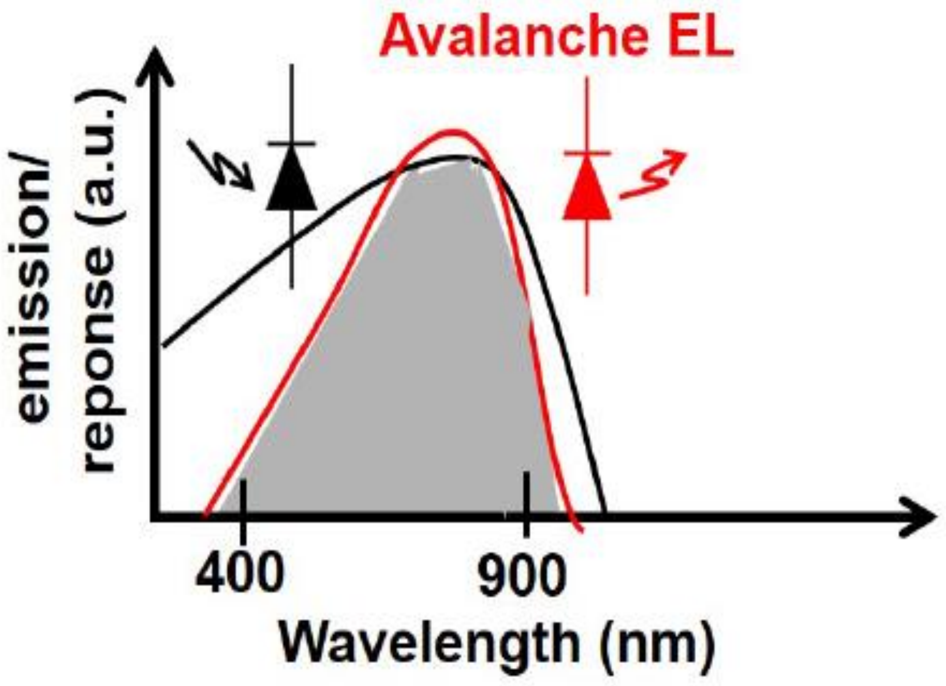


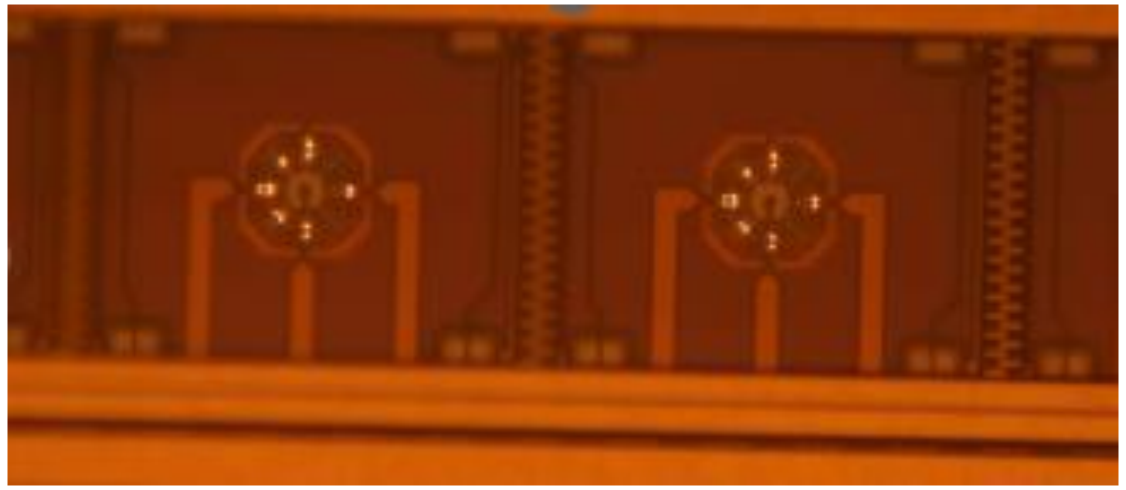
# Monolithic QRNG
## In-silicon source of light

Implementation of a silicon LED:

- Forward emission: peaked at NIRevice description → poor matching with the detector
- Reverse-avalanche emission: broad range with better matching with detector



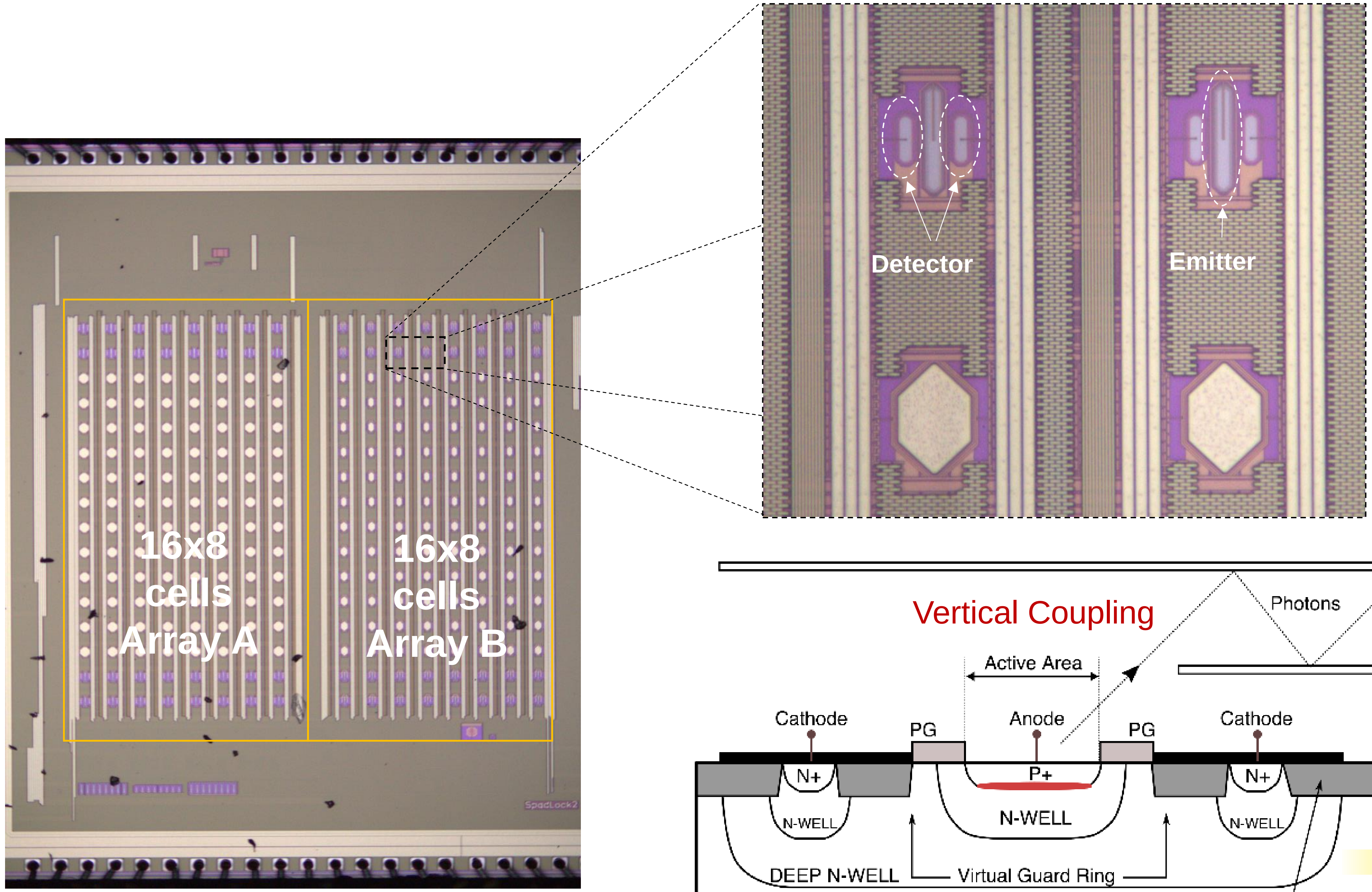



Visible light observed in test structures and capture through a microscope

*[Khan15] [Ace20]*

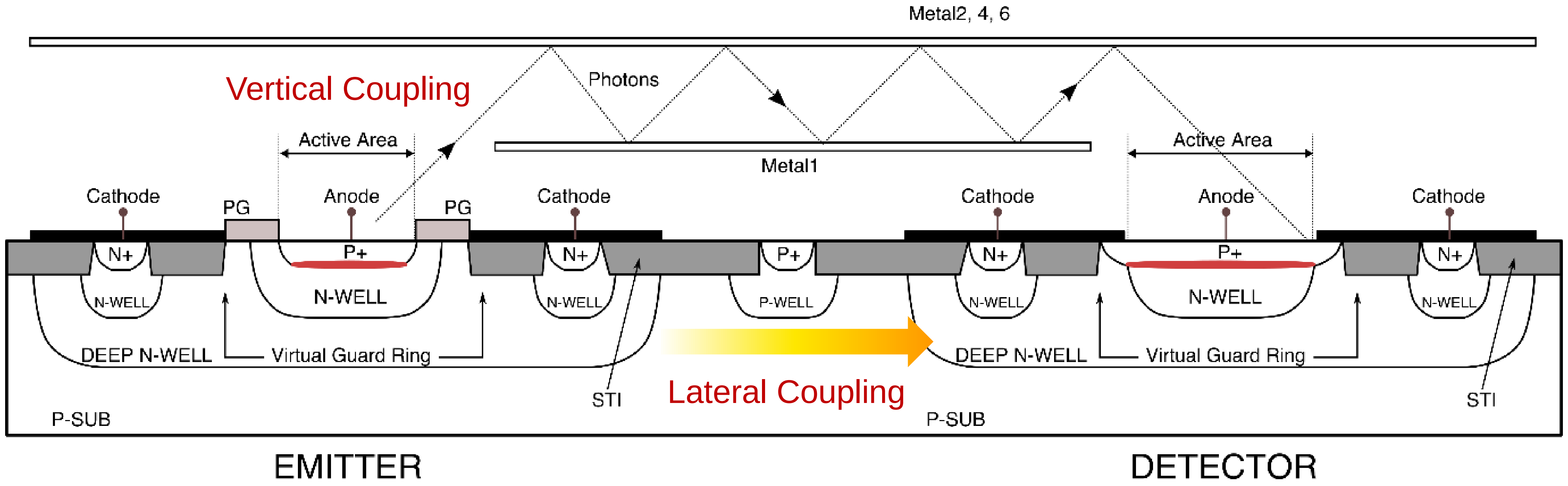
# Monolithic QRNG
## In-silicon source of light



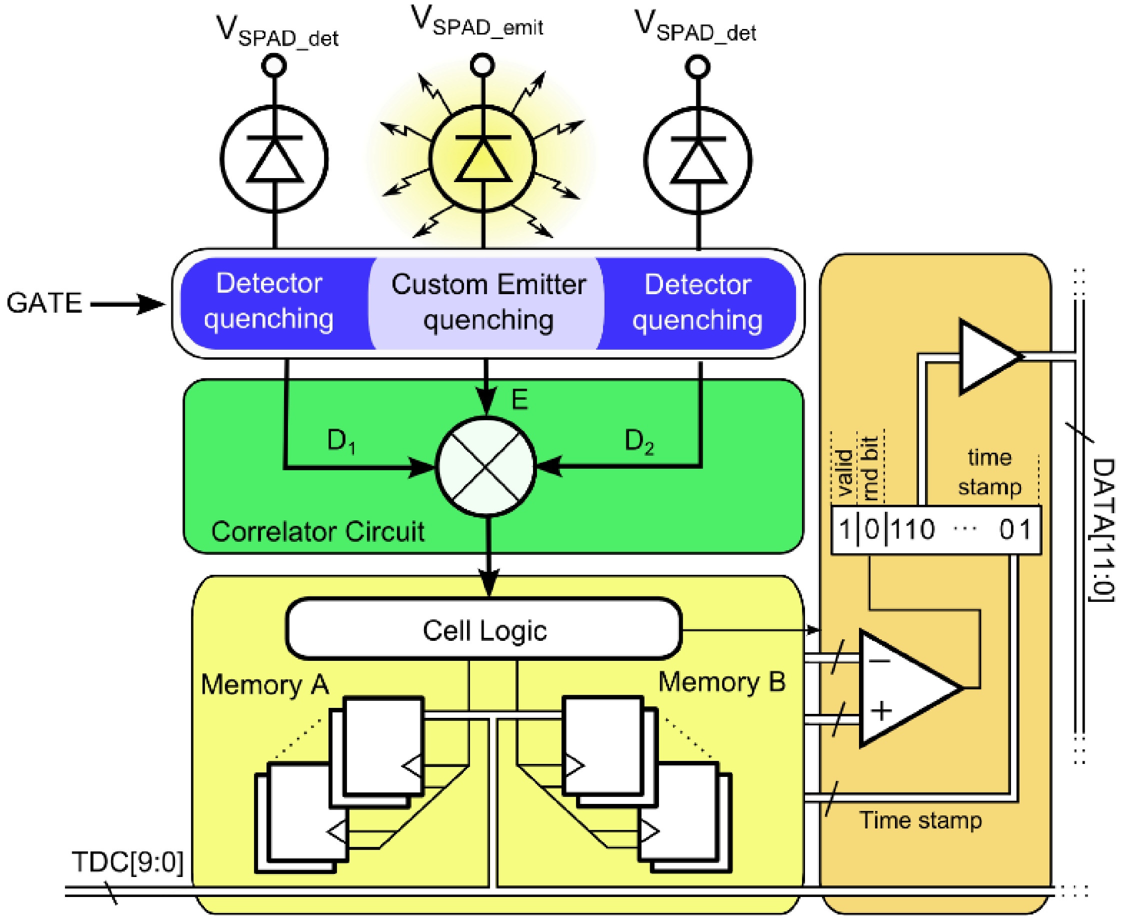

Two arrays of 18x8 cells, each having a couple of SPADs as detector and a central SPAD as an emitter of light

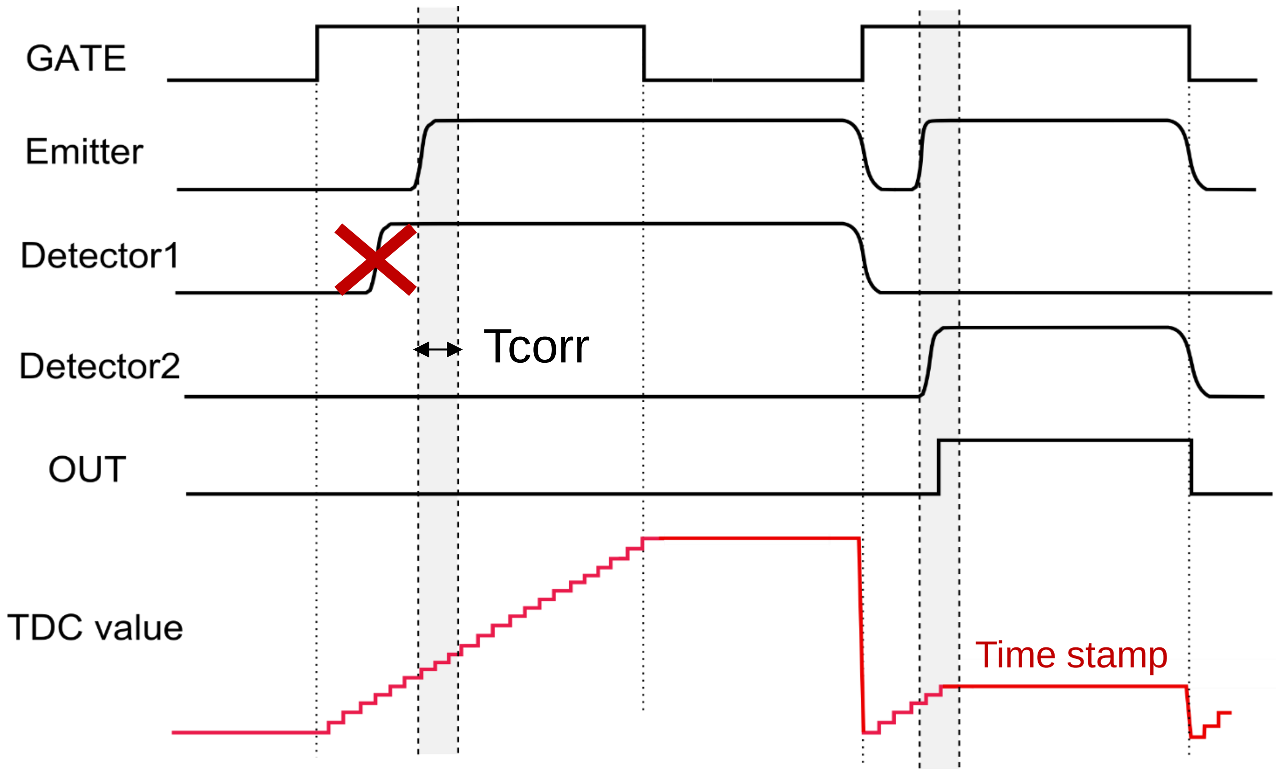
The emission of light is controlled by means of electrical parameters

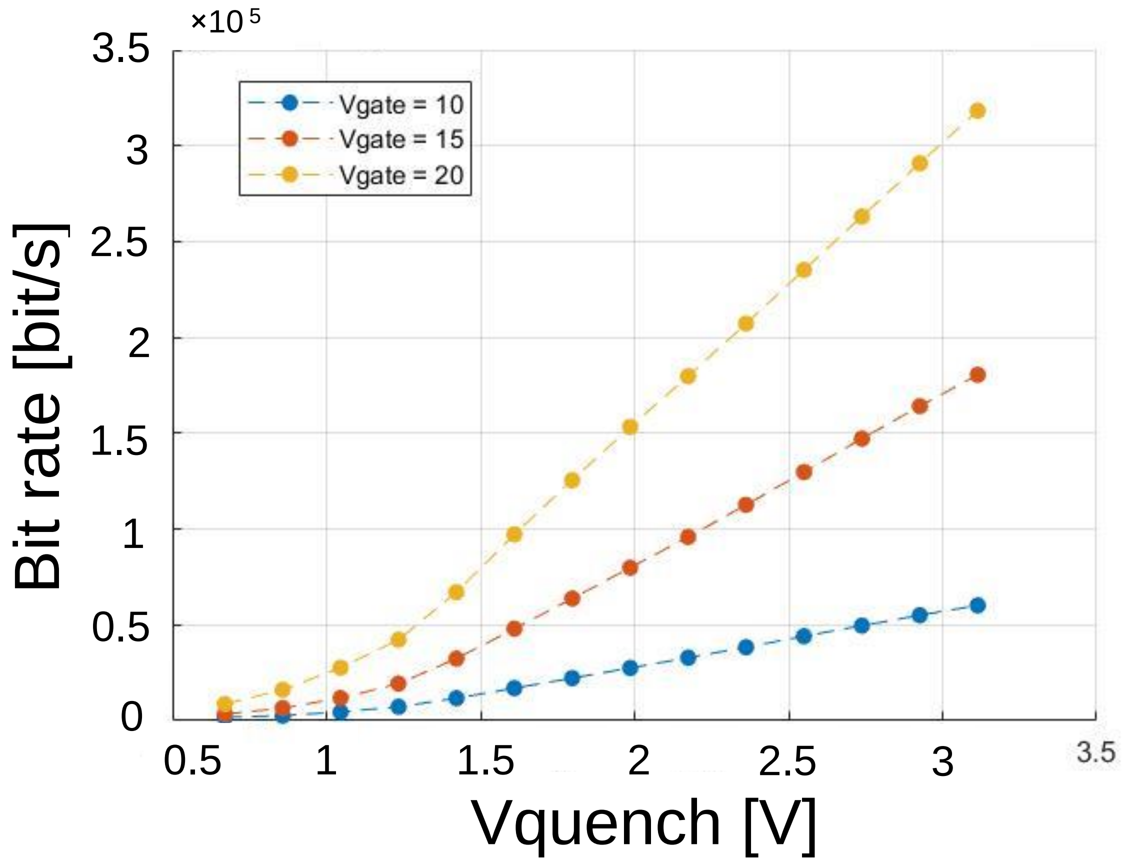
Optical cross-coupling is enhanced by using a top metal shield



# Monolithic QRNG
## In-silicon source of light




Every cell has proper circuit to control the light emission (custom emitter quenching) and a correlator circuit to exclude dark events for the generation of random numbers.

Achieved speed is ~ 400 Kbps

# QRNG review
## Conclusions

- Optical QRNG based on SPAD have shown encouraging results
- Different approaches has been shown with pros and cons
- SPAD-based QRNG can be potentially integrated in a standard state of the art CMOS technology
- SPAD-based QRNG can be implemented in an array to speed-up the generation (up to 5 Gbps have been demonstrated)
- A bit of effort has to be spent in order to increase the actual TRL of this technology

# Thank you

# Bibliography
## QRNG papers


[Stef00]: A. Stefanov et al., “Optical quantum random number generator”, JOURNAL OF MODERN OPTICS, 2000, VOL. 47, NO. 4, 595-598

[Sue07] C. Suematsu et al., “Generation of Physical Random Numbers by means of photon counting”, Electronics and Communication in Japan, Part 3, Vol.90, No. 2, 2007

[Jenn00] T.Jennewein et al., “A fast and compact quantum random number generator”, Review of Scientific Instruments, Volume 71, No. 4, April 2000.

[Ren11]: M.Ren et al, “Quantum random-number generator based on a photon-number-resolving detector”, PHYSICAL REVIEW A 83, 023820 (2011)

[Tisa15]: S.Tisa et al., “High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors”, IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 21, NO. 3, MAY/JUNE 2015.

[Wei18]: W.Wei et al, “A bias free true random number generator”, October 2018  arXiv:0905.0779v2

[Burri13]: S.Burri et al., “Jailbreak Imagers: Transforming a Single-Photon Image Sensor into a True Random Number Generator”,

[Stip07]: M.Stipcevic et al., “Quantum random generator based on photonic emission in semiconductor”, Rev. Sci. Instrum. 78, 045104 (2007)

[Mas16]: N.Massari et al., “A 16×16 pixels SPAD-based 128-Mb/s quantum random number generator with −74dB light rejection ratio and −6.7ppm/°C bias sensitivity on temperature”, ISSCC, San Francisco, CA, USA, 2016

[Xu18]: H.Xu et al., “A 16x16 Pixel Post-Processing Free Quantum Random Number Generator Based on SPADs”, IEEE Transactions on Circuit and Systems, Vol.65(5).

[Tom18]: A.Tomasi et al., “Model, Validation, and Characterization of a Robust Quantum Random Number Generator Based on Photon Arrival Time Comparison”, J. Lightwave Technol. 36, 3843-3854 (2018).

[Way09]: M.Wayne et al., “Photon arrival time quantum random number generation”, Journal of Modern Optics 2009

[Yan15]: Q.Yan et al., “High-speed quantum-random number generation by continuous measurement of arrival time of photons”, Review of Scientific Instruments 86, 073113 (2015).

[Bis18]: Z.Bisadi et al.,  “Compact Quantum Random Number Generator with Silicon Nanocrystals Light Emitting Device Coupled to a Silicon Photomultiplier”, Front. Phys., Sec. Optics and Photonics Volume 6 – 2018

[Bis17], Z.Bisadi et al., “Robust Quantum Random Number Generation With Silicon Nanocrystals Light Source”, JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 35, NO. 9, MAY 1, 2017

# Bibliography
## QRNG papers


[Mas19] N.Massari et al, “A Compact TDC-based Quantum Random Number Generator”, IEEE International Conference on Electronics, Circuits and Systems (ICECS), Genoa, Italy, 2019

[Kes23]: P.Keshavarzian et al., “A 3.3-Gb/s SPAD-Based Quantum Random Number Generator”, IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 58, NO. 9, SEPTEMBER 2023

[Reg21] F.Regazzoni et al., “A High Speed Integrated Quantum Random Number Generator with on-Chip Real-Time Randomness Extraction”, arXiv:2102.06238v1 [quant-ph] 11 Feb 2021

[Cac20] M.Caccia et al., “In-silico generation of random bit streams”, Nuclear Inst. and Methods in Physics Research, A 980 (2020) 164480

[Saj24] M. S. Sajal and M. Dandin, "True Random Number Generation Using Dark Noise Modulation of a Single-Photon Avalanche Diode," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 71, no. 3, pp. 1586-1590, March 2024

[Sta19]: A.Stanco et al., “Efficient random number generation techniques for CMOS SPAD array based devices”, arXiv:1910.05232v1 [quant-ph] 11 Oct 2019.

[San14]: B.Sanguinetti et al., “Quantum random number generation on a mobile phone”, arXiv:1405.0435v1 [quant-ph] 2 May 2014.

[Khan15] A.Khanmohammadi et al., “A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time”, IEEE Photonics Journal, Volume 7, Number 5, October 2015

[Ace20] F.Acerbi et al., “Structures and Methods for Fully-Integrated Quantum Random Number Generators”, in IEEE Journal of Selected Topics in Quantum Electronics, vol. 26, no. 3, pp. 1-8, May-June 2020

[Ton19] A.Tontini et al., “SPAD-Based Quantum Random Number Generator With an Nth-Order Rank Algorithm on FPGA”, in IEEE Trans on Circuit and Systems II, Express Briefs, 66, n. 12 (2019)

[Way10] M.Wayne et al.. “L’ow-bias high-speed quantum random number generator via shaped optical pulses”, Vol. 18, No. 9 / OPTICS EXPRESS 9351, 2010.

[San14] B.Sanguinetti et al., Quantum Random Number Generation on a Mobile Phone” PHYSICAL REVIEW X 4, 031056 (2014)