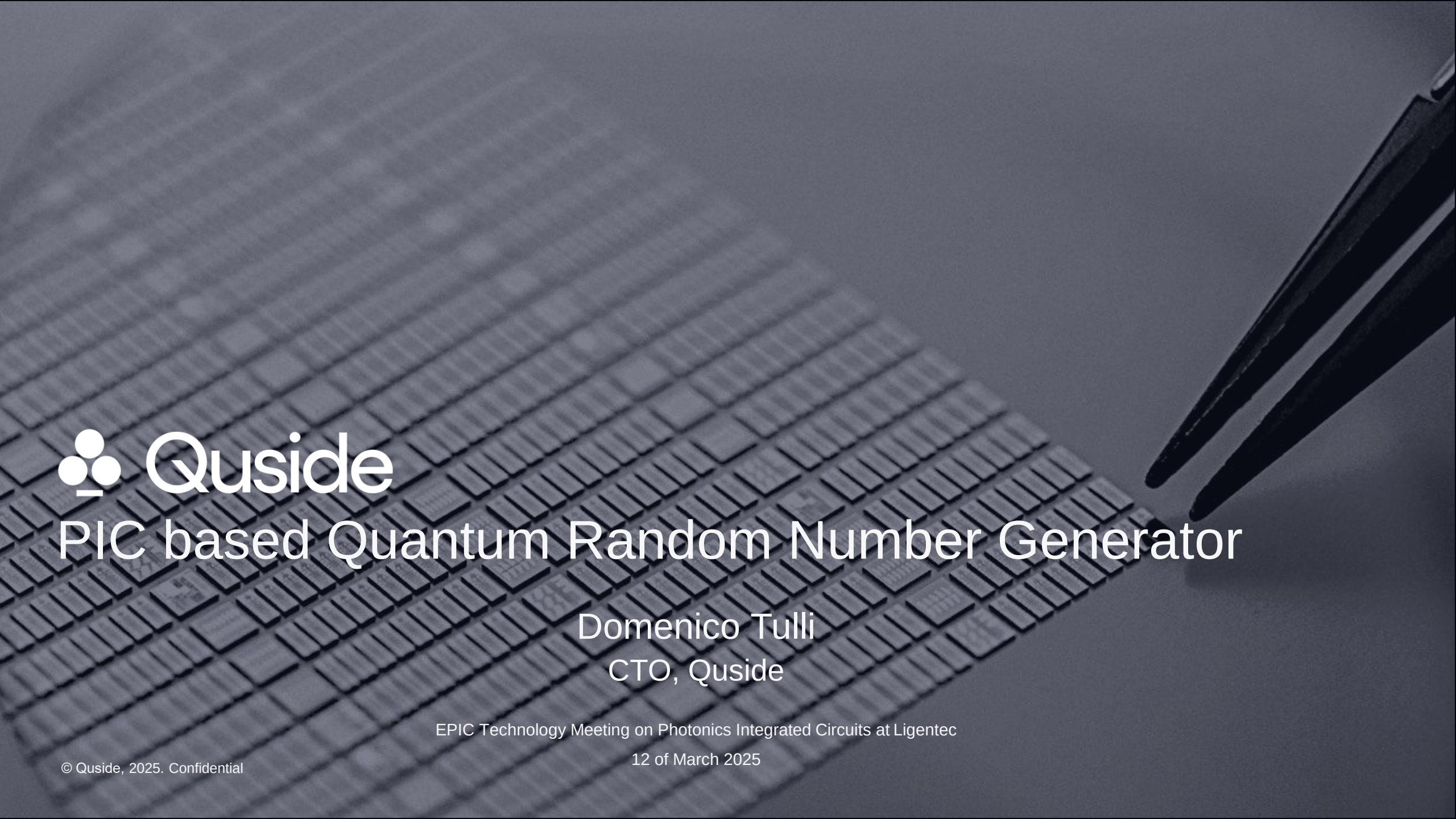


PIC based Quantum Random Number Generator

Domenico Tulli
CTO, Quside

EPIC Technology Meeting on Photonics Integrated Circuits at Ligentec

12 of March 2025

© Quside, 2025. Confidential

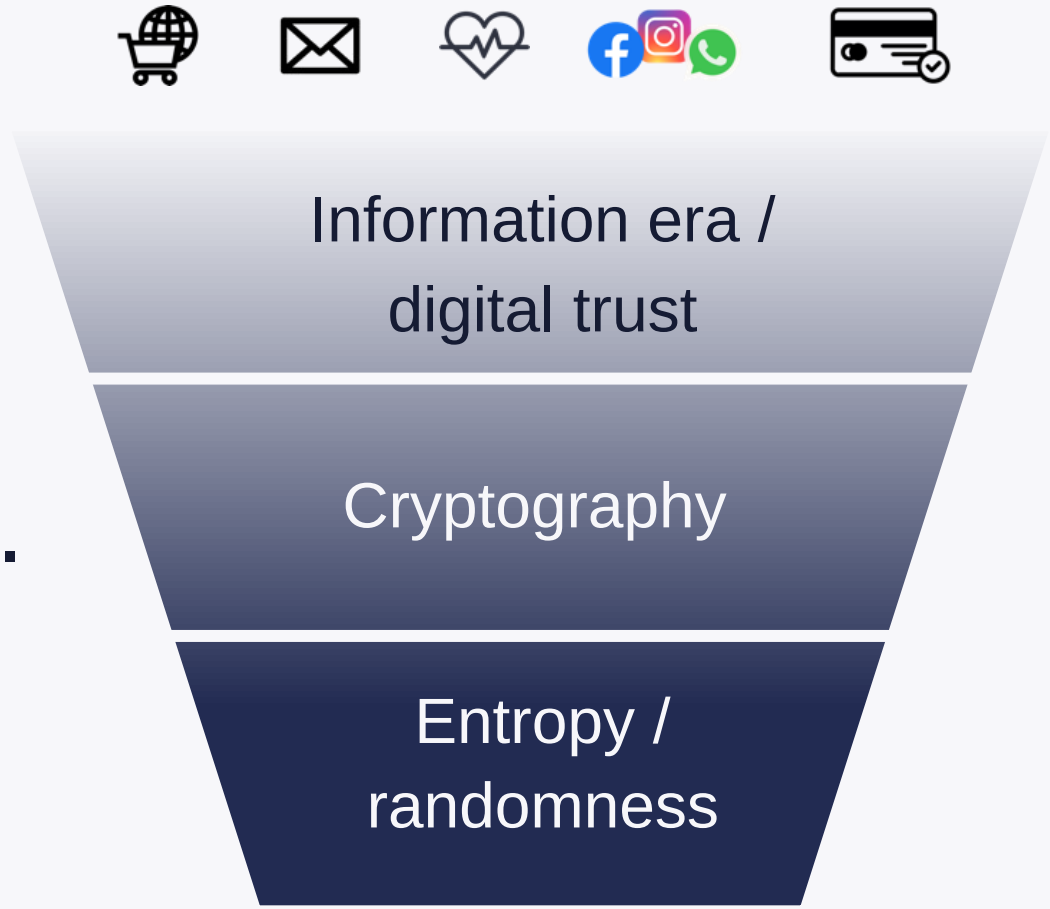
About Us

Founded **2017**	Investment **15M+**
Employees **50+**	Patents Worldwide **70+**

Located in Barcelona, Spain
Span-out from ICFO

© Quside, 2025. Confidential

We believe everyone, everywhere should have access to the **strongest foundation of digital trust**.



© Quside, 2025. Confidential

The cost of bad randomness

No (hardware) randomness, no security

2022

Affected SAMSUNG

100M+ phones affected

2023

Affected CISCO

Low-entropy key vulnerability in firewalls

Discovered by KUDELSKI SECURITY

10M€ stolen and nobody noticed (random!)

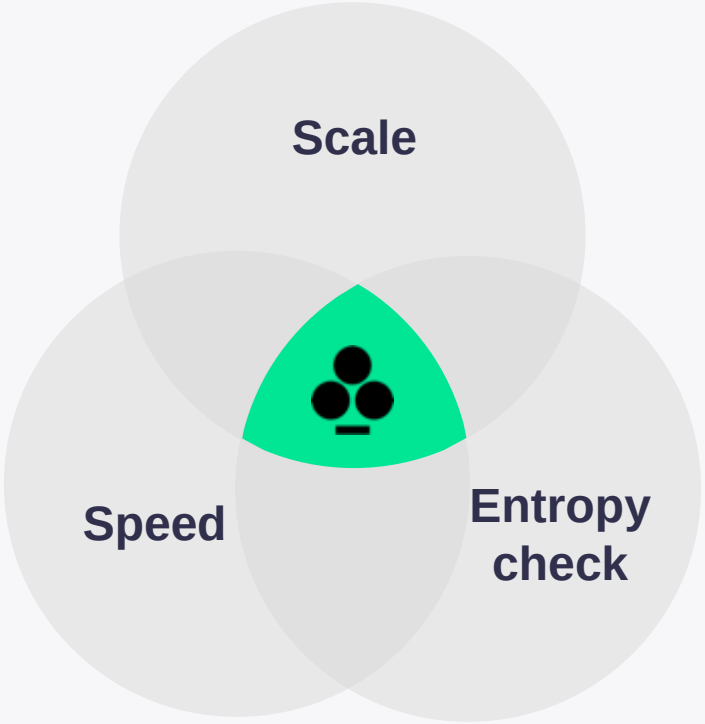
2024

Affected

Random flaw in ECDSA library

Published by Meta

Vulnerability in LWE due to bad random



No solution properly checks quality at speed & scale

True random numbers assure key quality (foundation)

© Quside, 2025. Confidential

Our Products

Scalable quantum entropy with runtime entropy monitoring

QRNG	Entropy Core	RPU
	EQUINIX aws	aws marketplace
IP, Chips & Modules	Infrastructure Solutions	Stochastic Acceleration

© Quside, 2025. Confidential

Our Focus Areas

Data Centers, Networks, and AI Factories

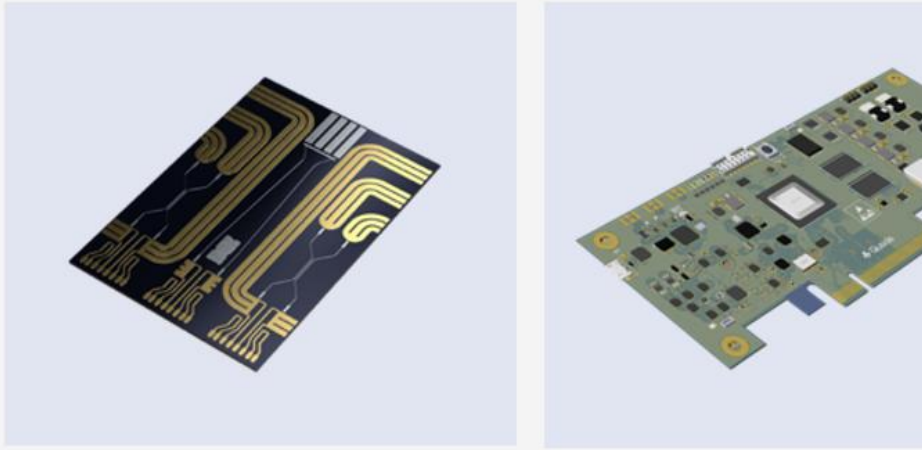
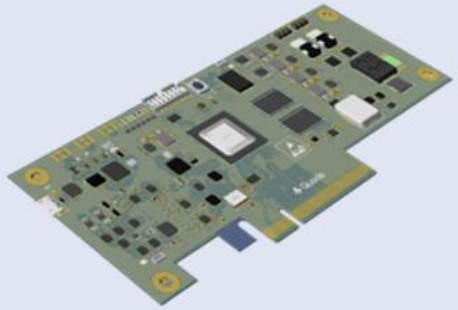
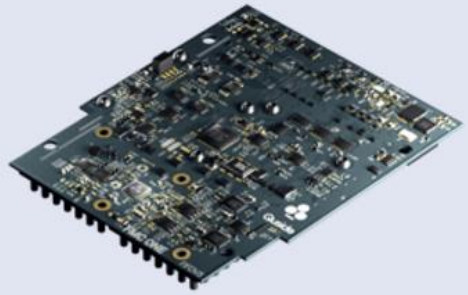
Consumer Products

Space, Government, and Defense Security Systems

© Quside, 2025. Confidential

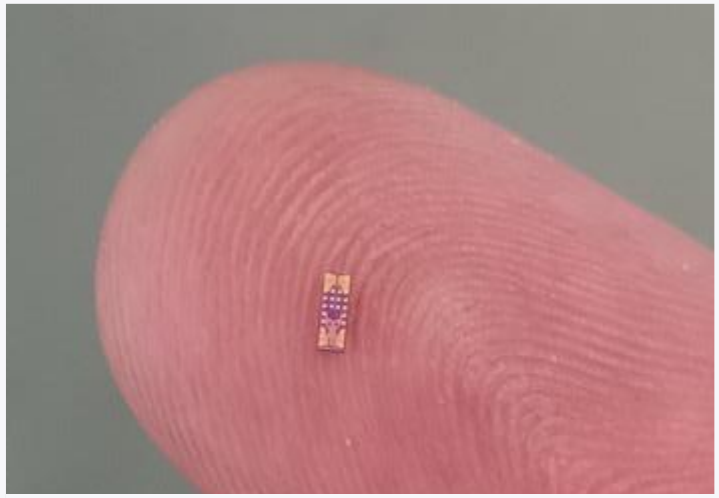
QRNG offerings – Observable & NIST SP800-90B certified

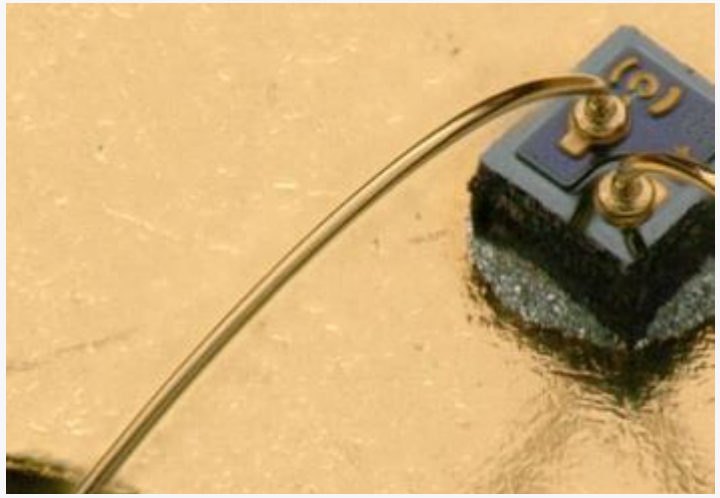
Scalable quantum entropy with runtime entropy monitoring

Ruby™ Series	Garnet™ Series	Nellite™ Series	Onyx™ Series
			
Ruby N1 (1Gb/s) Ruby S1 (50Mb/s) Scalable	Versatile (100Mb–1Gb/s Plug-and-Play PCIe Gen2x4	Versatile (100Mb–1Gb/s Developer-Ready FMC (ANSI VITA)	Reliable (50–100 Mb/s) Efficient Integration Space-Saving Design

© Quside, 2025. Confidential

Our Core Quantum Entropy Technologies





Our quantum photonic entropy core technologies

N1 chip
The high-performance solution
Gain switching / Phase
Wafer-level capability
Gb/s +

S1 chip
High-volume solution
Gain switching / Polarization
Partnered with volume manufacturers
~50 Mb/s

Benefits of embedding Quside entropy technology in your next hardware design

- ✓ Stronger security & trust with runtime entropy verification (enabled by quantum)
- ✓ Reduced software dependence with faster hardware performance.
- ✓ Simpler design verification with Silicon-independent entropy design.

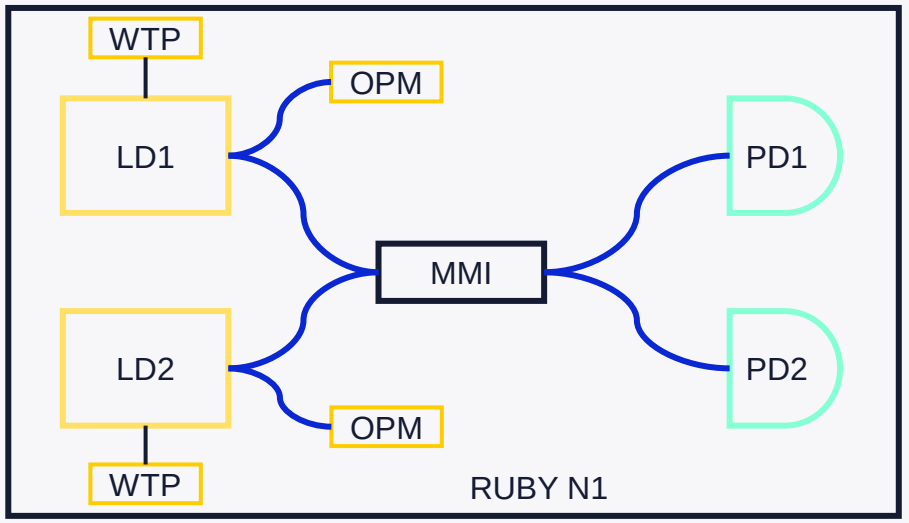
© Quside, 2025. Confidential

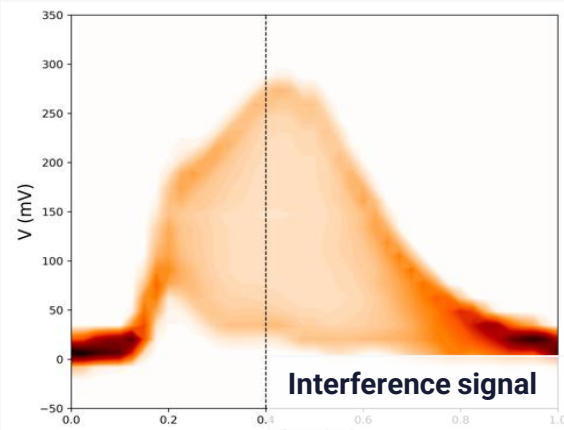
RUBY N1 Integrated Entropy Source in InP

Principle of operation.

How do we convert quantum phase fluctuations into digital random bits?

1. Gain-switched laser generates phase-random optical pulses.
2. Local oscillator & interferometer transform phase into amplitude.
3. Random amplitudes are photodetected & easily digitized.





Interference signal

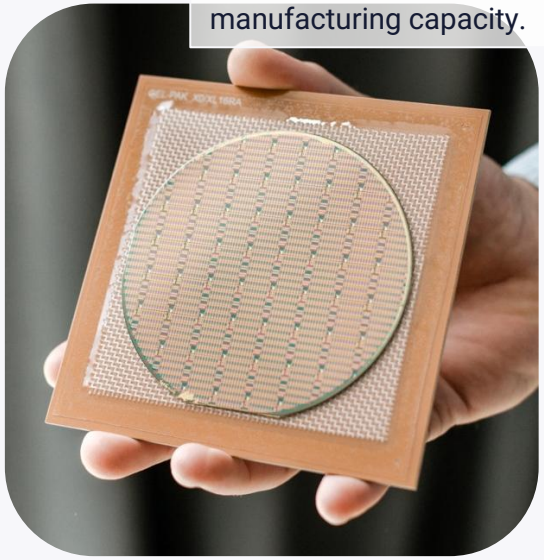
Very high interference range demonstrates high quality quantum noise detection.

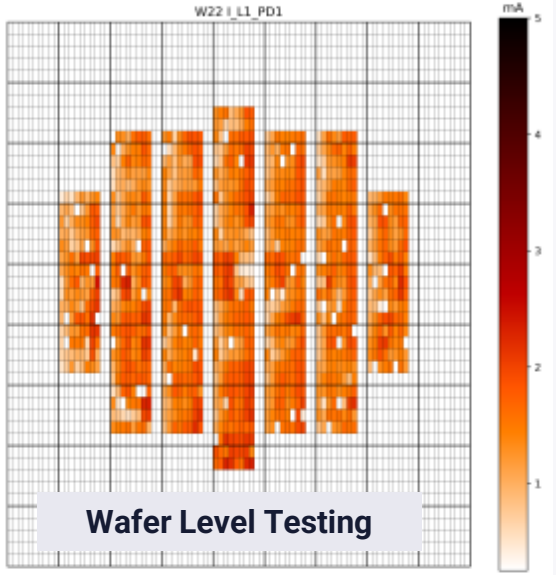
$$i_{PD}(t) = i_{L1}(t) + i_{L2}(t) + 2\sqrt{i_{L1}(t)i_{L2}(t)}\cos(\Omega_b t + \Delta\phi)$$

Quantum random phase

RUBY N1 chips

Wafer-level photonic chip manufacturing capacity.



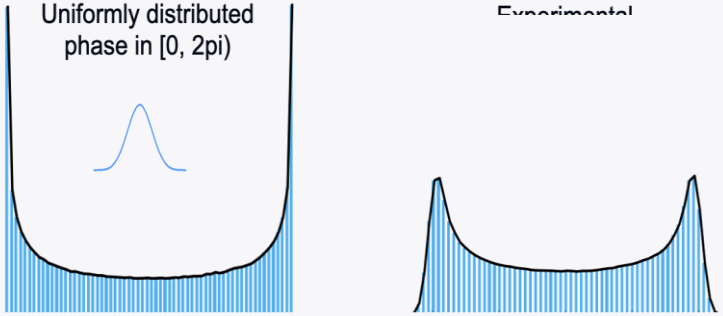


Wafer Level Testing

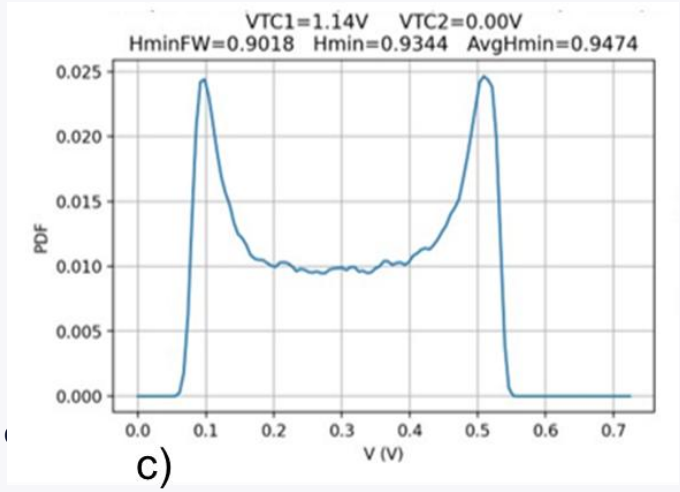
© Quside, 2025. Confidential

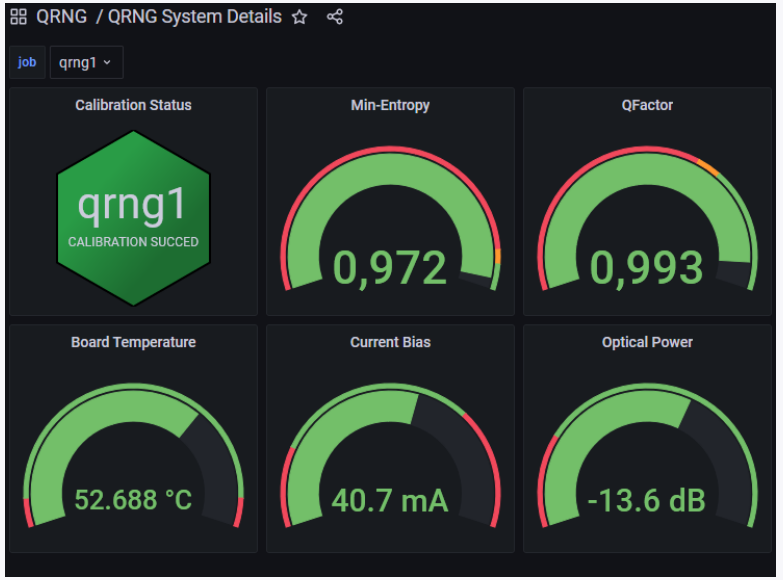
QRNG Metrology

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



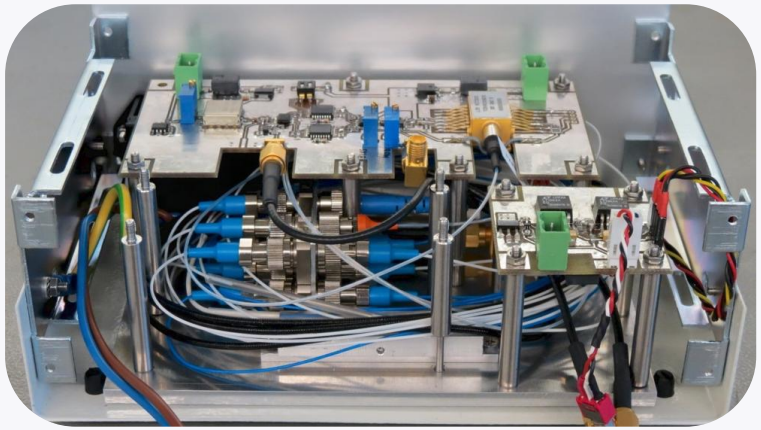
Other processes:
Typically, gaussian processes, or similar
The noise and source distributions are the same
Hard to estimate noise effects



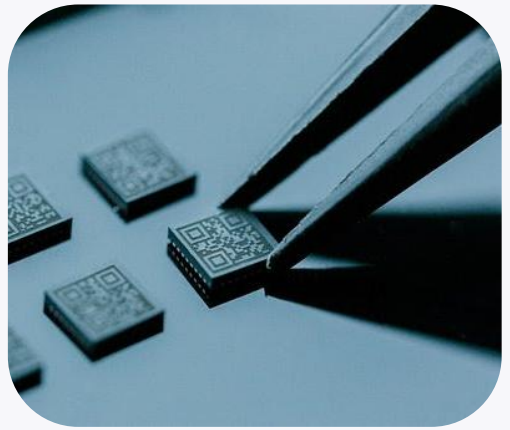


© Quside, 2025.

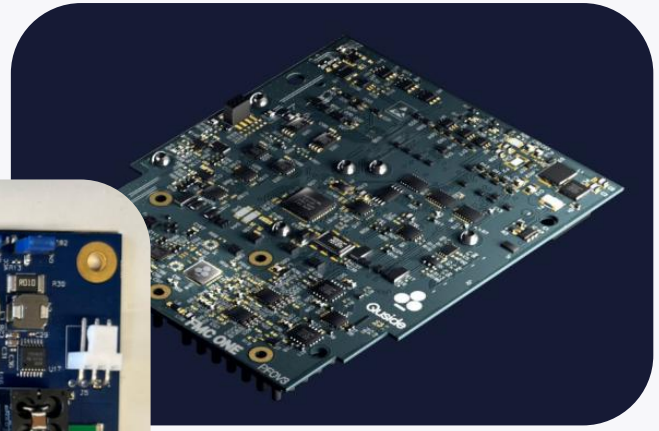
QRNG generation at Quside

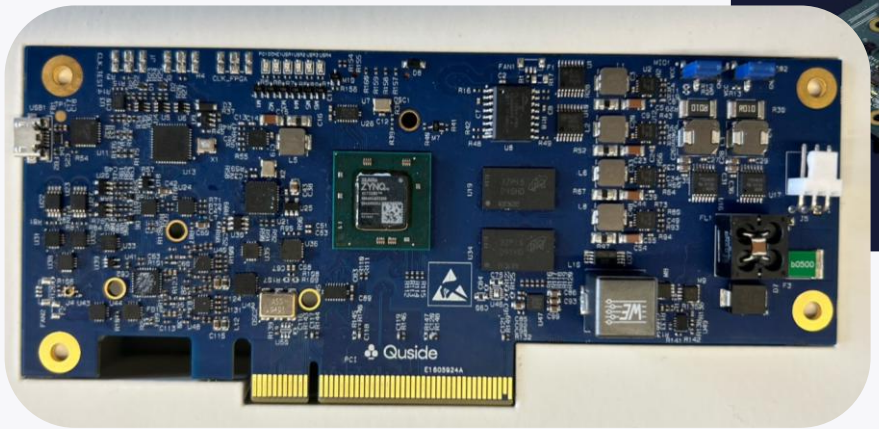


2012: first prototype

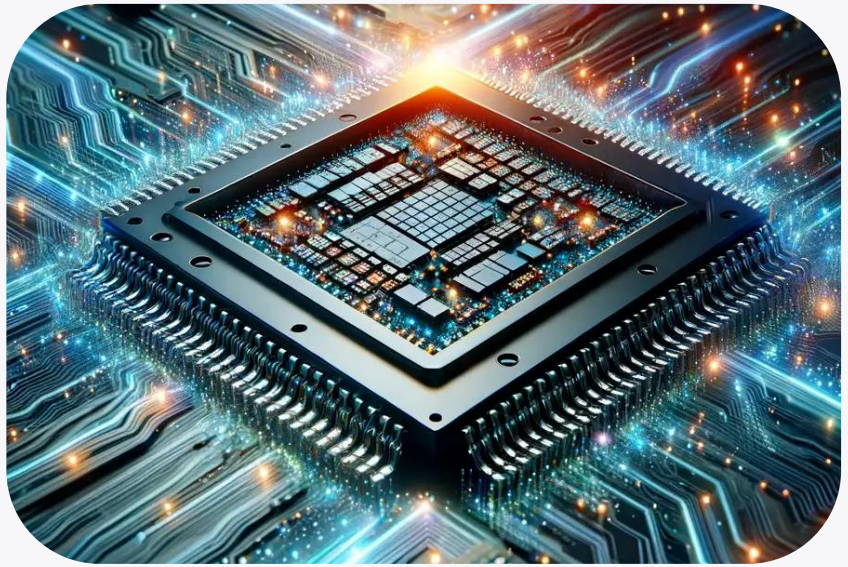


2021: Scalable PIC QES





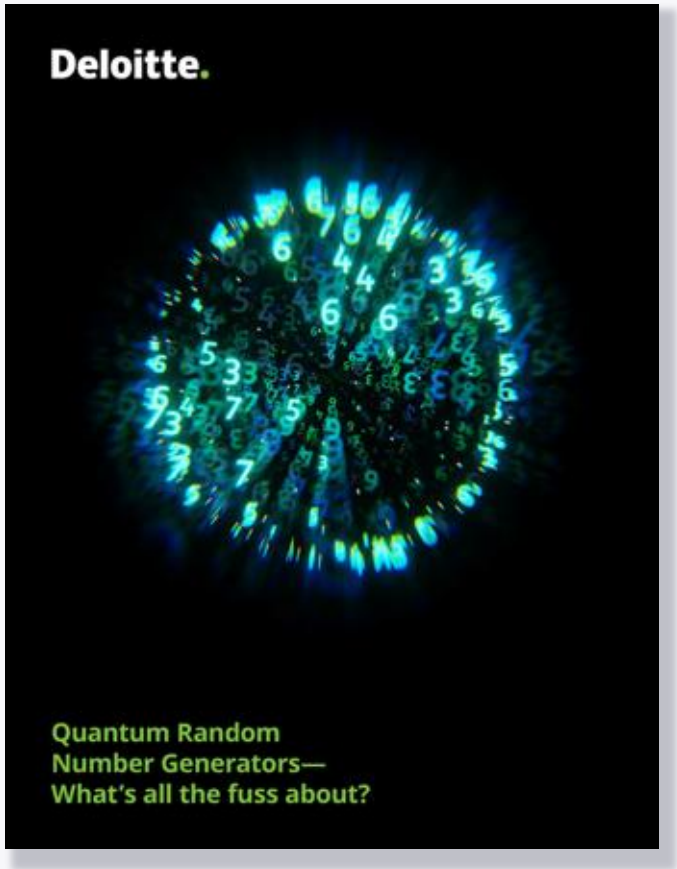
2023-2024: modules



Next: SoC

Navigating the Level of Random Number Generation

Joint Publication Between **Quside** And Deloitte Global Quantum Cyber Readiness Capability Team



Classification of RNG sources

			Examples
Quantified uncertainty	**Level 4**	Ability to model and verify the unpredictability of the physical processes underlying the entropy generation process in real time.	QRNG with metrology
Engineered chaos	**Level 3**	Components are tailored to generate entropy by design, however, attacks are still possible. Their unpredictability relies strongly on statistical tests, as physical tests of unpredictability are either impossible or are too complex.	TRNG (ring oscillators, avalanche diodes...)
Opportunistic randomness	**Level 2**	Systems leverage processes that exhibit seemingly unpredictable behaviour as non-dedicated entropy sources. Rely on external, often uncontrolled factors.	Mouse movement, keyboard strokes, clock jitter...
Illusion of randomness	**Level 1**	There's a facade of randomness rather than its actual presence. Low or non-existing entropy is used. E.g., same numbers are used again and again, or deterministic/pseudo-RNG use.	Software-based RNG, RN files

- Unpredictability +

https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/qrng-what-is-the-fuss-all-about.pdf

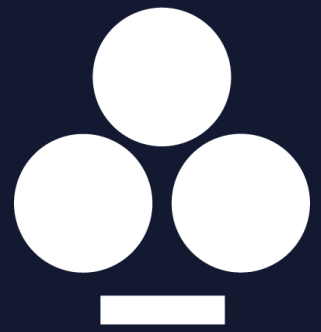
© Quside, 2025. Confidential

Conclusions

- **Interested in:**
- hybrid/heterogeneous approaches to accelerate innovation
- PIC/EIC co-integration
- Wafer level testing both DC and RF
- Digital and Analog SoC design and manufacturing

© Quside, 2025. Confidential

Thank you!



dtulli@quside.com