QRNG Class

Random Number Generation with State-of-the-Art Photonic Technologies

Dr. José Ramón Martínez Saavedra

VP Innovation, Quside

July 8th 2025 - Bari

Introduction

Objectives

- Explore random number generation methods.
- Understand the limitations of traditional methods.
- Introduce state-of-the-art photonic technologies in QRNGs.

Agenda

- RNG typologies
- Quantum phase diffusion models.
- Metrological techniques and randomness extraction.
- System integration and practical applications.

Why do we need randomness?

- Cryptography: for the creation of the security parameters (keys)
- Secure comms: QKD schemes, TLS schemes
- Proof-of-Stake, Zero-Knowledge Proofs
- HPC: for the simulation of complex systems (Monte Carlo)
- Biological and genetic simulations
- Gaming: procedural generation, gambling
- Generative art: images, video, audio

Entropy: the Physics' secret sauce of RNs

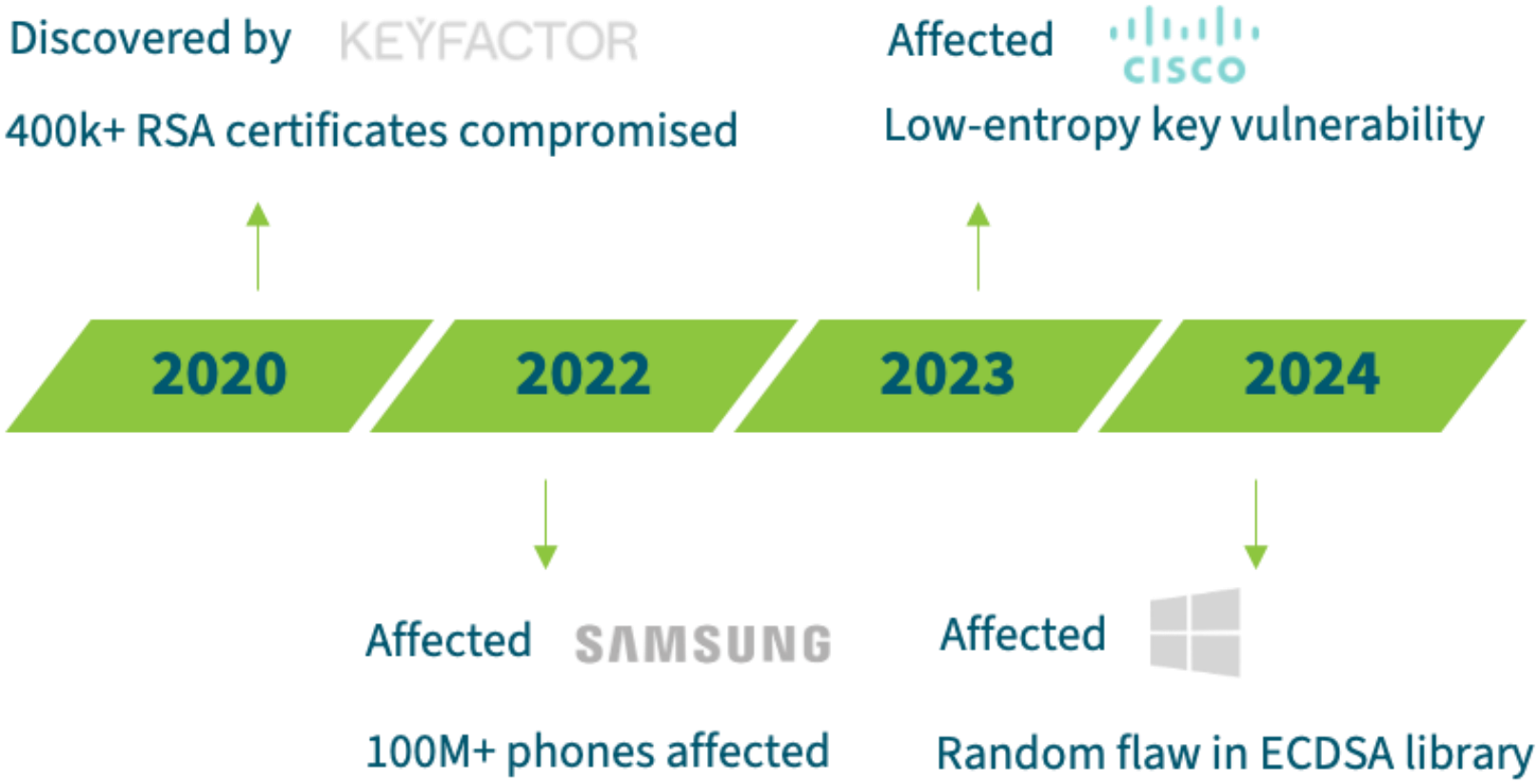
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A

Low surprise → Low information gain → Low entropy

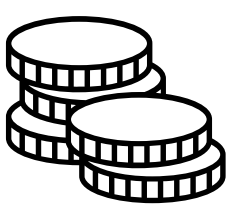
QX9L8RTZB3A2MJHKD7PS4NFW5V1G6 A

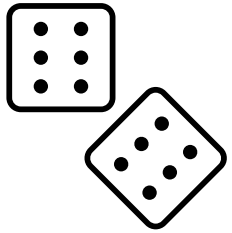
High surprise → High information gain → High entropy

When entropy fails: the cost of weak RNs



How do we generate a random number?



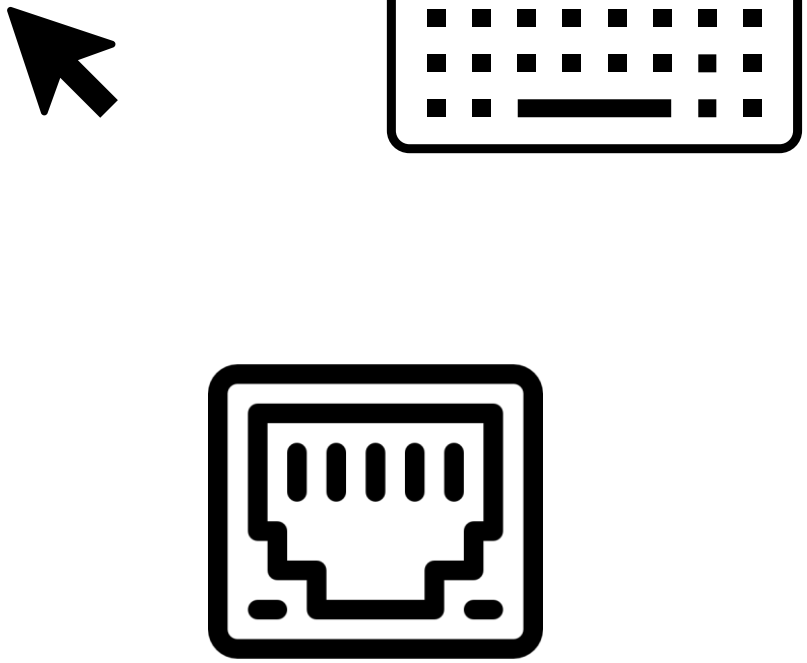


`np.random.rand()`

Level 1: Illusion of randomness

- Processes that fake randomness
- No entropy is used
- Some of these are very fast processes (software PRNGs)
- Useful when quality is not a limiting factor

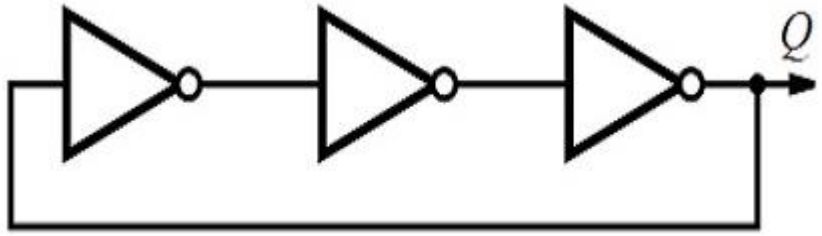
How do we generate a random number?



Level 2: Opportunistic randomness

- Use unpredictable behavior as an entropy source
- Rely on external, uncontrolled factors

How do we generate a random number?



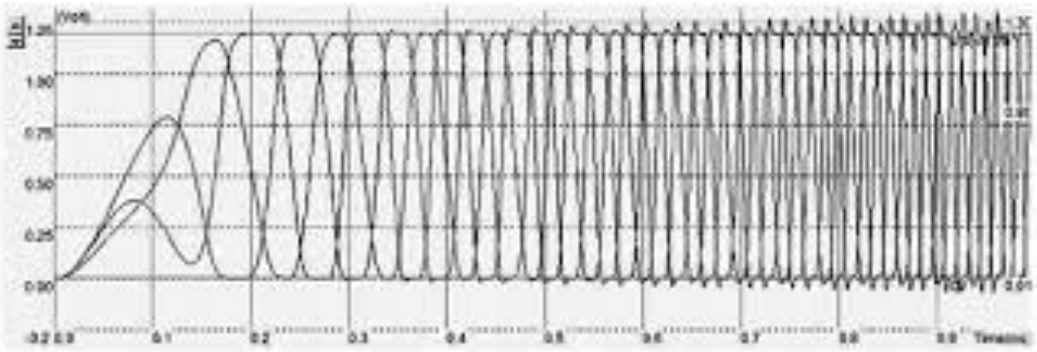


Fig.2: A typical output waveform of a 3-inverter ring oscillator.

Level 3: Engineered chaos

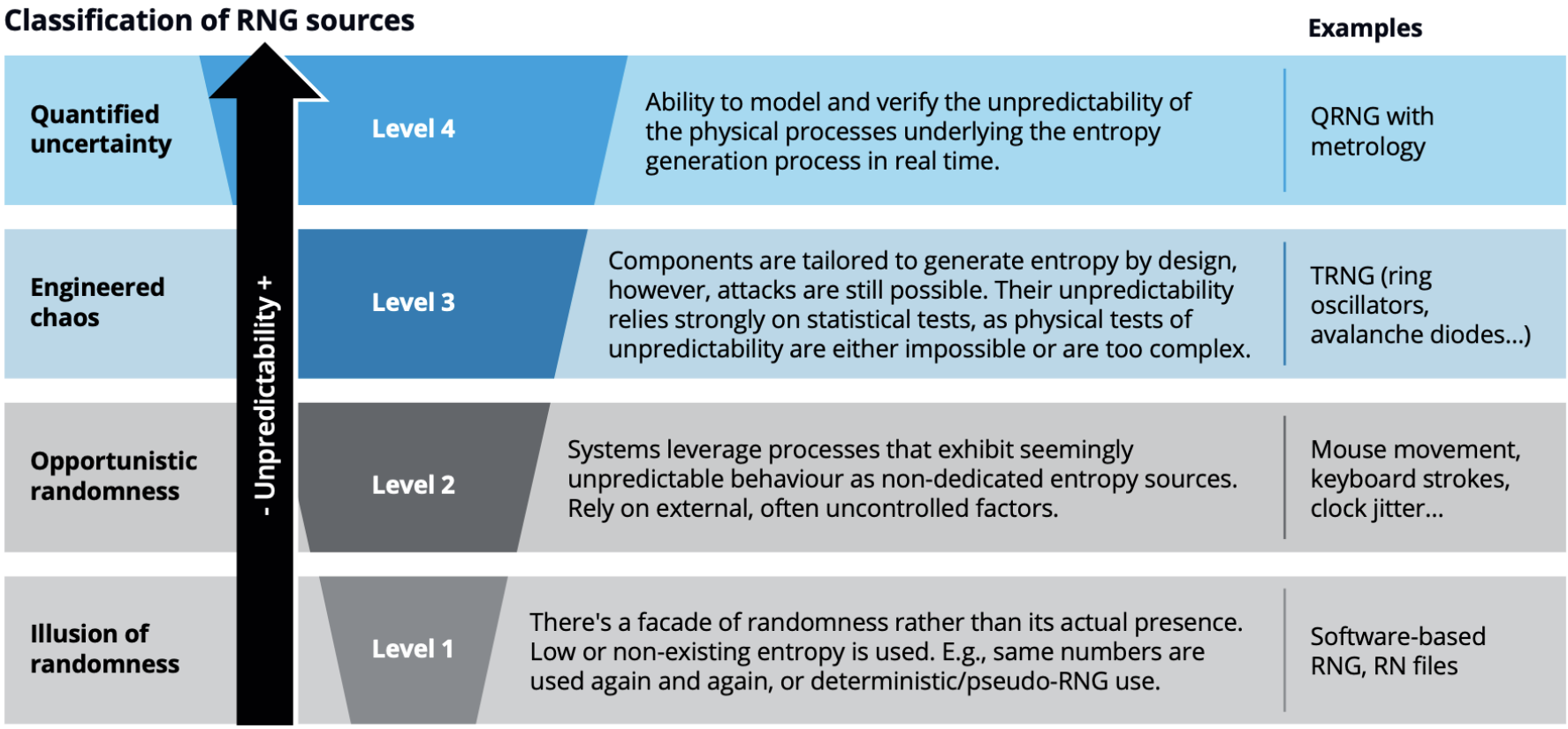
- Unpredictable process specifically engineered for random number generation
- Lack physical tests of unpredictability

How do we generate a random number?

Level 4: Quantified Uncertainty

- Unpredictable process specifically engineered for random number generation
- Provably, quantifiable randomness

How do we generate a random number?



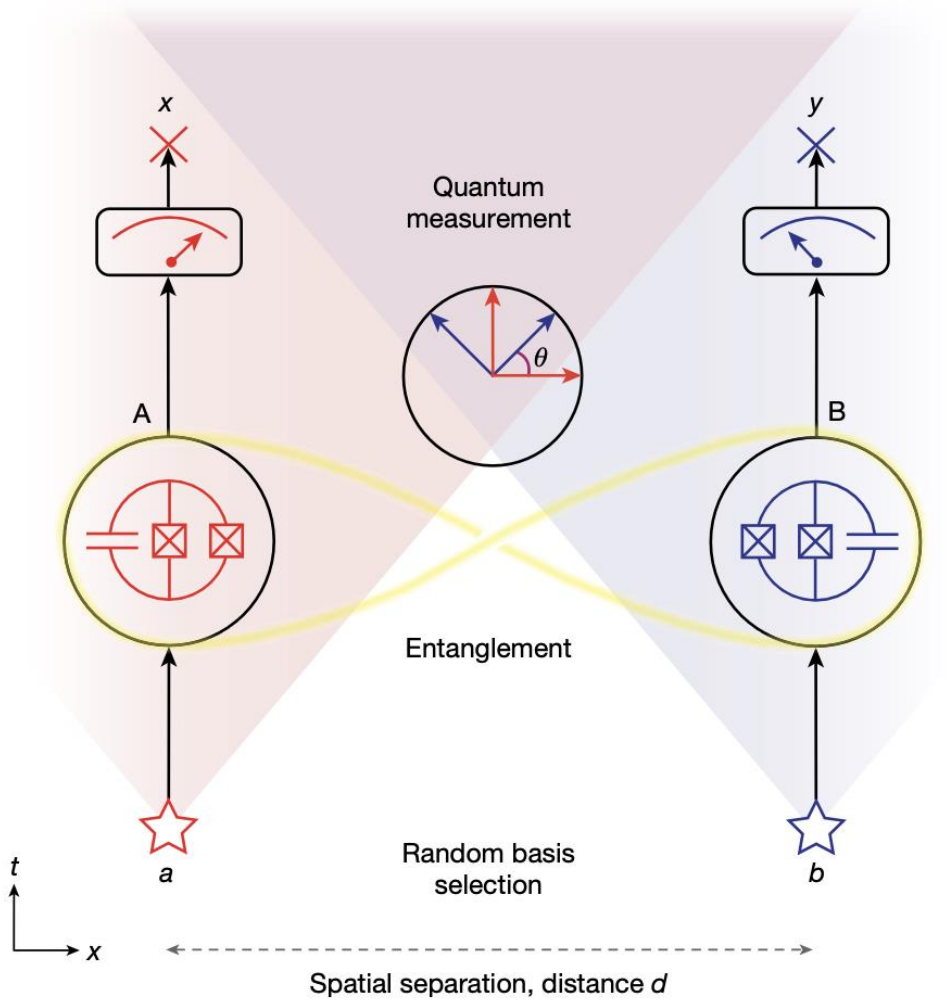
bit.ly/qrng-paper

Quside

Why quantum is random?

- Realism vs. localism
- Bell inequalities: theories that provide both realism (=the world is not probabilistic) and localism (there are no non-local interactions) must satisfy Bell's inequalities.
- Some experiments (Bell tests) can be used to verify whether these Bell inequalities are fulfilled (= both realistic and local world) or violated.

(Loophole-free) Bell tests



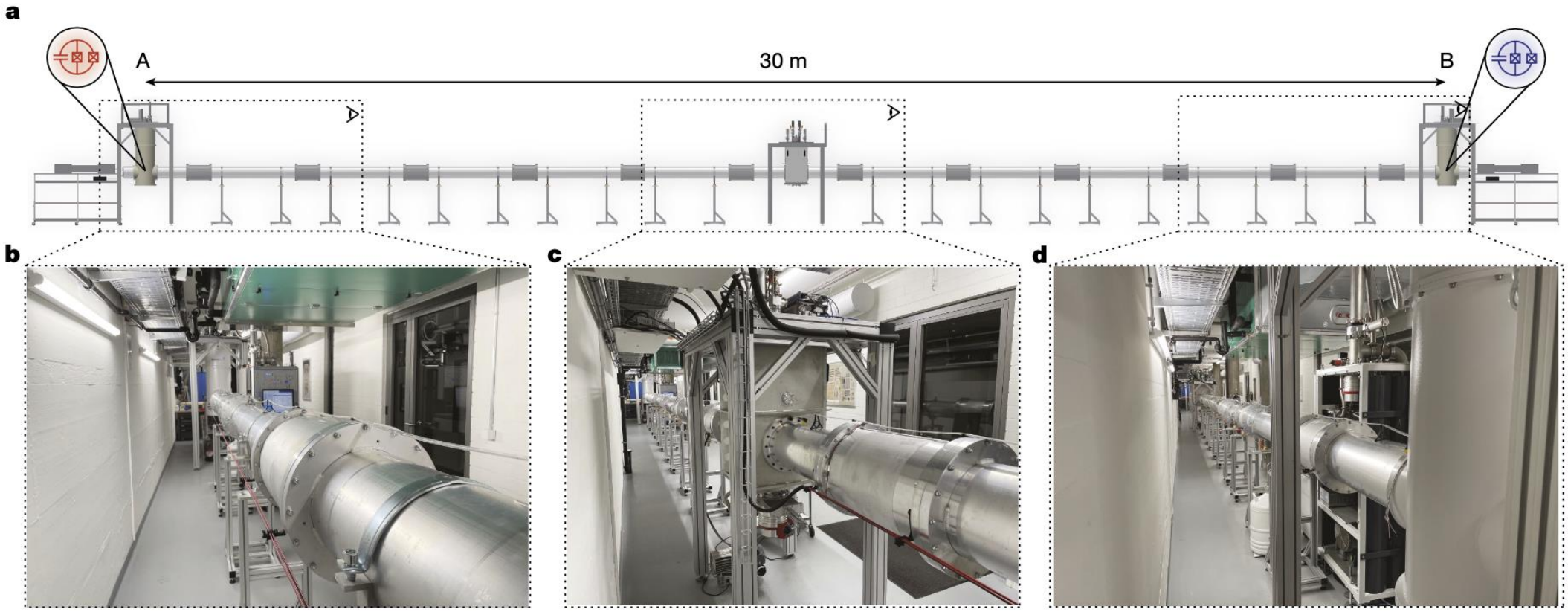
$$S(\theta) = \langle xy \rangle_{(0,0)} - \langle xy \rangle_{(0,1)} + \langle xy \rangle_{(1,0)} + \langle xy \rangle_{(1,1)}$$

CHSH inequality:

$$|S(\theta)| \leq 2$$

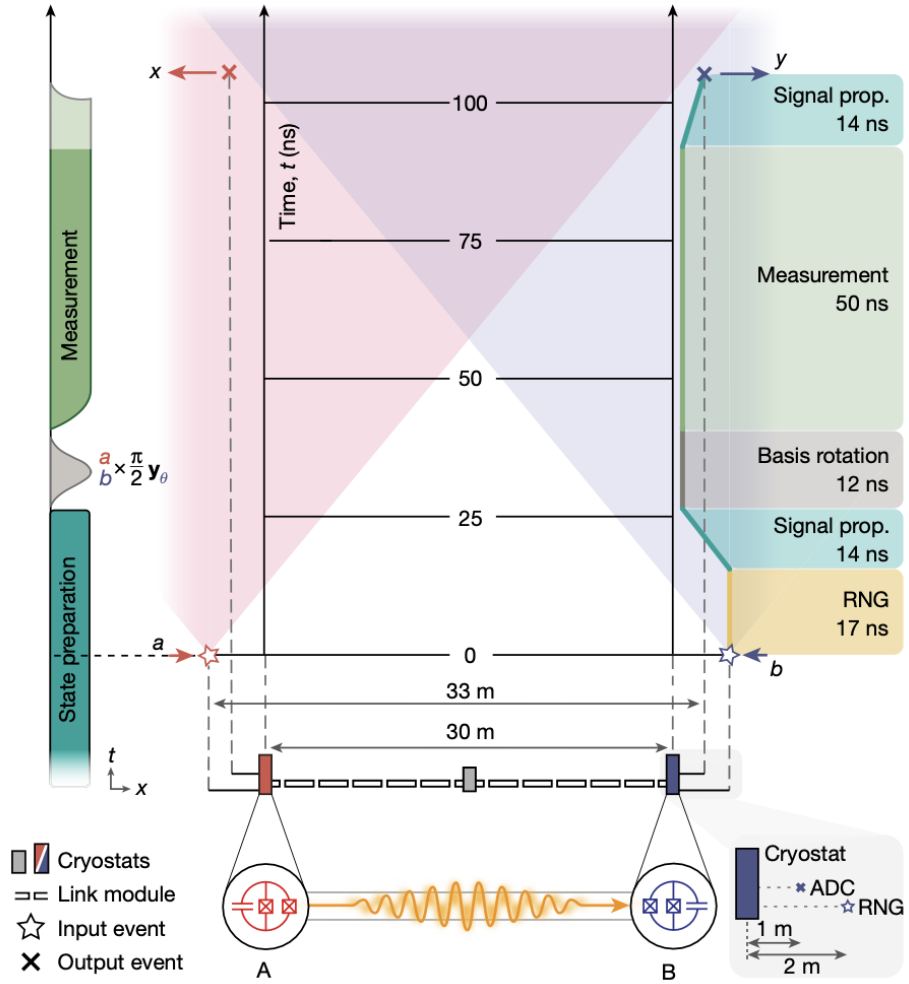
Nature **617**, 265–270 (2023)

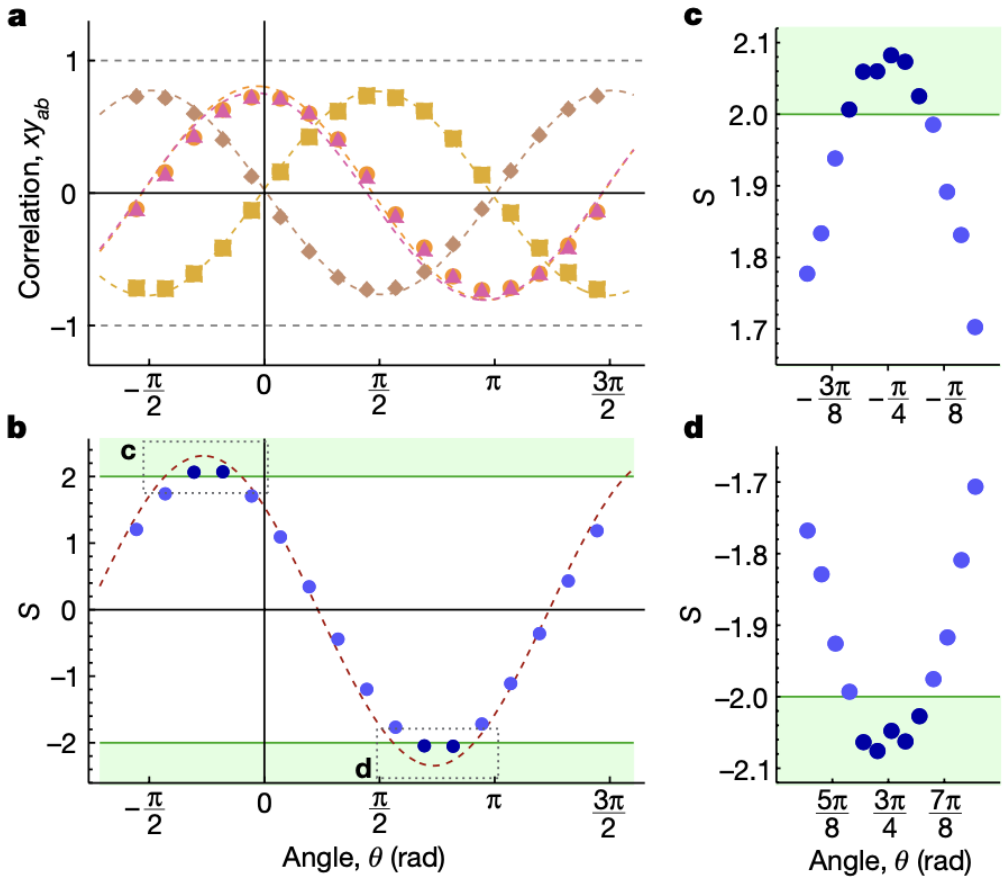
(Loophole-free) Bell tests



Nature **617**, 265–270 (2023)

(Loophole-free) Bell tests





Nature **617**, 265–270 (2023)

Quside

Why quantum is random?

- Realism vs. localism
- Bell inequalities: theories that provide both realism (=the world is not probabilistic) and localism (there are no non-local interactions) must satisfy Bell's inequalities
- Experimental results violate those inequalities, which means that the physical world is either:
  - Non-realistic: the world is probabilistic in nature.
  - Non-local: Einstein's relativity principle is not valid.

Other quantum sources of randomness

Quantum Process	Description	Advantages	Disadvantages	Companies
Radioactive Decay	Spontaneous emission of nuclear particles (e.g., electrons, photons, neutrinos).	- Highly unpredictable source. - Independent of external conditions.	- Requires handling radioactive material. - Slow generation speed. - Difficult to miniaturize.	

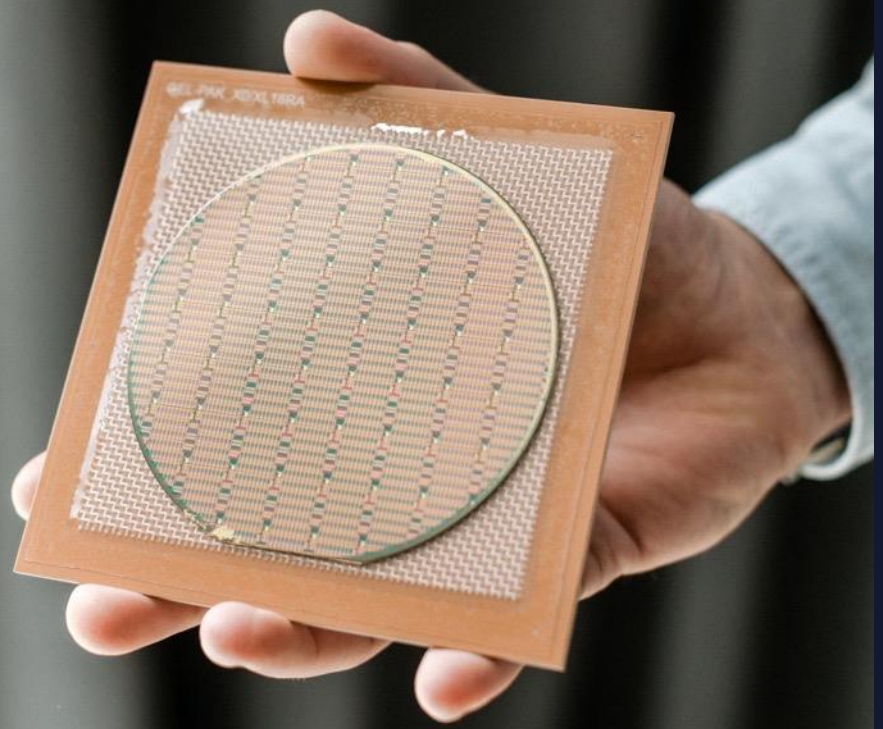
Other quantum sources of randomness

Quantum Process	Description	Advantages	Disadvantages	Companies
Radioactive Decay	Spontaneous emission of nuclear particles (e.g., electrons, photons, neutrinos).	- Highly unpredictable source. - Independent of external conditions.	- Requires handling radioactive material. - Slow generation speed. - Difficult to miniaturize.	
Photon Counting	Detection of individual photons in quantum states using highly sensitive detectors (e.g., APDs, SPADs).	- High bit generation speed. - Based on easily miniaturizable technology.	- Sensitive to environmental noise and temperature variations. - Requires specialized detectors.	ID Quantique SK Telecom QuantumCTek

Other quantum sources of randomness

Quantum Process	Description	Advantages	Disadvantages	Companies
Radioactive Decay	Spontaneous emission of nuclear particles (e.g., electrons, photons, neutrinos).	- Highly unpredictable source. - Independent of external conditions.	- Requires handling radioactive material. - Slow generation speed. - Difficult to miniaturize.	
Photon Counting	Detection of individual photons in quantum states using highly sensitive detectors (e.g., APDs, SPADs).	- High bit generation speed. - Based on easily miniaturizable technology.	- Sensitive to environmental noise and temperature variations. - Requires specialized detectors.	ID Quantique SK Telecom QuantumCTek
Phase Diffusion	Unpredictable fluctuations in the phase of laser light due to quantum uncertainty.	- Very high bit generation speed. - Easy integration with photonic systems. - Good balance between speed and security.	- Sensitive to optical conditions (alignment, optical loss). - Requires stabilization.	Toshiba QuintessenceLabs **Quside**

About Quside



10+ years delivering advanced randomness solutions.

QRNG
IP & Modules

Die / Chips / Embedded module / PCIE

Entropy Core
Infrastructure solution

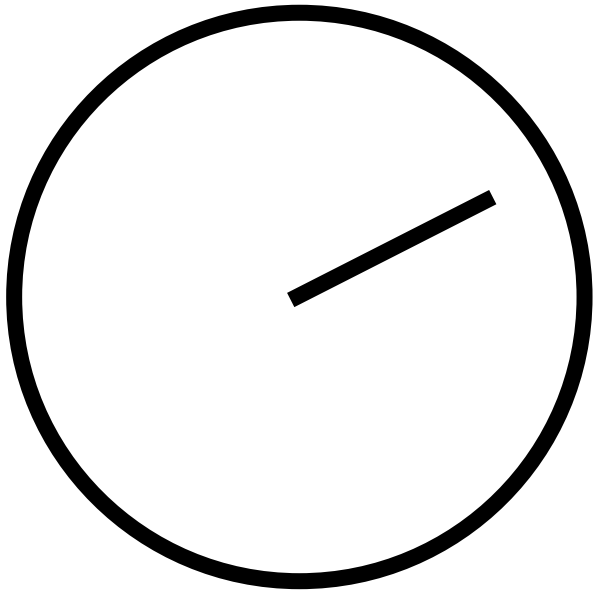
EQUINIX

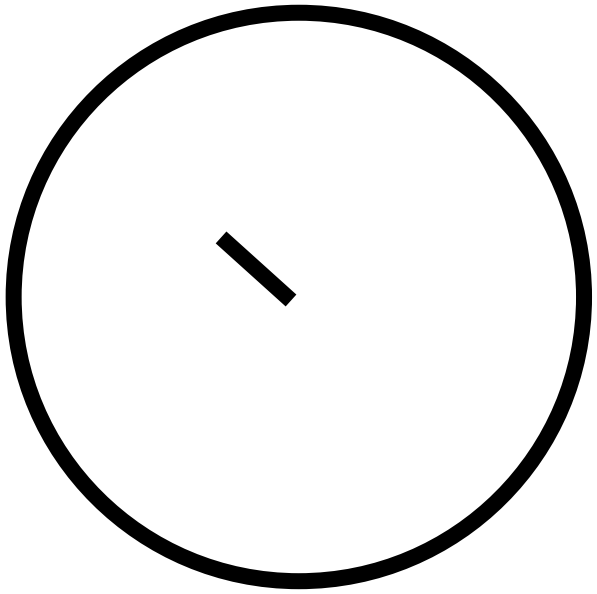
RPU
Stochastic acceleration

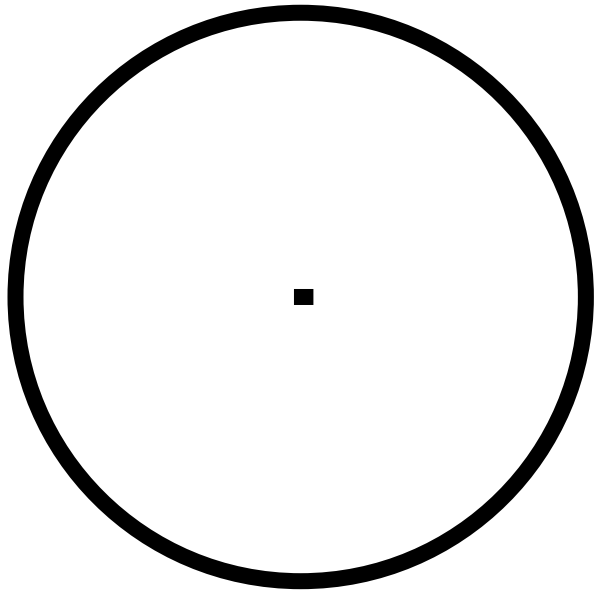
aws marketplace

EQUINIX · Telefónica · ThalesAlenia Space · paloalto NETWORKS · KEYFACTOR · quantropi Bring it on. · Qrypt · European Commission

Phase Diffusion Gedanken: What time is it?

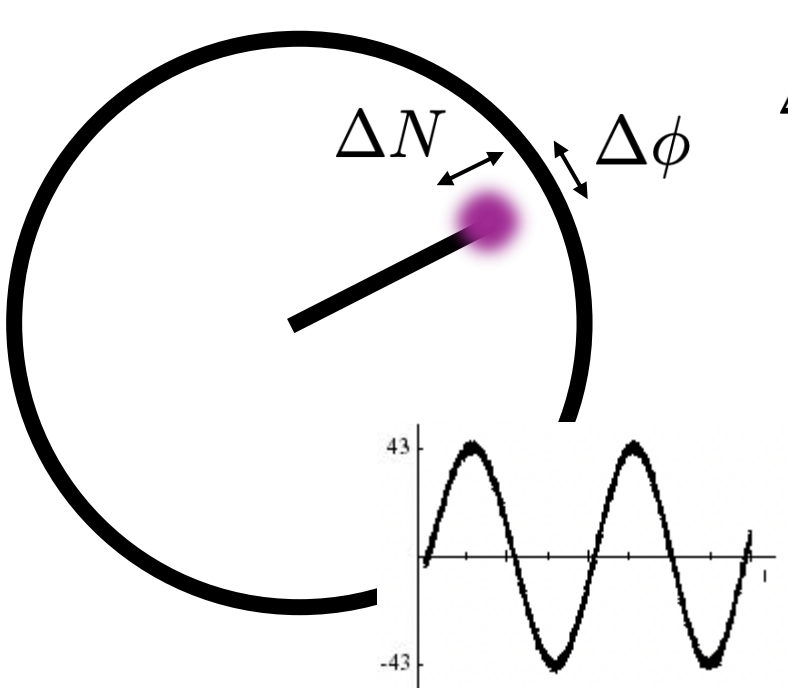


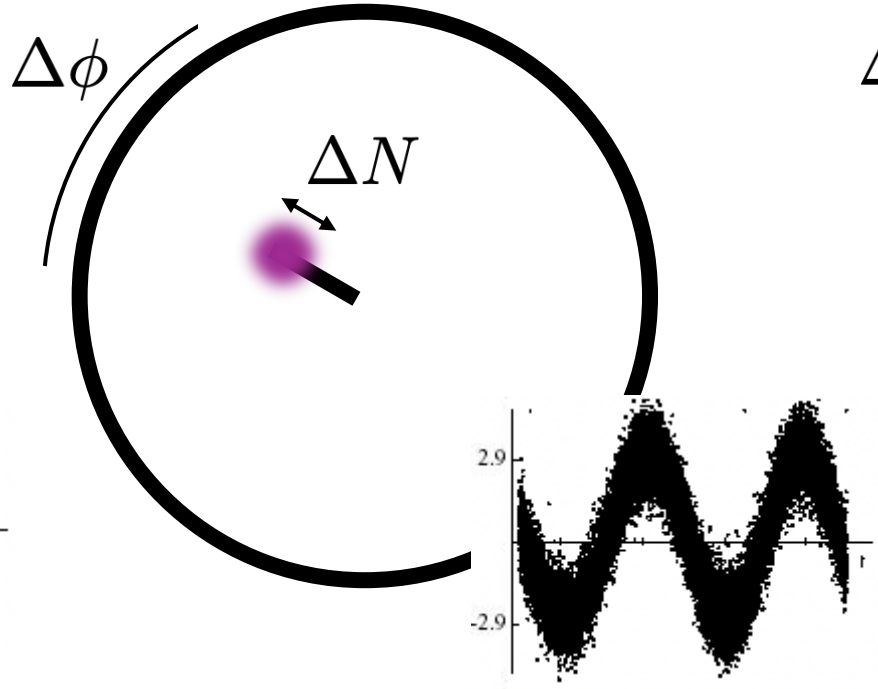


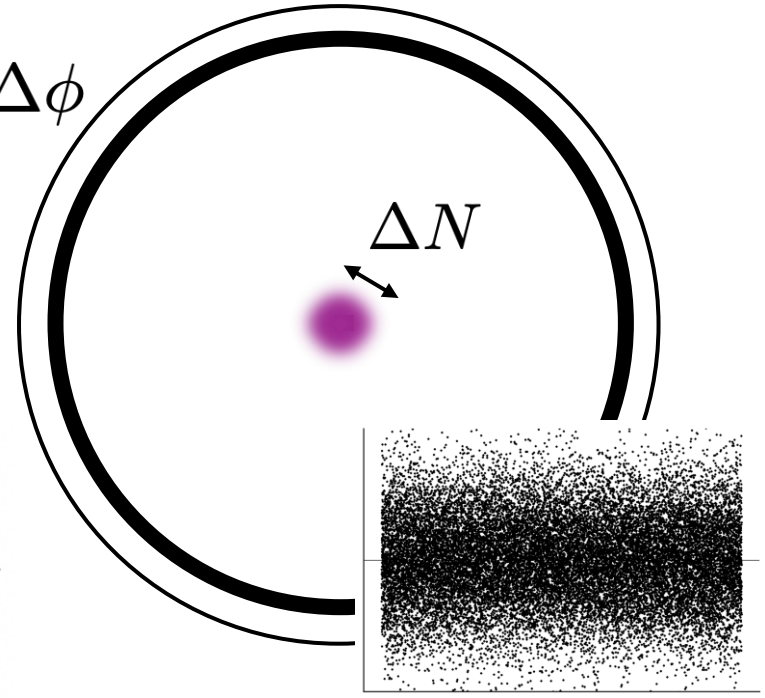


$$E = A\ \mathrm{e}^{\mathrm{i}\phi}$$

Phase Diffusion Gedanken: What time is it?

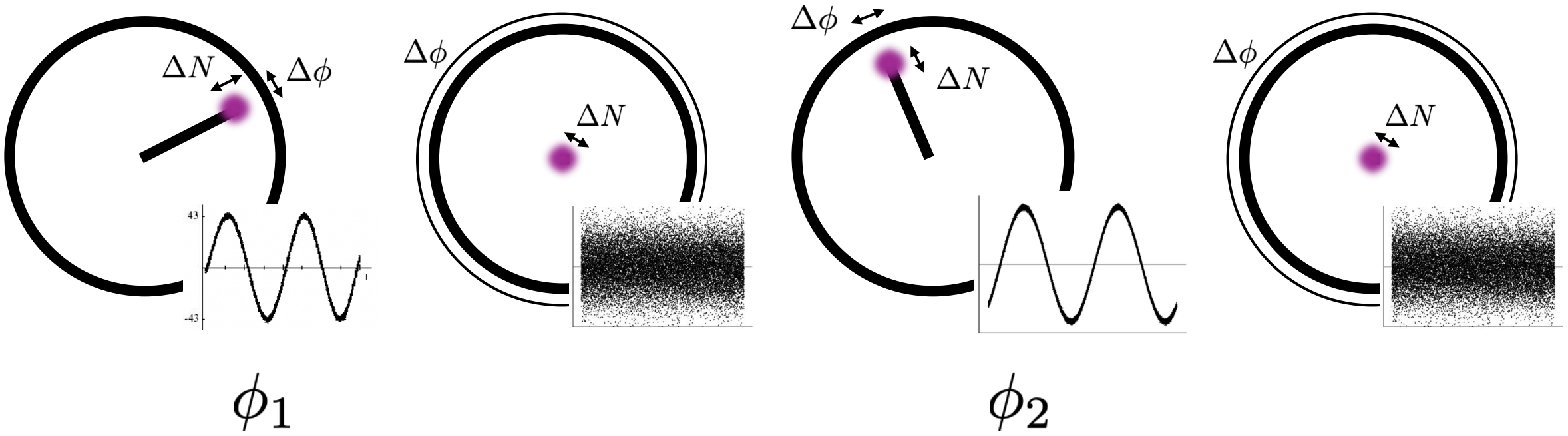






$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

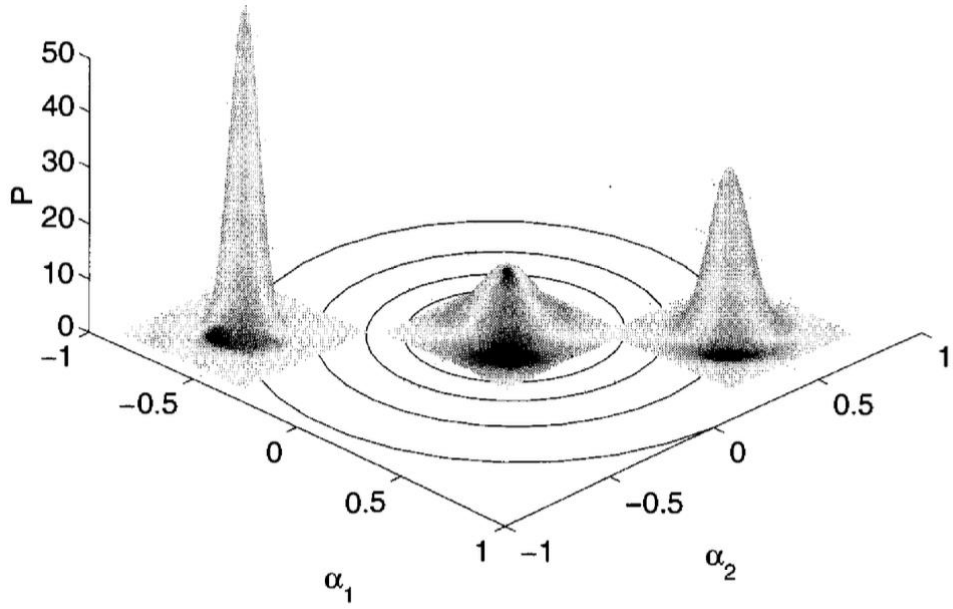
Switching on-off: phase-diffusion QRNG



- Each phase is random, iid with respect to the others
- Just recover the phase, and you have random numbers
- This can go as fast as the laser dynamics allows to (~50 GHz)

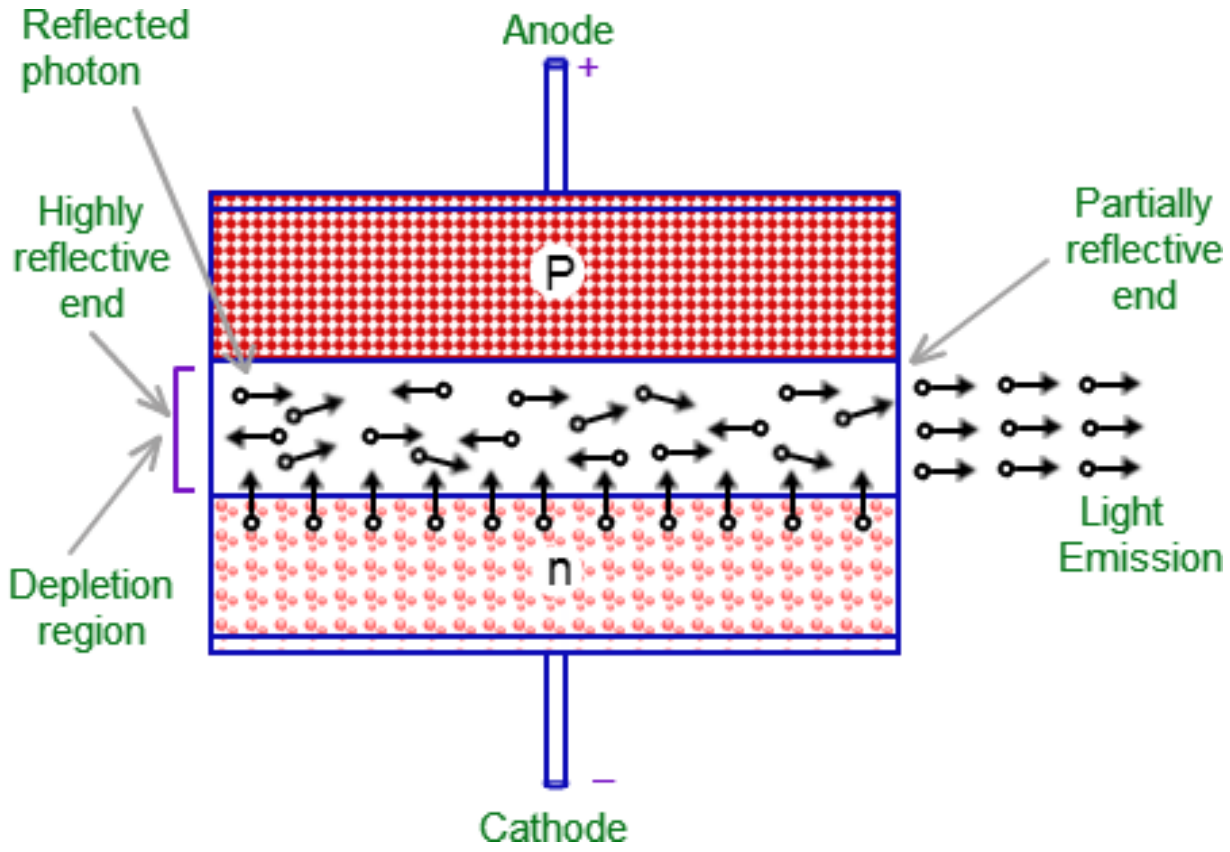
Deeper modelling: open quantum systems

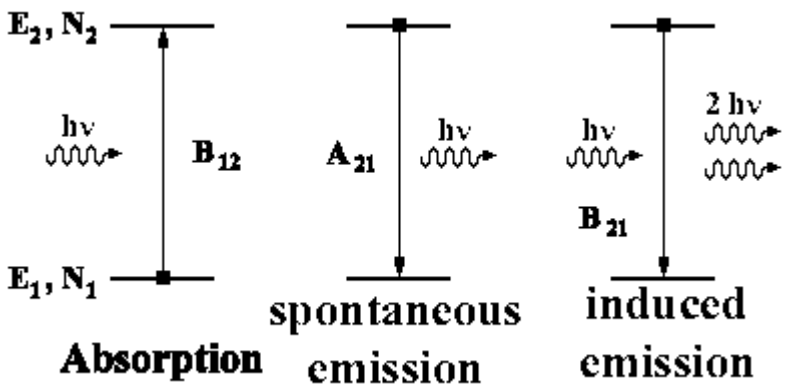
- We don't model coherent states, but their probability distribution
- $P(\alpha, \alpha^*, t)$: probability that the quantum state is given by the coherent state α at time t.
- Evolution given by a Fokker-Planck equation



$$\frac{\partial}{\partial t}P(\alpha,\alpha^*,t) = -\left[\left(-i\omega_0 - \frac{\gamma_0}{2} + \gamma_I\right)\frac{\partial}{\partial\alpha}\alpha + \left(+i\omega_0 - \frac{\gamma_0}{2} + \gamma_I\right)\frac{\partial}{\partial\alpha^*}\alpha^*\right]P(\alpha,\alpha^*,t)$$
$$+\gamma_0 N\frac{\partial^2}{\partial\alpha\partial\alpha^*}P(\alpha,\alpha^*,t).$$

A laser from a semiclassical perspective





A laser from a semiclassical perspective

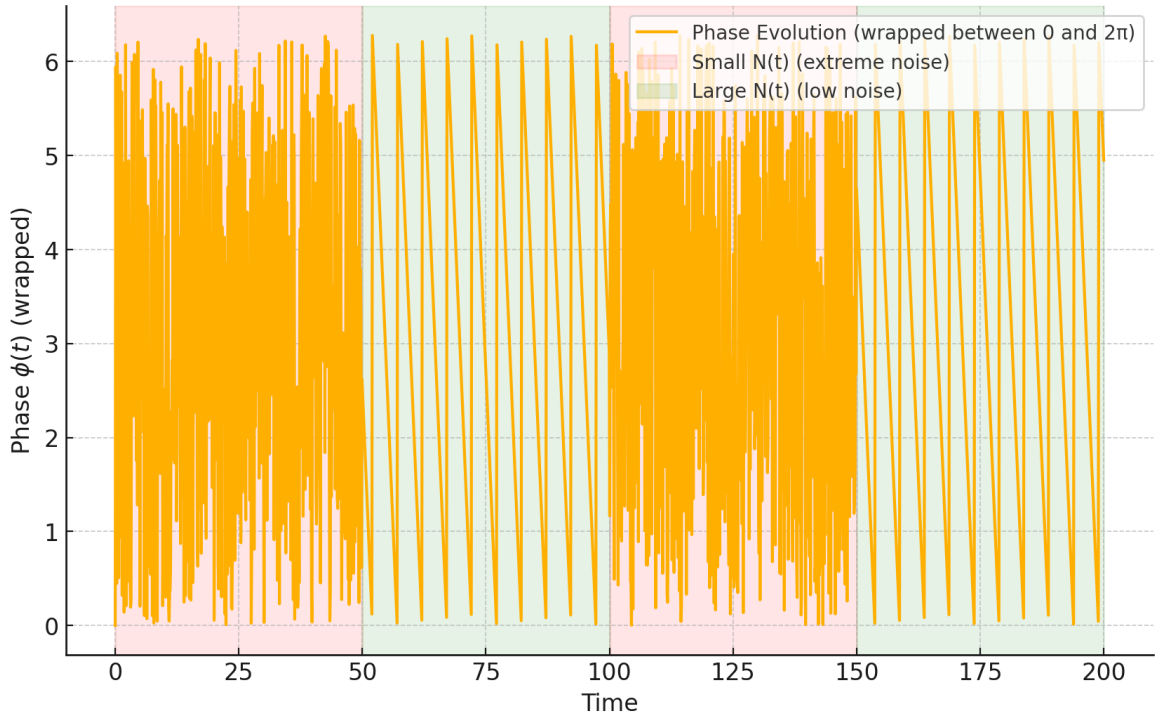
Laser rate equations (accounting for spontaneous emission):

$$\frac{dE(t)}{dt} = \frac{1}{2}G(E(t),N(t))E(t) - \frac{1}{2\tau_p}E(t) + \beta_{sp}\sqrt{N(t)}$$

$$\frac{d\phi(t)}{dt} = \omega_0 - \frac{\alpha}{2}G(E(t),N(t)) + \sqrt{\frac{\beta_{sp}}{2\tau_n N(t)}}\eta(t)$$

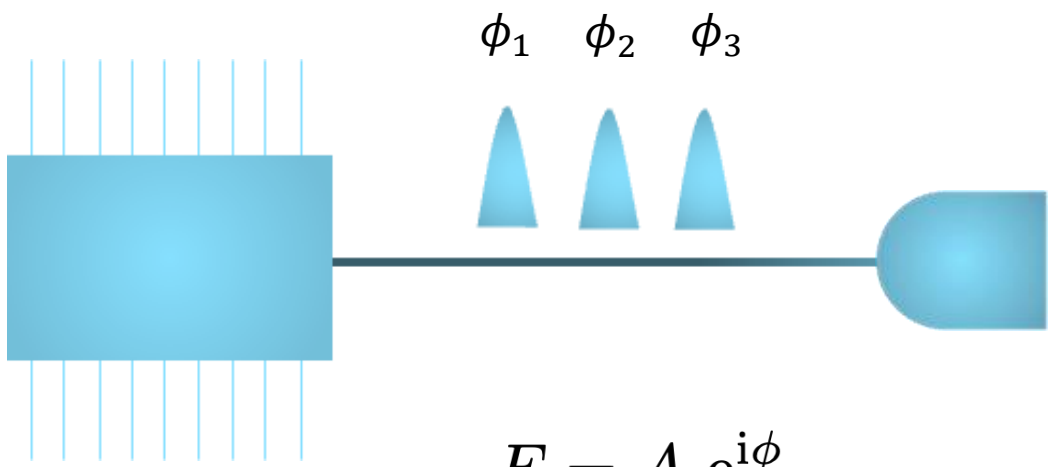
$$\frac{dN(t)}{dt} = \frac{I}{eV} - \frac{N(t)}{\tau_n} - G(E(t),N(t))E(t)^2$$

$$G(E(t),N(t)) = g0(N(t) - N_{th})$$



Quside

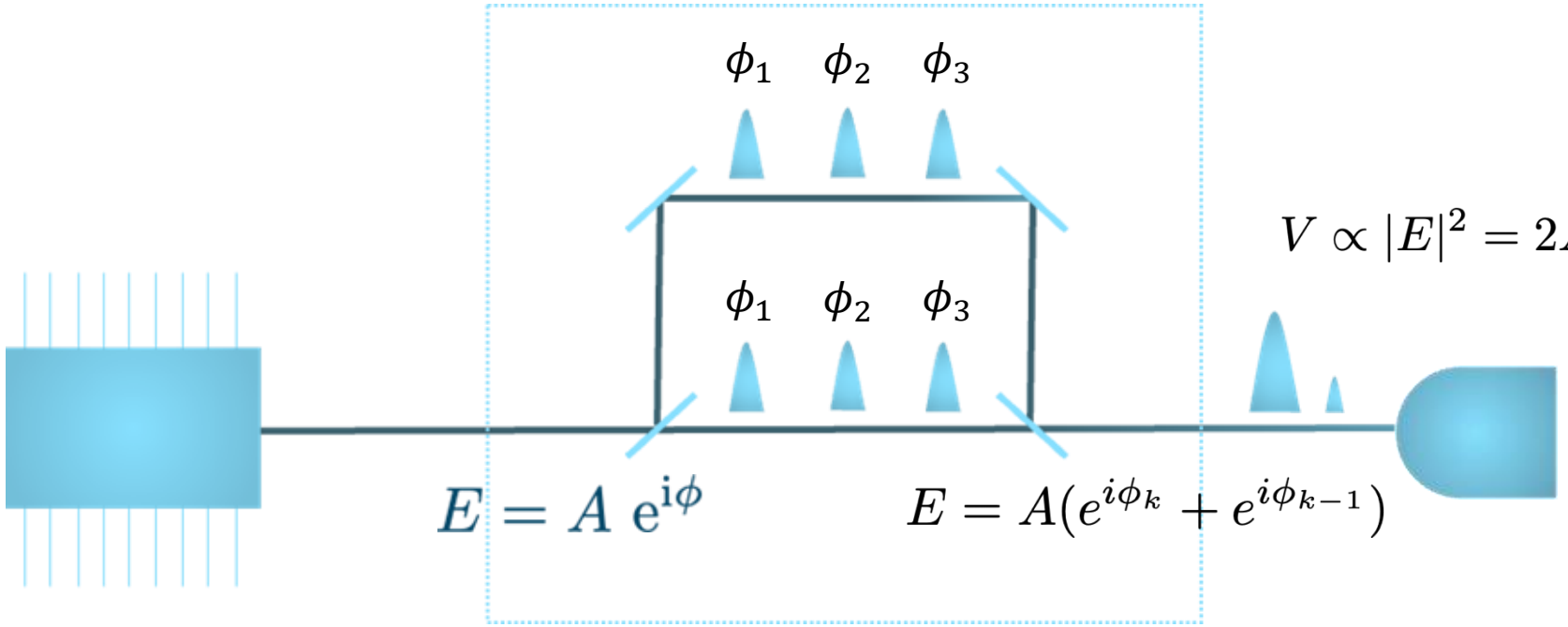
Recovering the phase: a workaround



$$V \propto |E|^2 = A^2$$

$$E = A\ \mathrm{e}^{\mathrm{i}\phi}$$

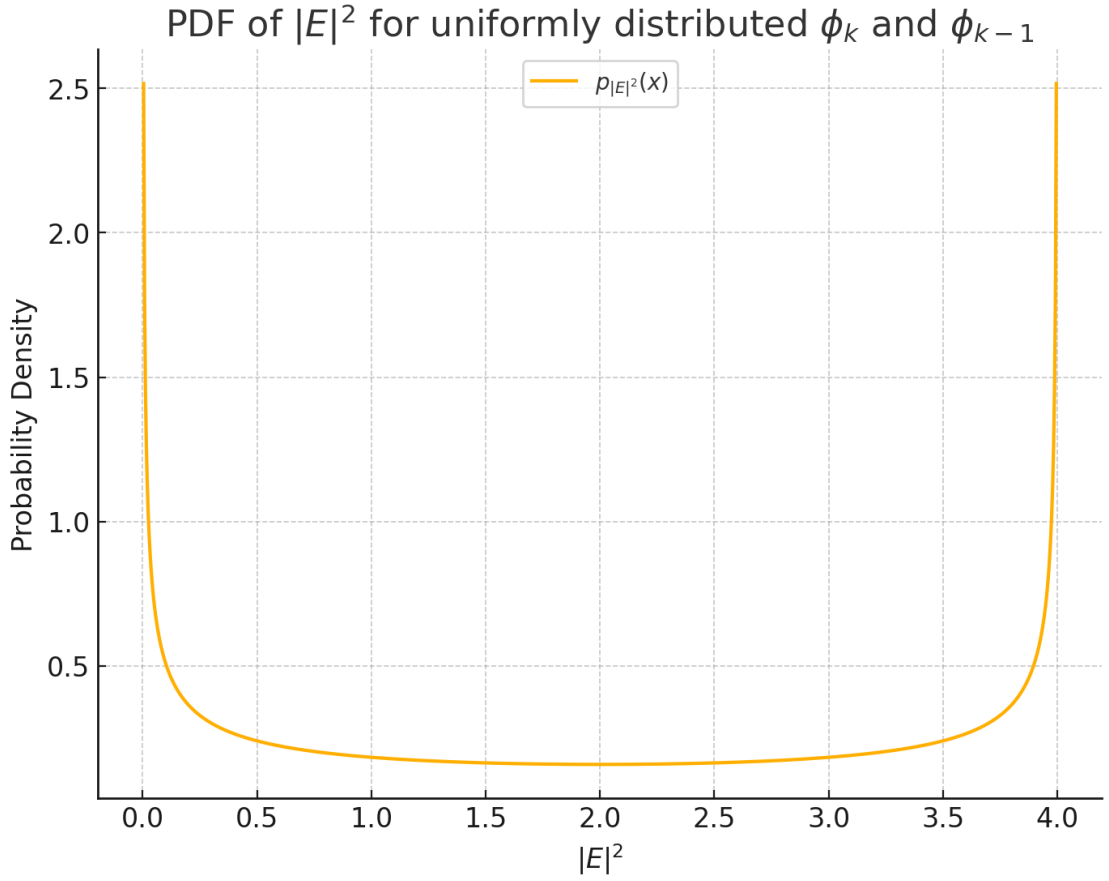
Recovering the phase: a workaround

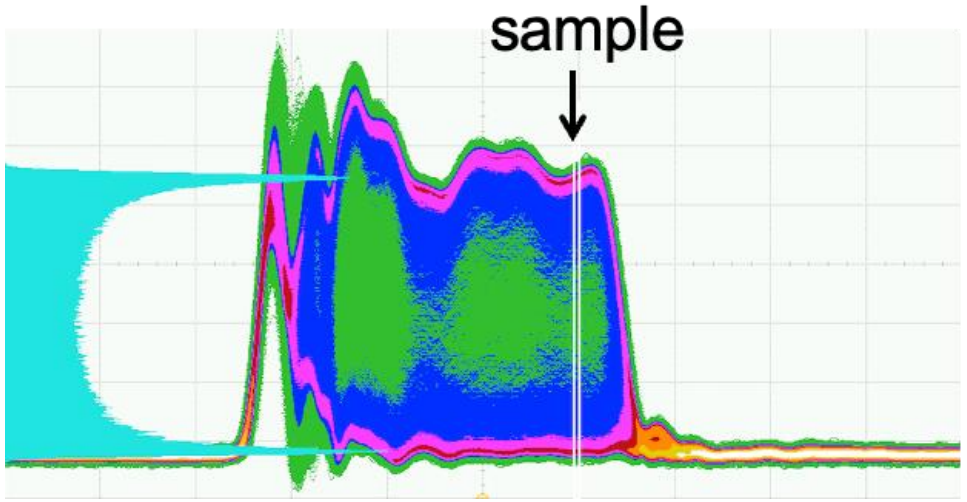


$$V \propto |E|^2 = 2A^2[1 + \cos(\phi_k - \phi_{k-1})]$$

Recovering the phase: a workaround

$$V \propto |E|^2 = 2A^2[1 + \cos(\phi_k - \phi_{k-1})]$$

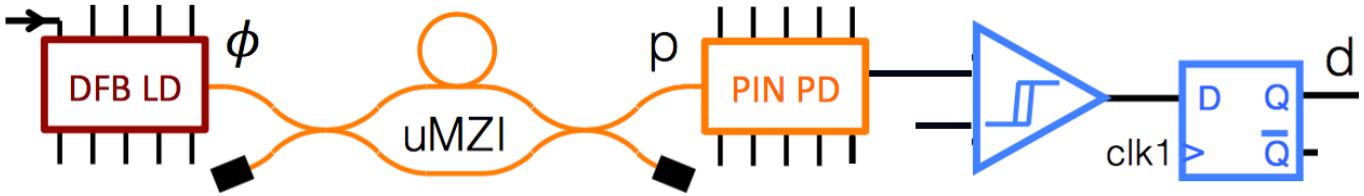


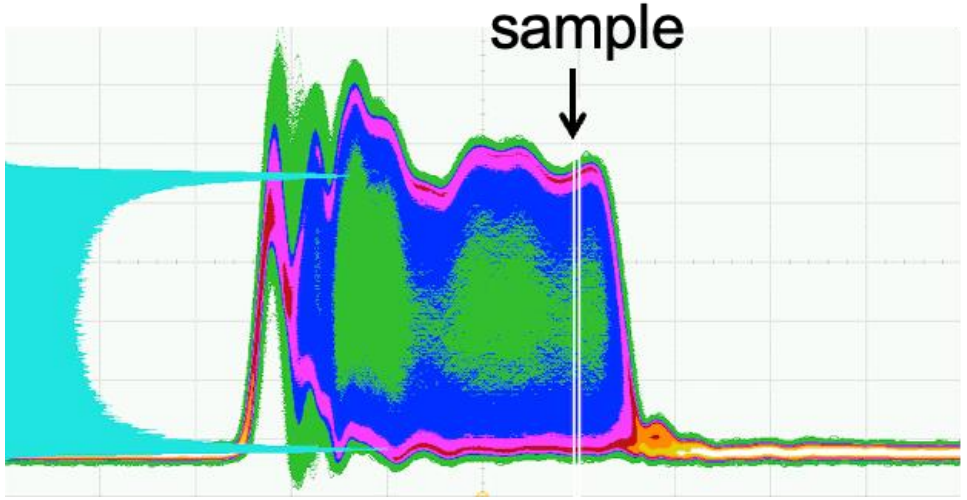


Quside

Recovering the phase: a workaround

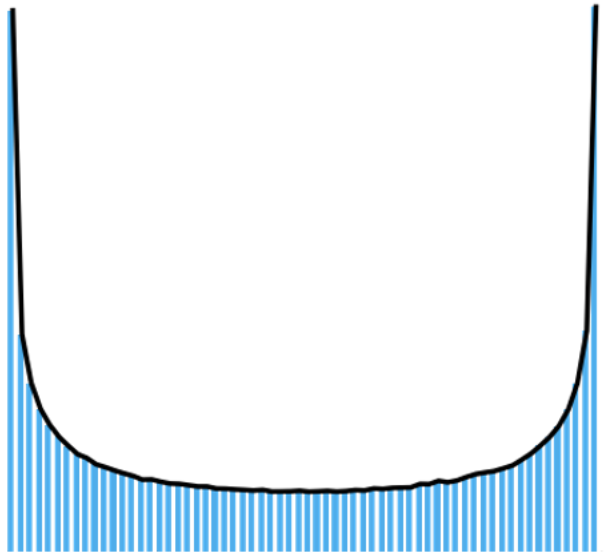
$$V \propto |E|^2 = 2A^2[1 + \cos(\phi_k - \phi_{k-1})]$$

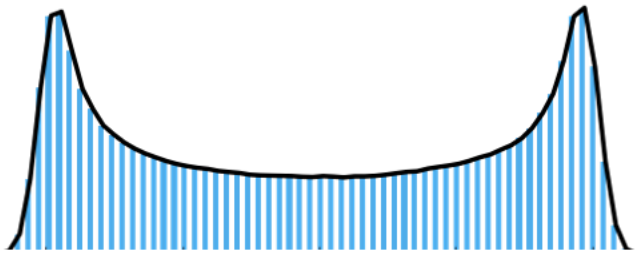




How quantum is my noise?

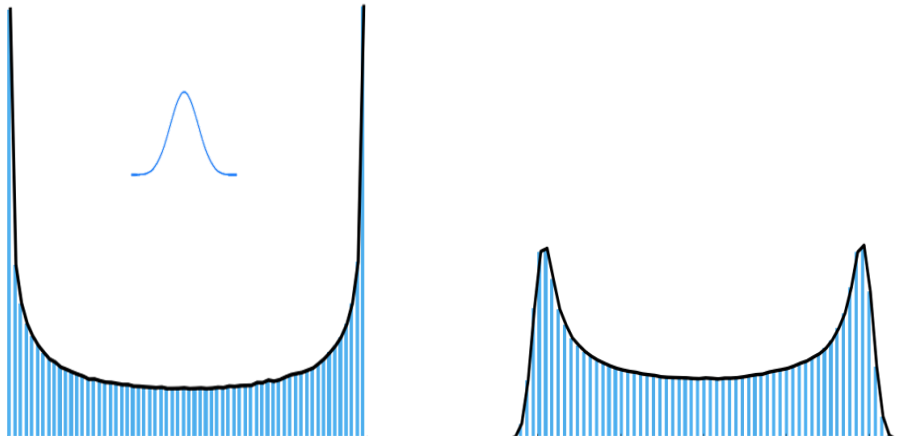
$$u^{(out)}(t) = u_A + u_B + 2\sqrt{u_A u_B}\cos\Delta\phi(t) + u_n$$



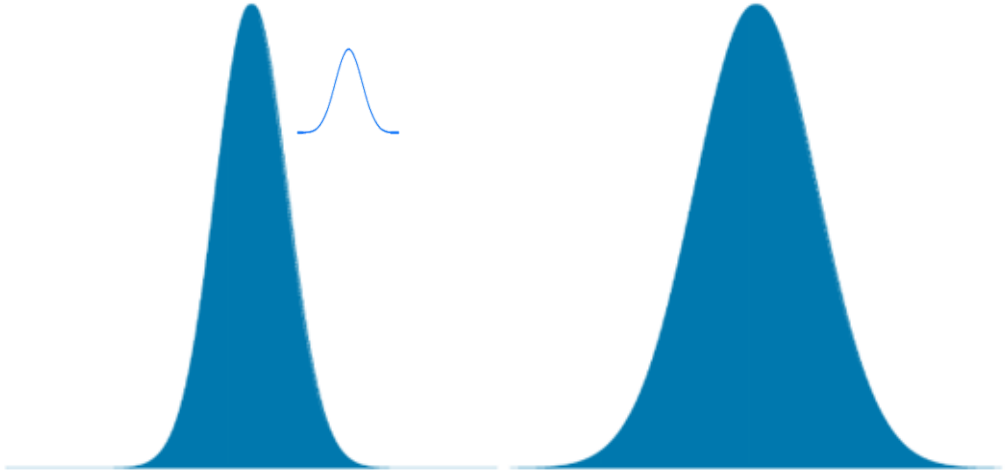


How quantum is my noise?

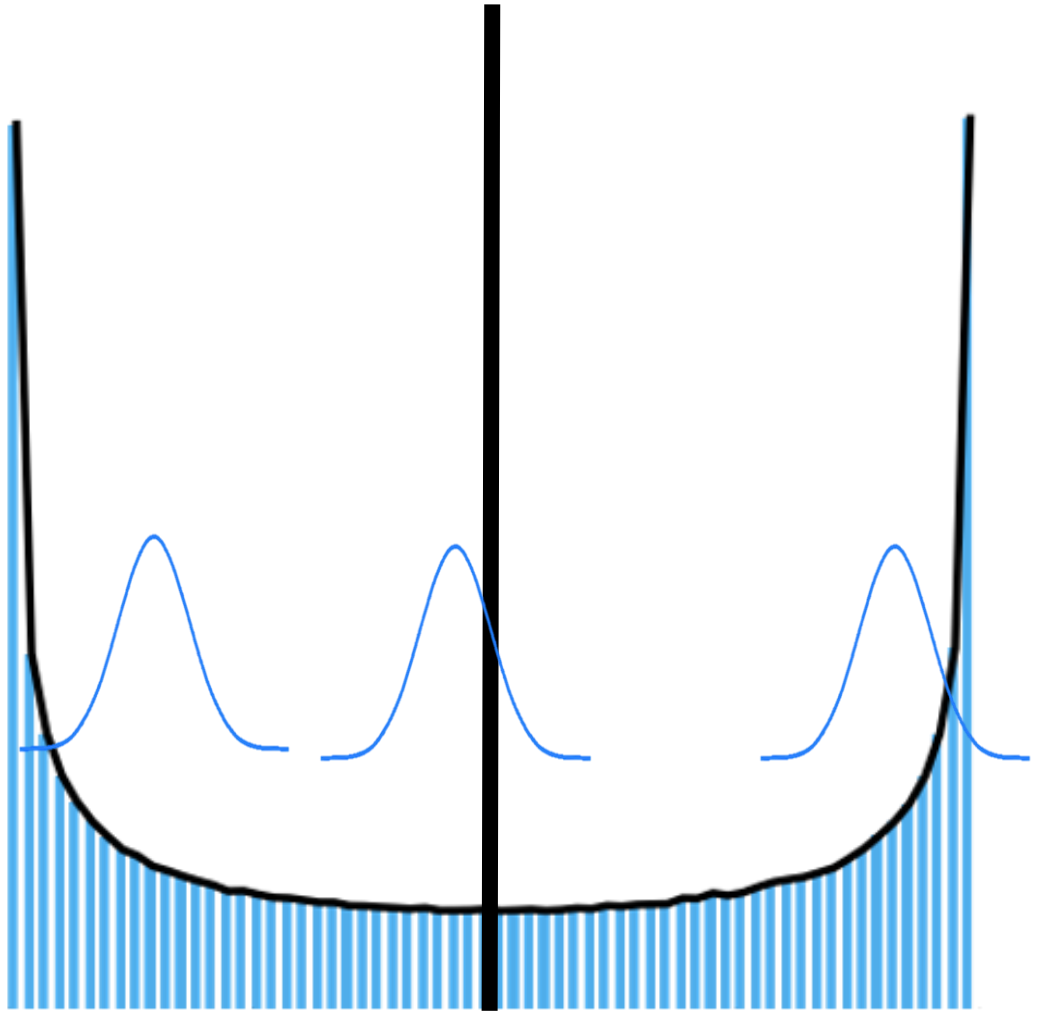
Phase-diffusion process:
Non-gaussian process
The noise and the source distributions are different
Easy to estimate noise effects



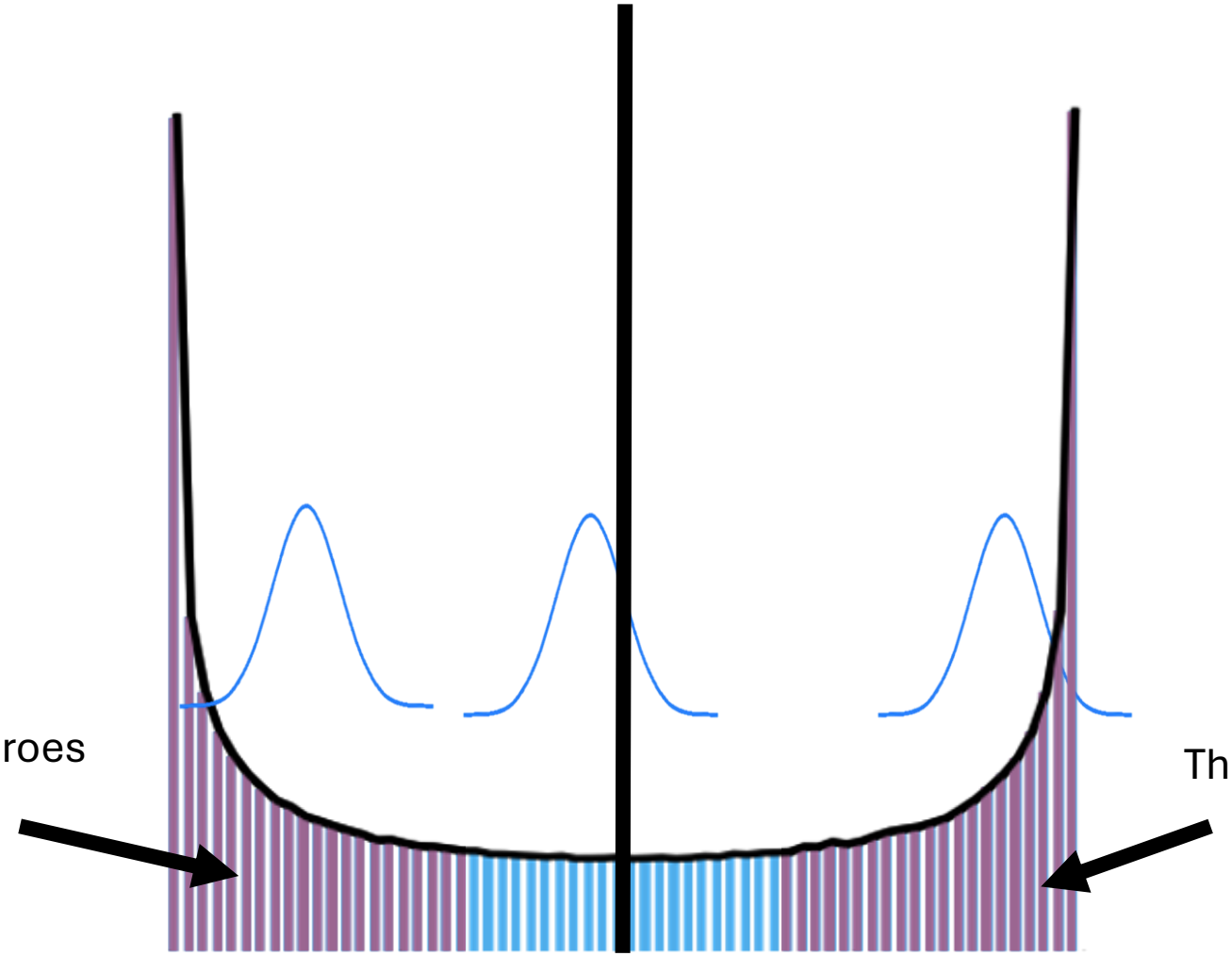
Other processes:
Typically, gaussian processes, or similar
The noise and source distributions are the same
Hard to estimate noise effects



How quantum is my noise?



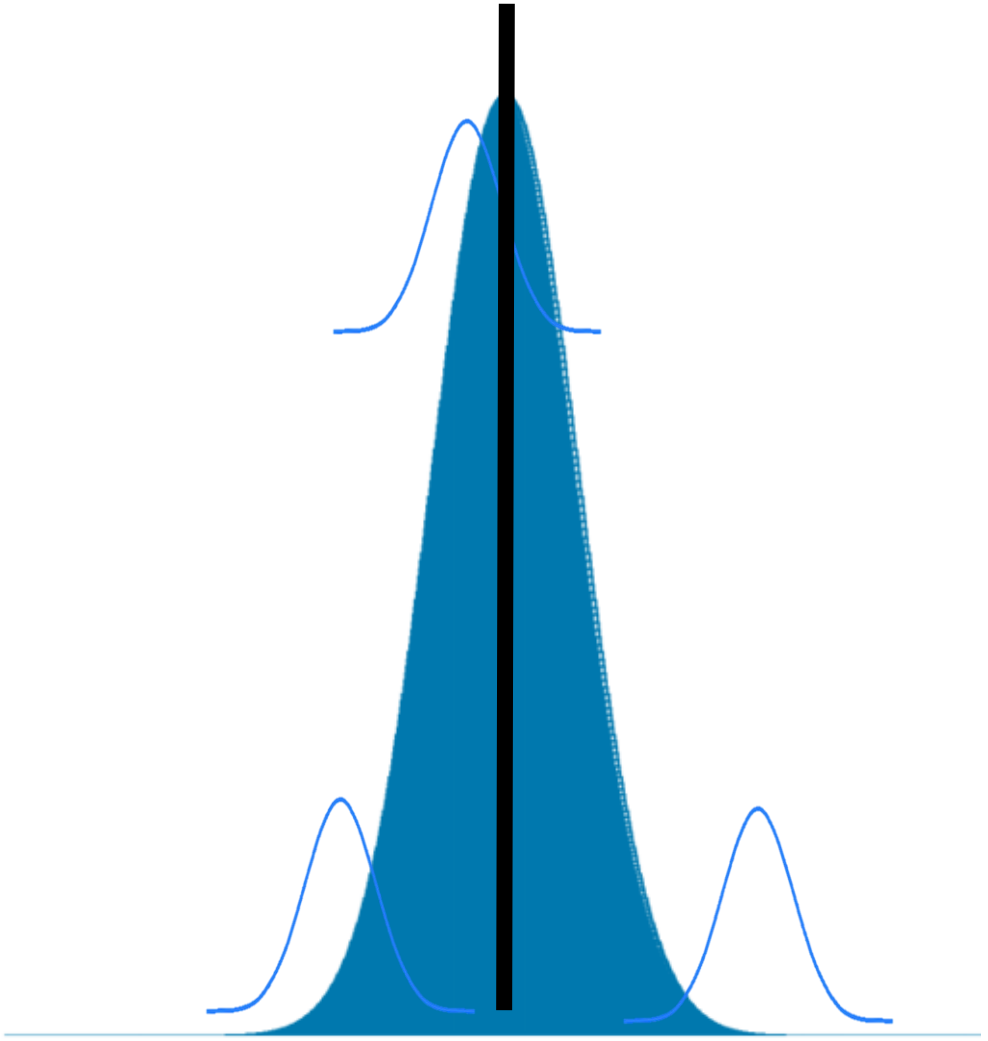
How quantum is my noise?



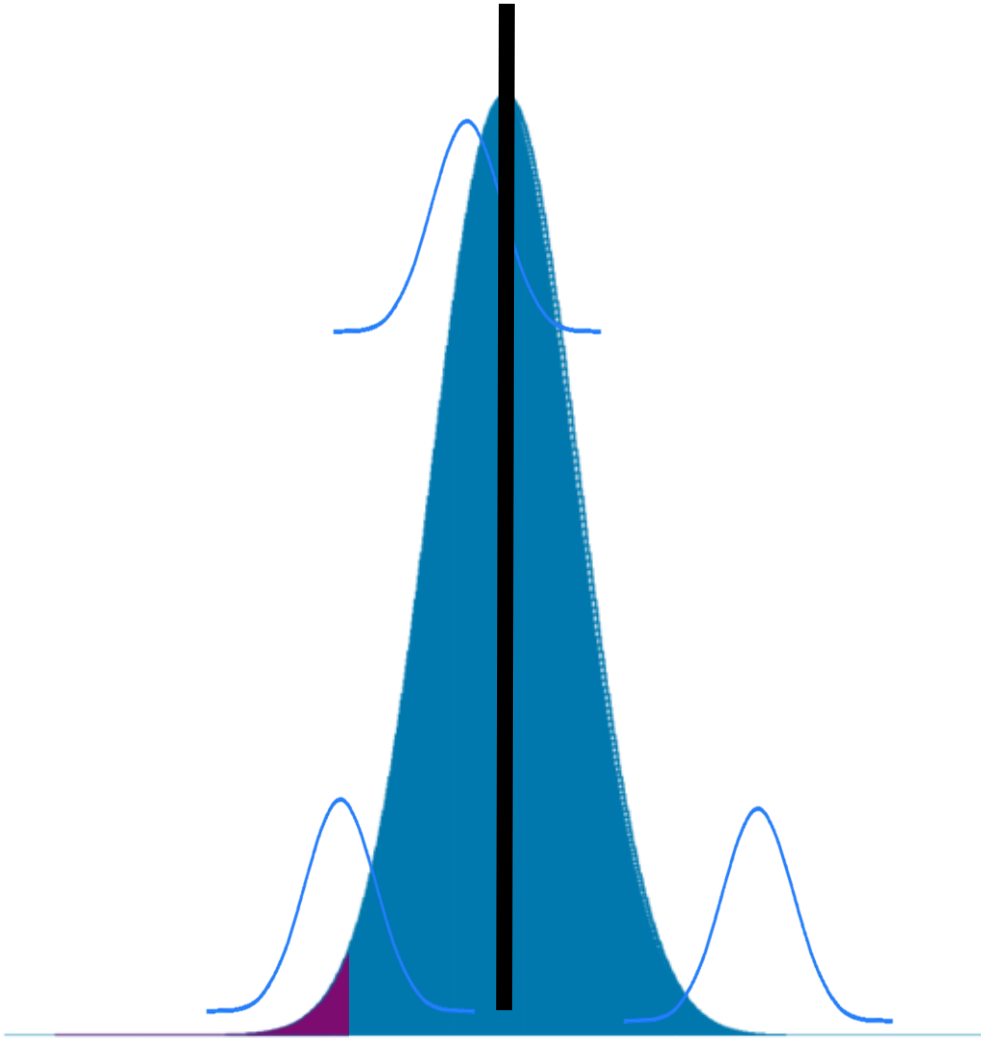
These zeroes are really zeroes

These ones are really ones

How quantum is my noise?

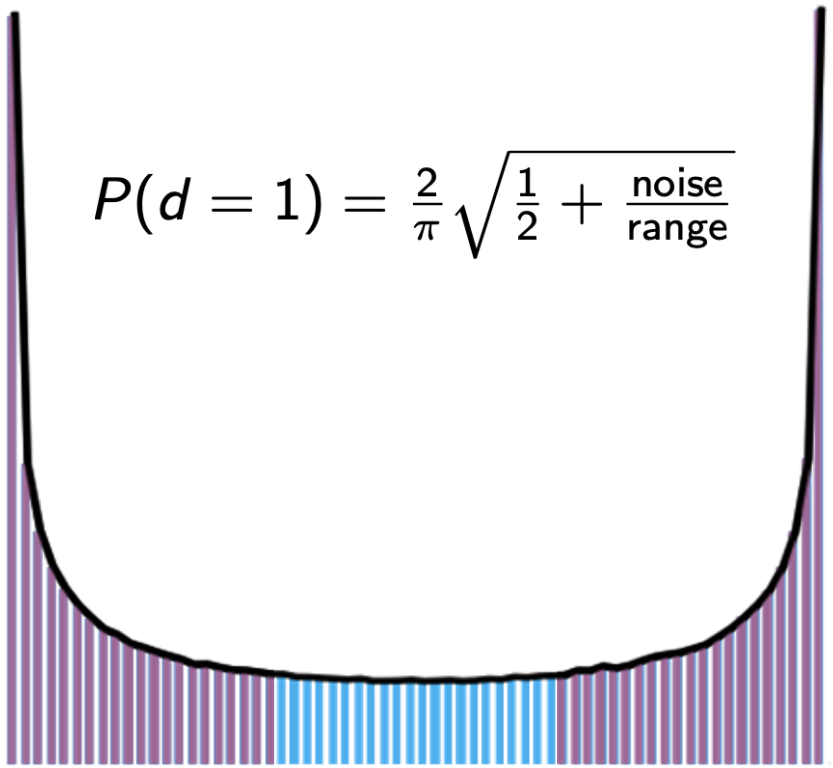


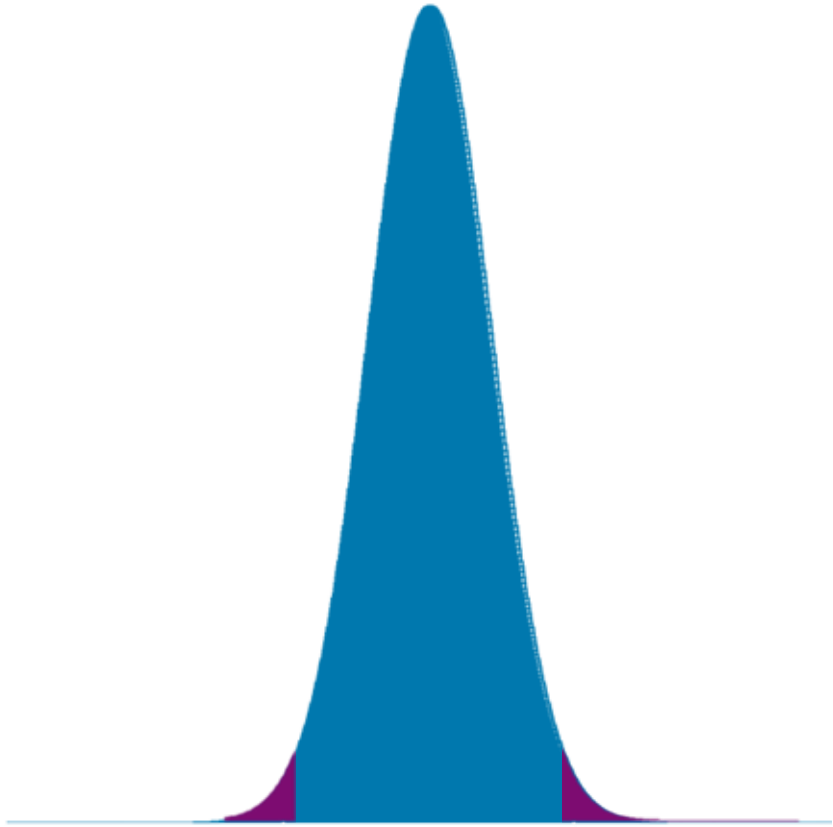
How quantum is my noise?



How quantum is my noise?

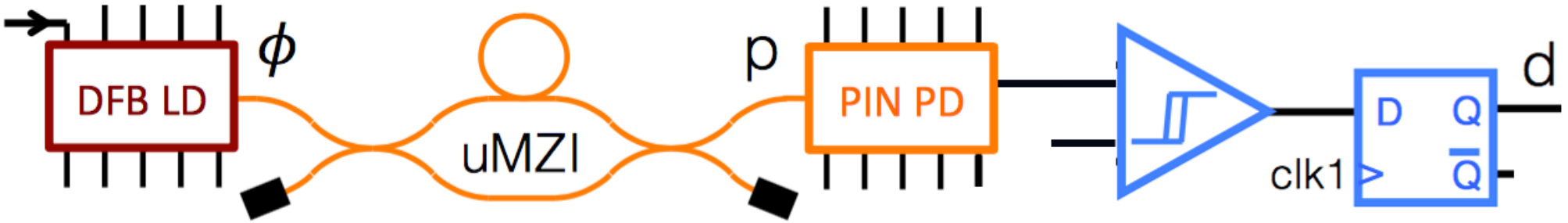
$$P(d=1) = \frac{2}{\pi}\sqrt{\frac{1}{2} + \frac{\text{noise}}{\text{range}}}$$



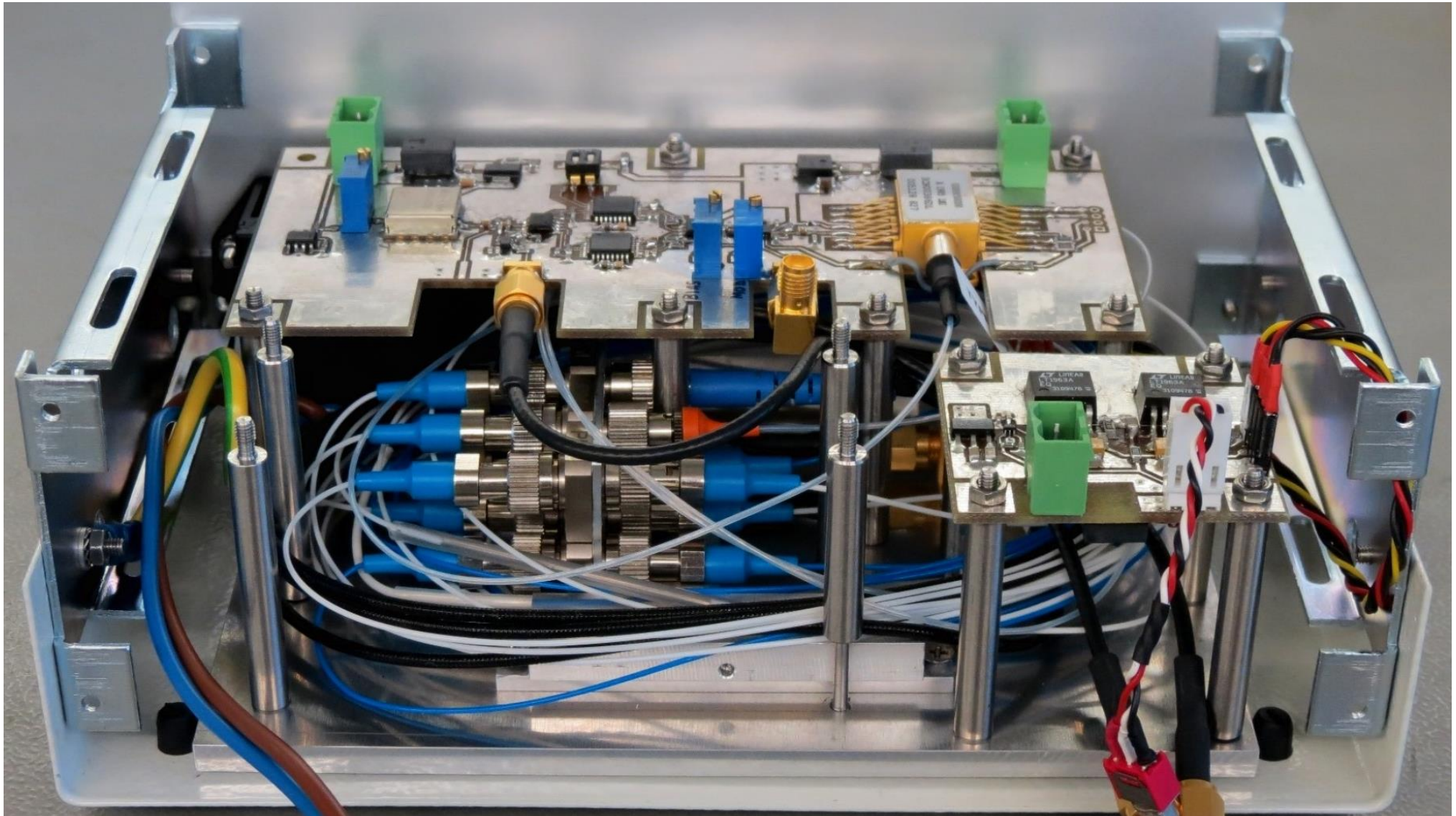


The **conditional min-entropy bound** (= our certainty of origin for the digitized randomness) is much higher for phase-diffusion processes (>90%) than for gaussian processes (<20%).

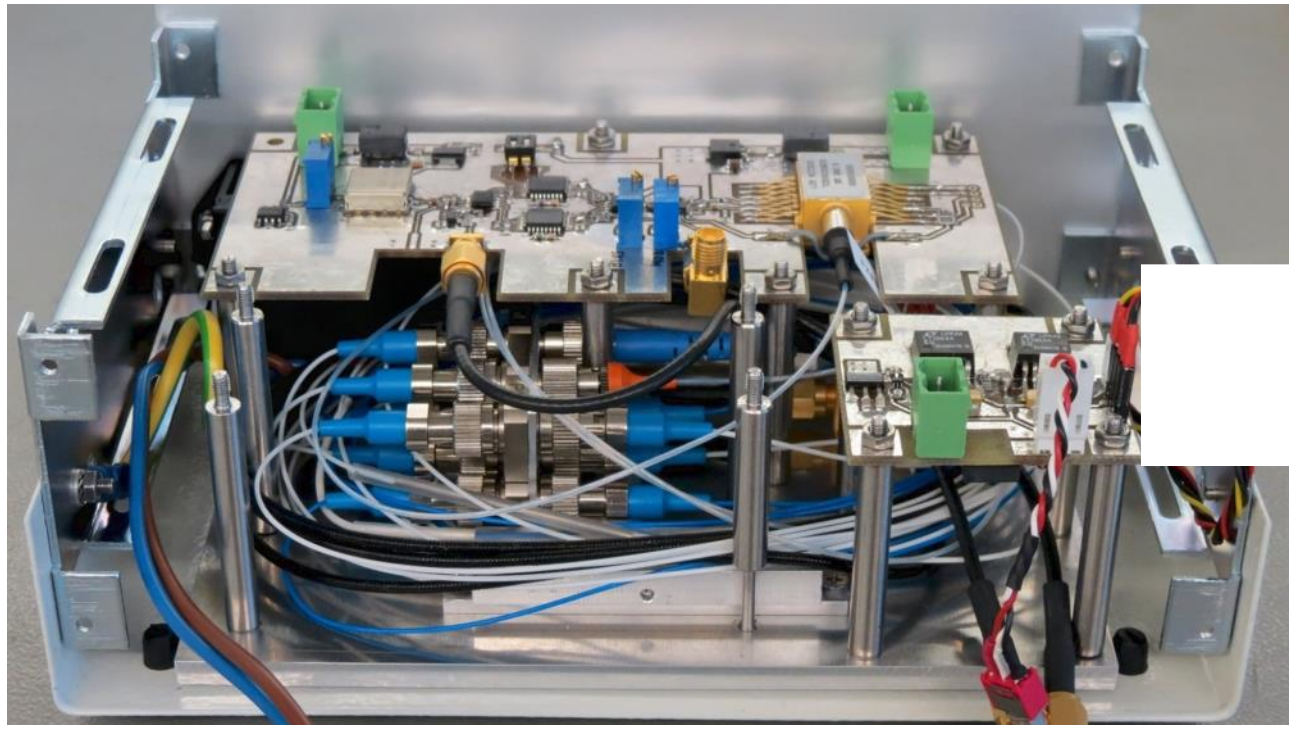
How tiny can you get?

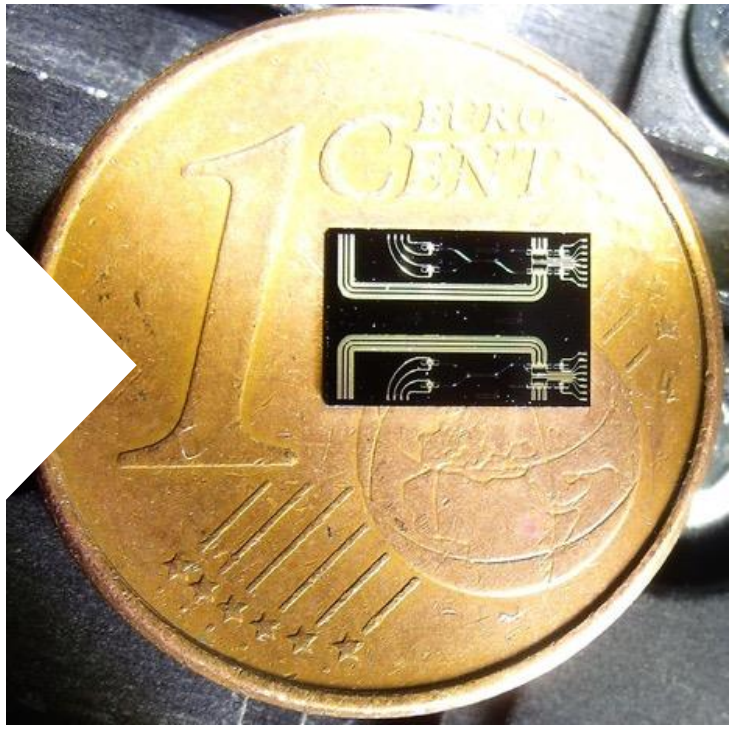


How tiny can you get?



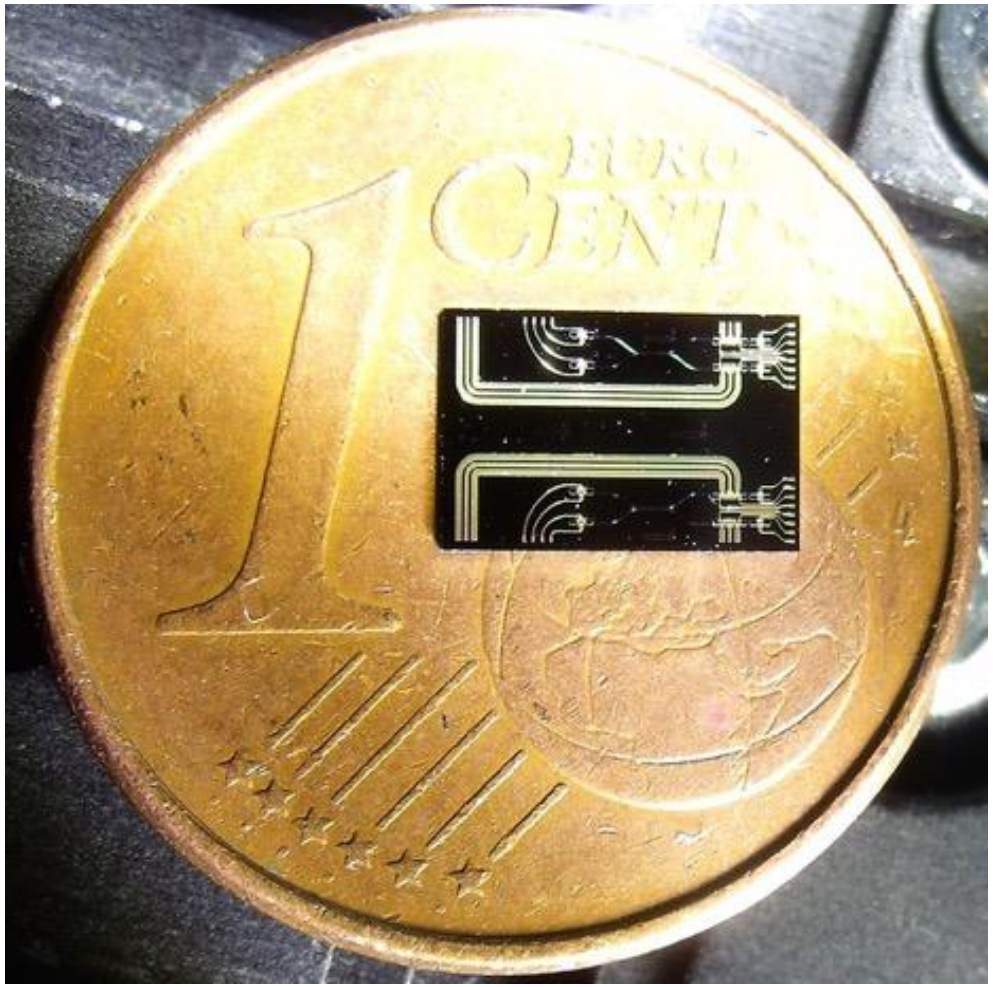
How tiny can you get?

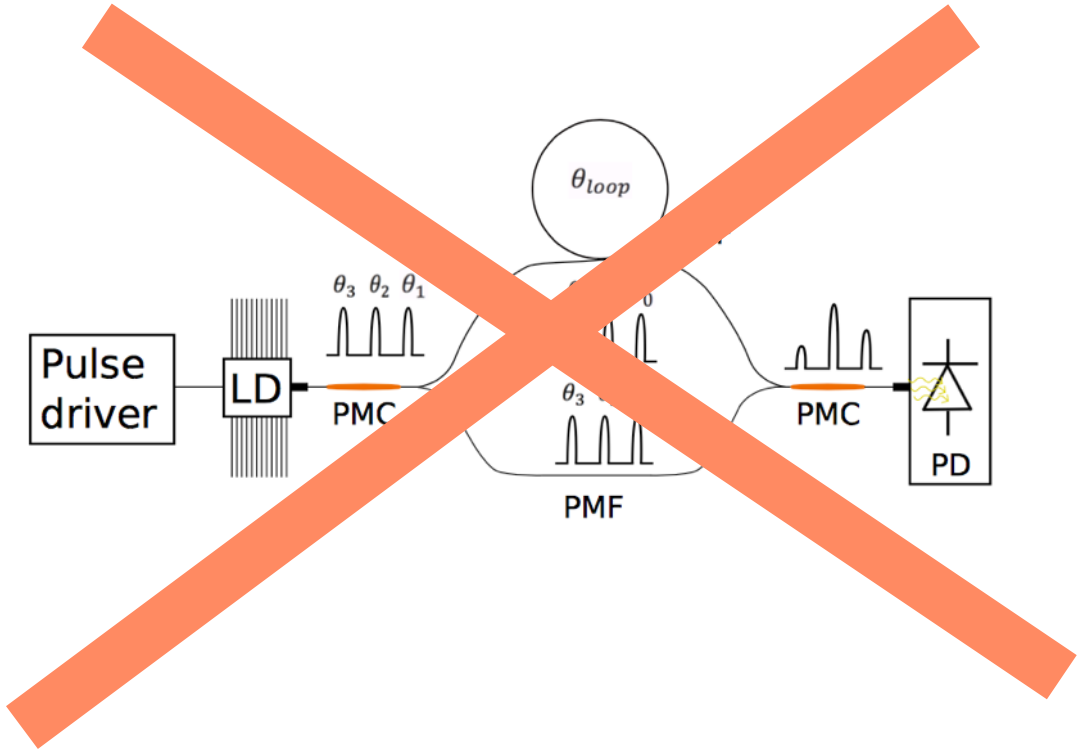




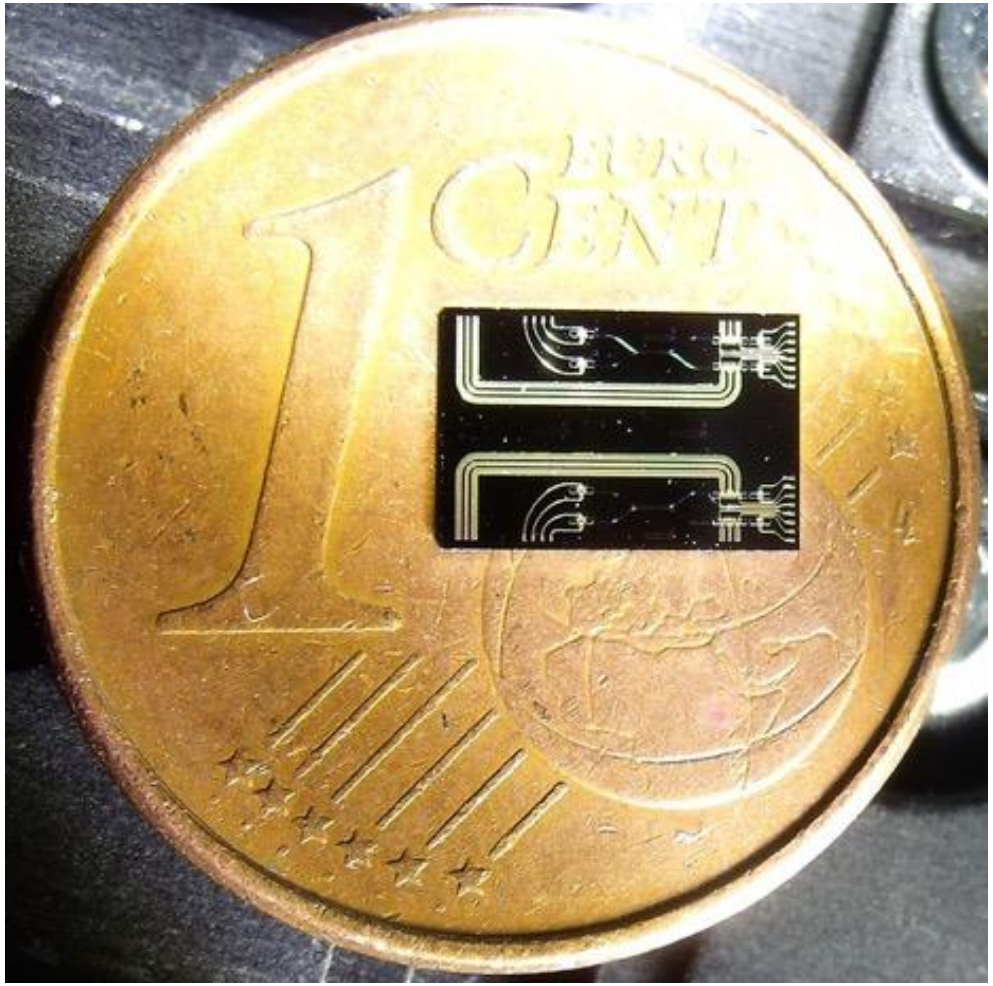
Quside

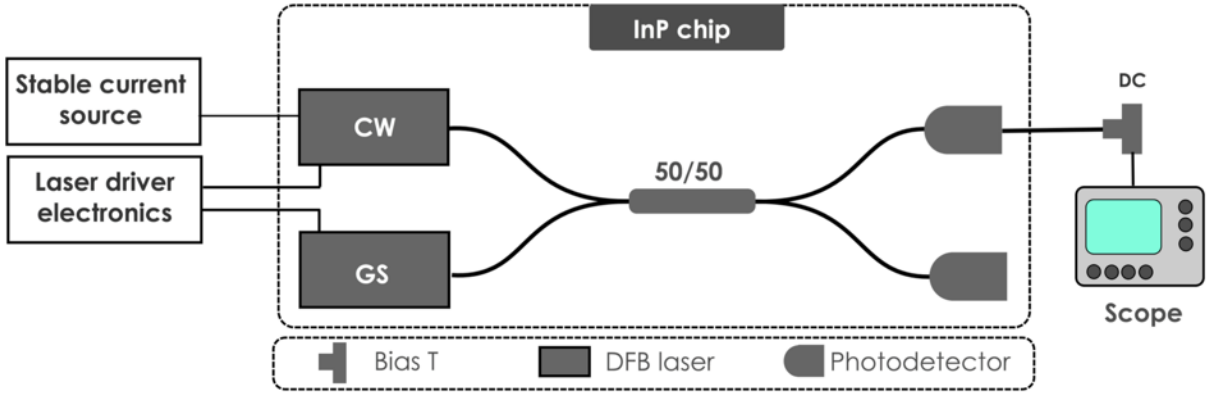
How tiny can you get?





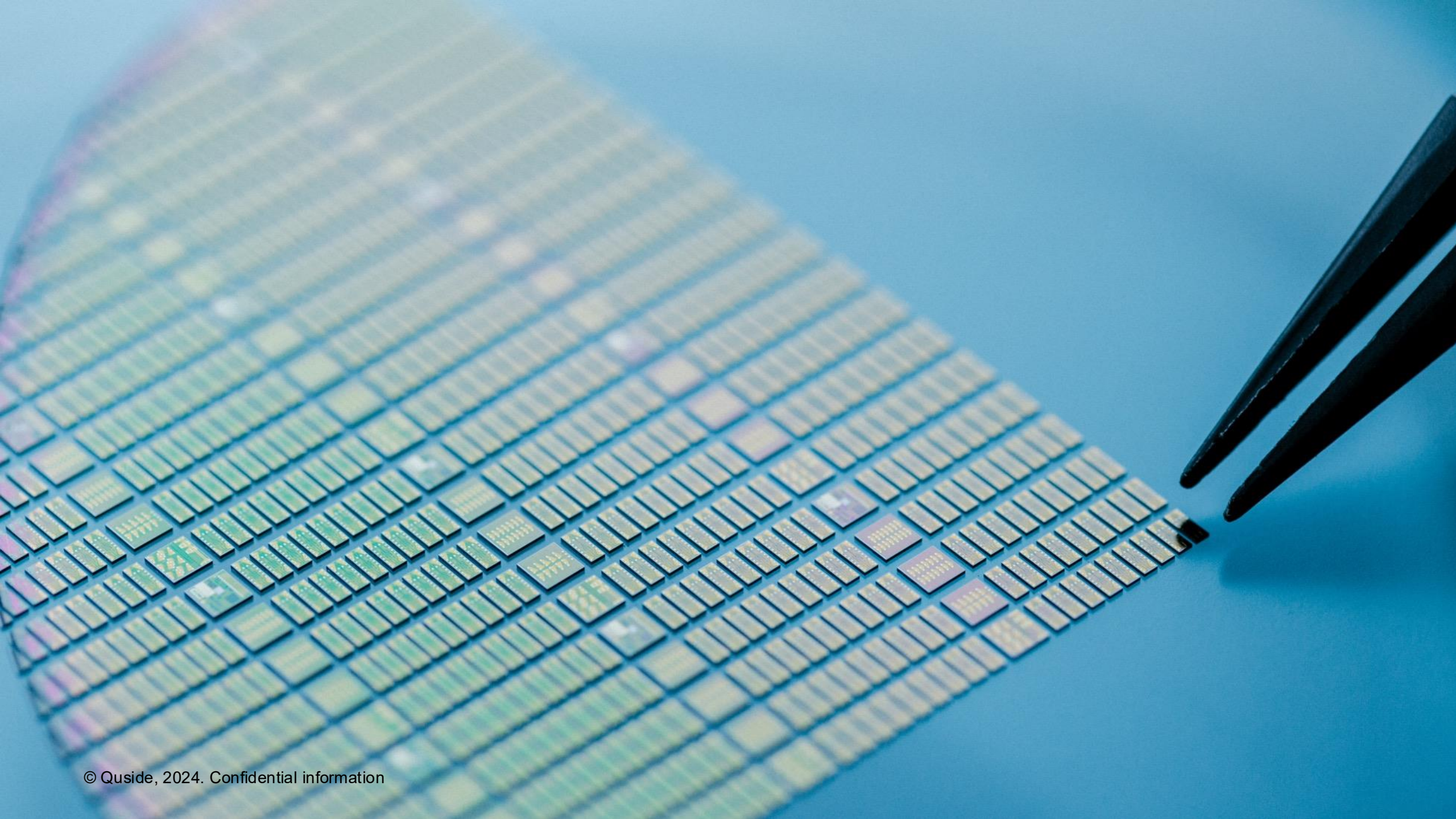
How tiny can you get?

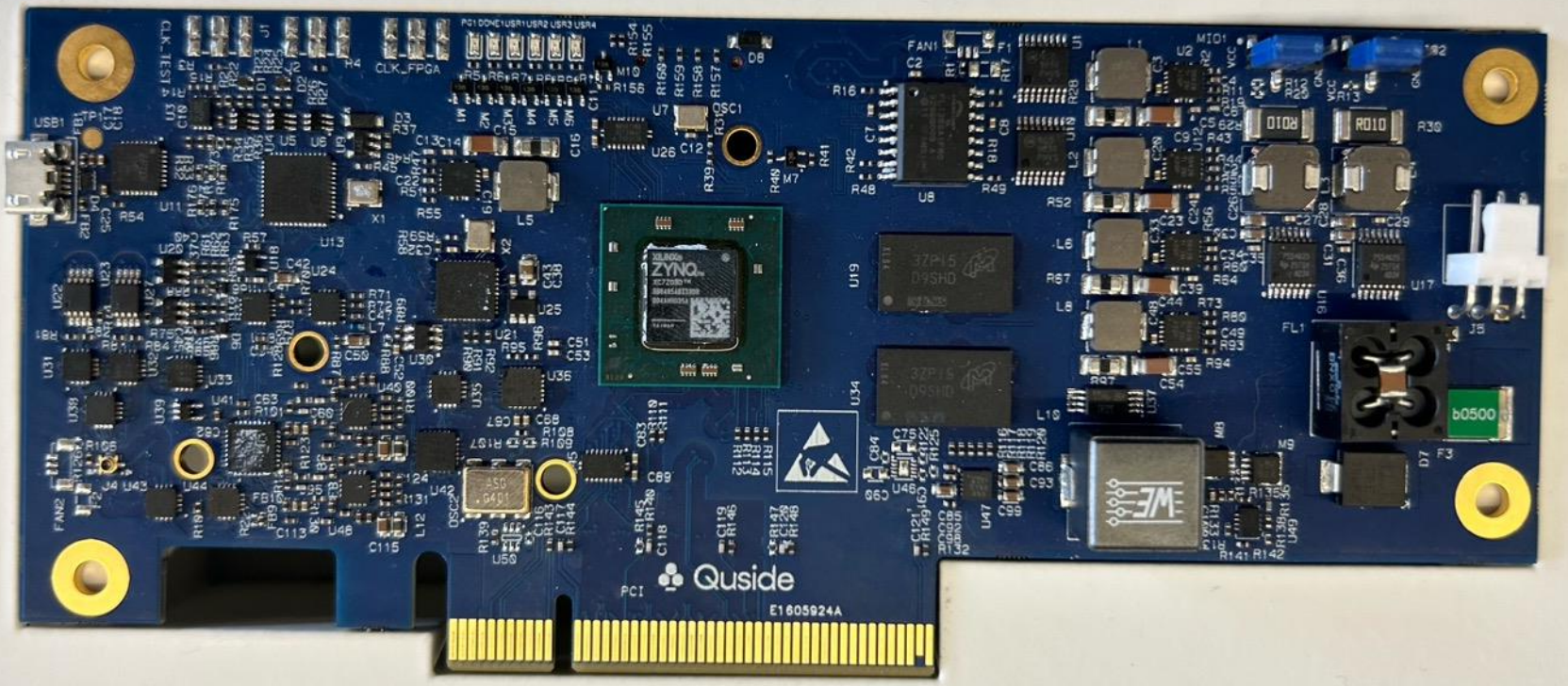




Where are we today at Quside?

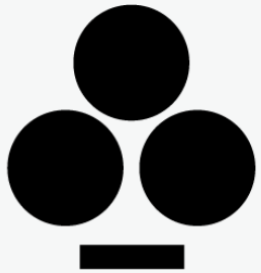
Quside






QRNG / QRNG System Details
job
qrng1
Calibration Status
qrng1
CALIBRATION SUCCED
Min-Entropy
0,972
QFactor
0,993
Voltage Comparator
135 mV
QFactor
1
0.995
0.99
0.985
0.98

Quside



Randomness Processing Unit - Beta Version

By: Quside Latest Version: Beta 0.2.5

Quside's new acceleration platform, based on high-speed randomness sampling and fine-tuned hardware acceleration. Quside's RPUs allow customers to offload their randomness generation and processing tasks from the CPU, thereby accelerating and optimizing their randomized workloads. This fact simultaneously improves their effective computational capacity and the quality of their simulation, optimization, and prediction needs.

Show less

Linux/Unix

Continue to Subscribe

Save to List

Typical Total Price

$1.65/hr

Total pricing per instance for services hosted on f1.2xlarge in US East (N. Virginia). View Details

Product Overview

Random number generation subroutines may involve up to 95% of the total simulation resources for stochastic workloads. Quside's RPU technology accelerates randomized workloads, thus improving your effective computational capacity and the quality of your simulation, optimization, and prediction needs. Thanks to these improvements you can obtain competitive advantages with the possibility of making better decision in a shorter time and reduce your infrastructure costs in terms of CAPEX and OPEX.

Highlights

- Optimized sampling from the most frequently utilized probability distributions in computational workloads.
- Provable performance improvements of up to 10X and energy efficiencies of up to 20X,

hello@quside.com