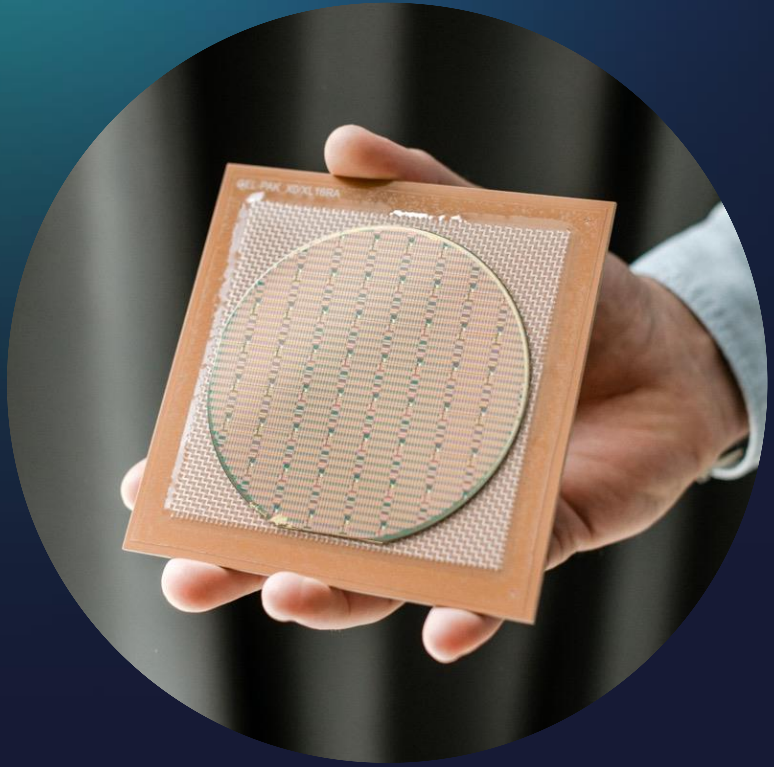
Quside

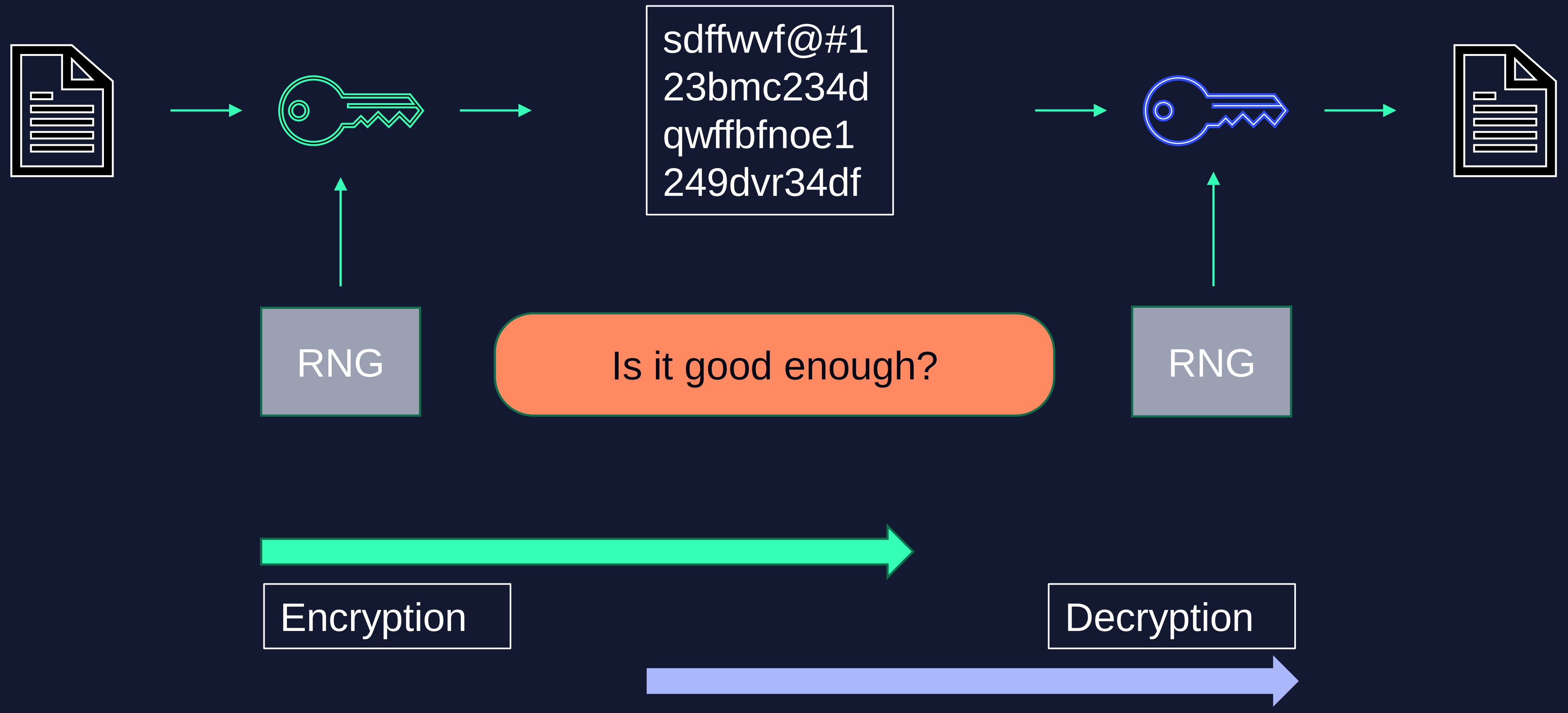


Fast and Scalable PIC-based QRNG for Advanced Solutions

Domenico Tulli

IST-SET-198-RSY on Quantum Technology for Defence and Security
04 October 2023, Amsterdam

Randomness is at the base of any encryption system



Military experts at NATO and partner forces looking at encryption and HF radio to assure secure links on the battlefield

Military & Aerospace Electronics, 2020

Senior Officials: DoD Supports Strong Encryption for Defense, Commercial Security

U.S. Department of Defense, DoD News, 2016

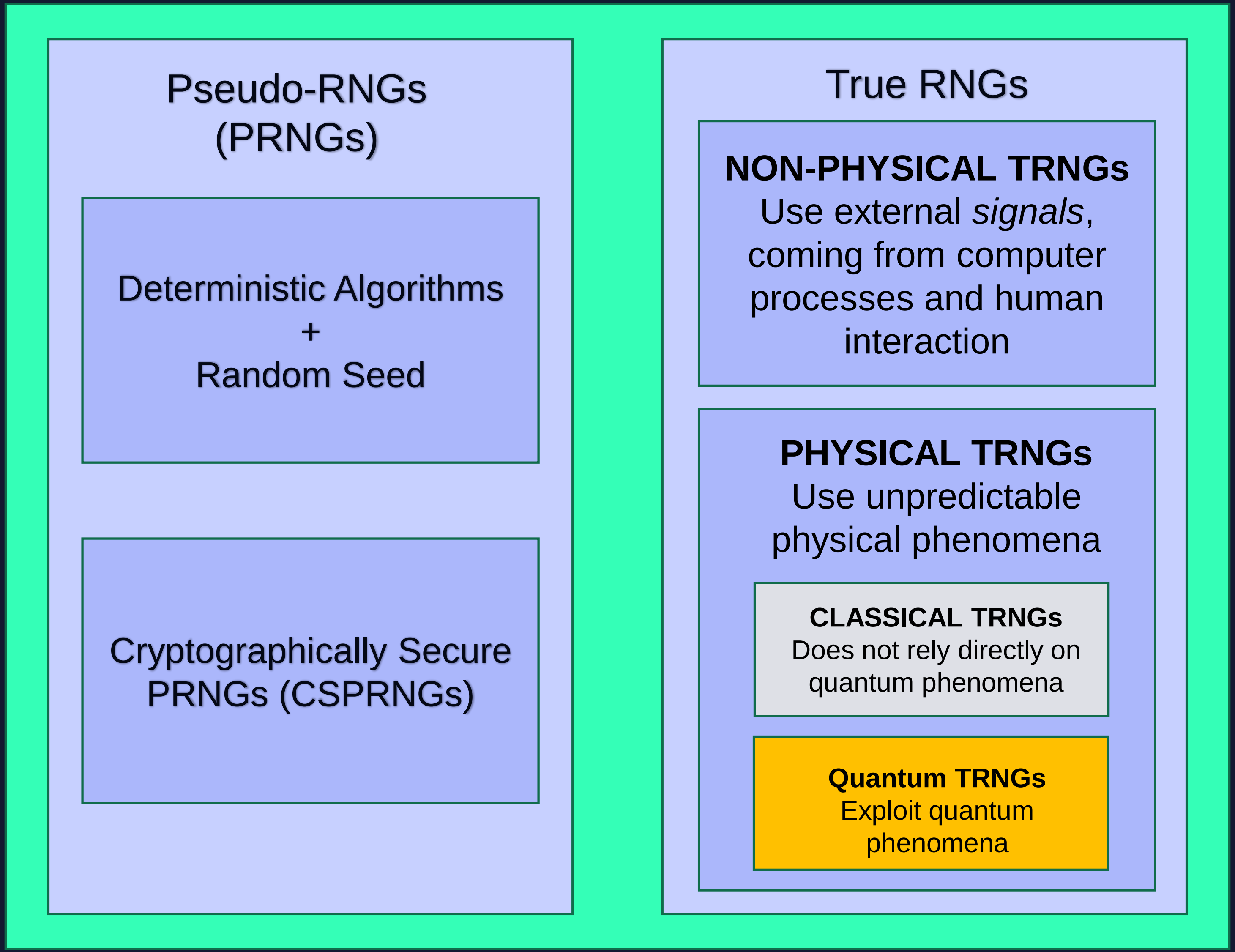
Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 3 min read

No randomness, no security

No Information superiority

Randomness Generation



Pseudo-RNGs (PRNGs)

Deterministic Algorithms
+
Random Seed

Cryptographically Secure PRNGs (CSPRNGs)

True RNGs

NON-PHYSICAL TRNGs
Use external *signals*, coming from computer processes and human interaction

PHYSICAL TRNGs
Use unpredictable physical phenomena

CLASSICAL TRNGs
Does not rely directly on quantum phenomena

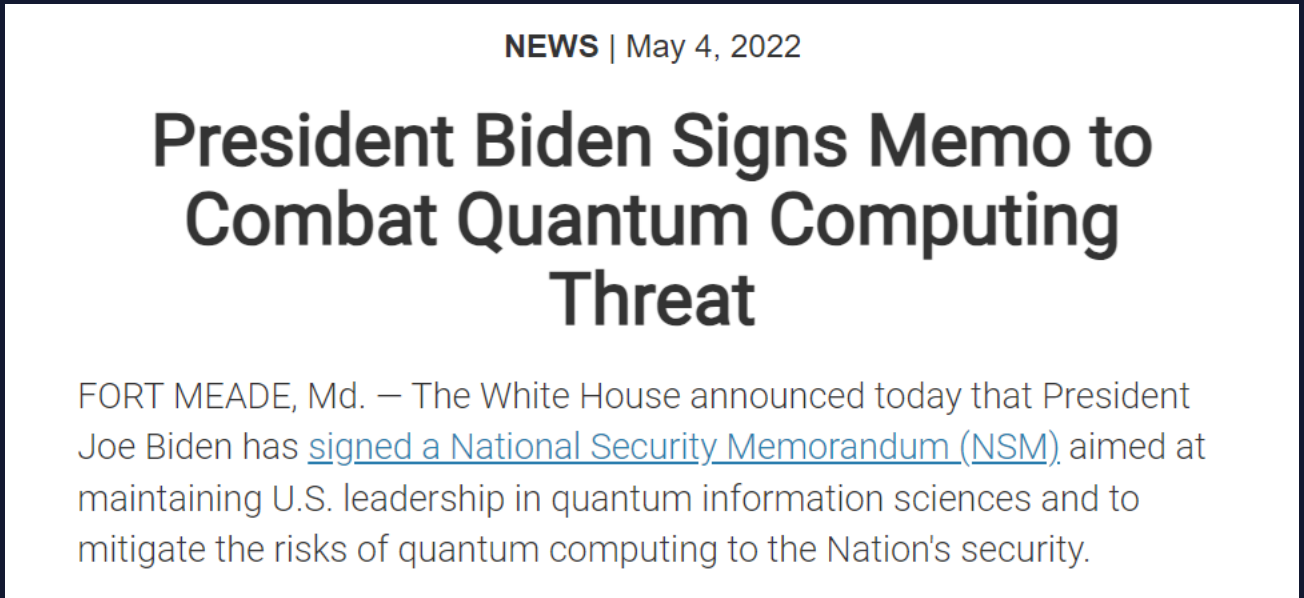
Quantum TRNGs
Exploit quantum phenomena

The perfect timing

A confluence of technology maturity & market need

/ Cryptography

The evolution to quantum-resistant cryptography has started.



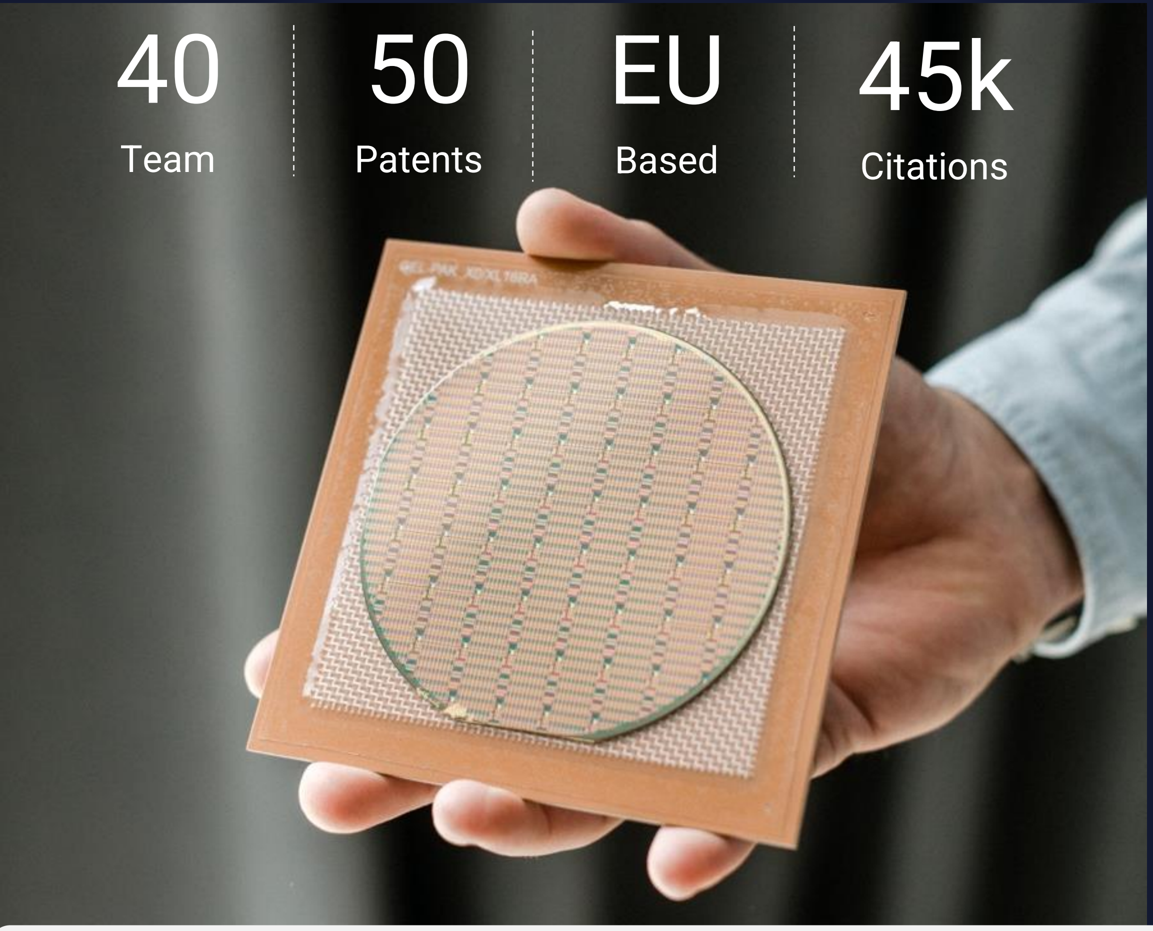
NEWS | May 4, 2022

President Biden Signs Memo to Combat Quantum Computing Threat

FORT MEADE, Md. — The White House announced today that President Joe Biden has signed a National Security Memorandum (NSM) aimed at maintaining U.S. leadership in quantum information sciences and to mitigate the risks of quantum computing to the Nation's security.

About Quside

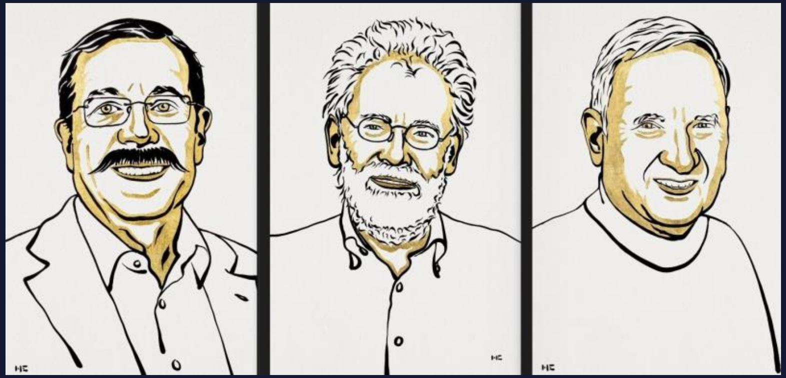
An ICFO spin-off



40	50	EU	45k
Team	Patents	Based	Citations

10+ years inventing and delivering the most advanced randomness technologies.

The experiments of the Nobel Prize in Physics in 2022 used Quside's technology



Telefónica Tech · ThalesAlenia Space · JUNIPer NETWORKS · EY · Qrypt · European Commission

World leading customers and partners

/ Data center

Telefónica Tech

Delivering Entropy-as-a-Service within Telefonica’s Virtual Data Center

/ Space

ThalesAlenia Space

a Thales / Leonardo company

Engineering a high-rate QRNG for secure space connectivity missions

/ Finance

CaixaBank

Accelerating Monte Carlo simulations for risk and pricing methods

/ By technology

Cryptography

Monte Carlo Simulations

Heuristic optimizations

/ By use case

Synthetic data generation

Risk analytics

Post quantum crypto evolution

/ Quside benefits

No entropy starvation

Monitored quality

Workload acceleration

Products and solutions

Security. Performance. Efficiency. Trust.

QRNG / Quantum random number generators

High-quality, fast entropy sources that can be **checked**; from chips to racks. **Enjoy a lifetime of security.**

RPU / Randomness Processing Units

Quantum randomness, hardware-level acceleration & reprogrammability. **Better decisions, made faster.**

aws marketplace

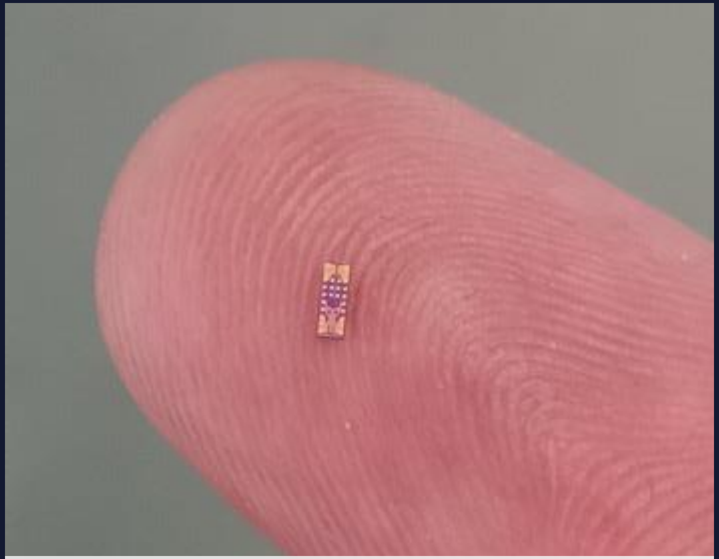
Solutions / End user solutions for on-prem and cloud environments

Together with a network of world-leading partners, we offer bundled solutions in cryptography & compute.

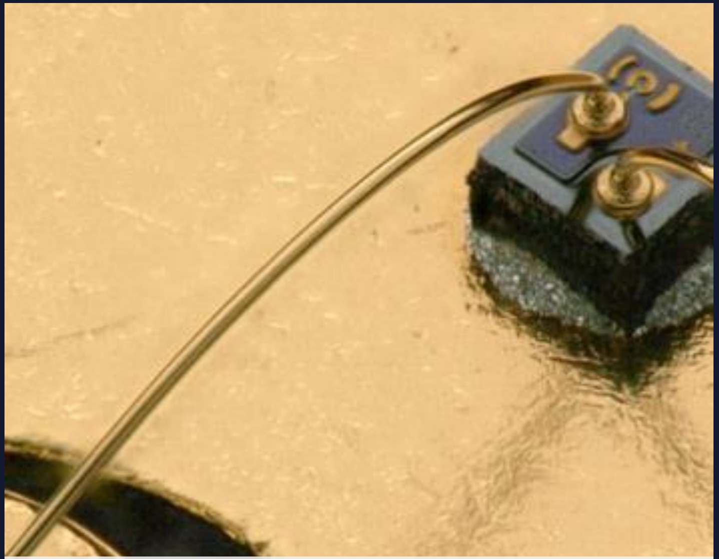
Also available in the AWS marketplace for non-cryptographic workloads

Core technology

Photonic inside, electronic outside.



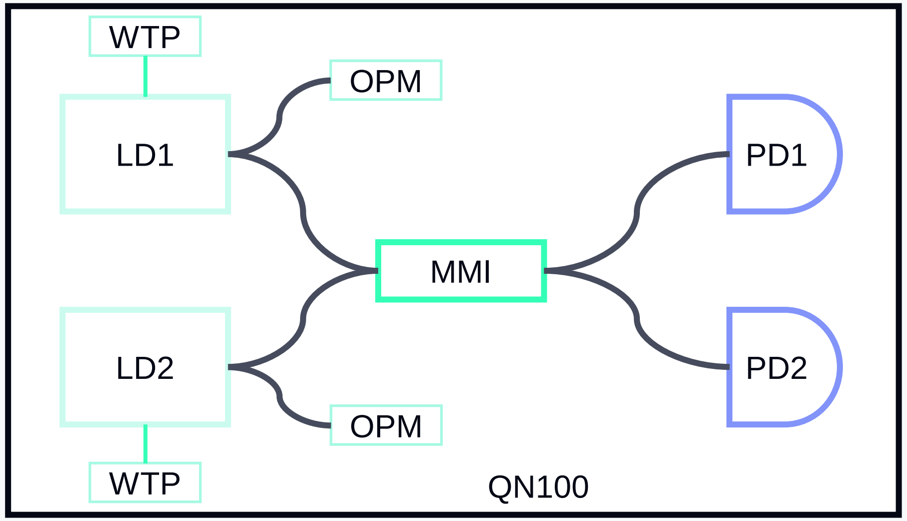
QN 100
The high-performance solution
Gain switching / Phase
Wafer-level capability
Gb/s +



QV 100
The low complexity solution
Gain switching / Polarization
First customers signed
~50 Mb/s

QN100 - Accelerated Phase Diffusion Scheme

A 2-laser scheme to get into a single chip

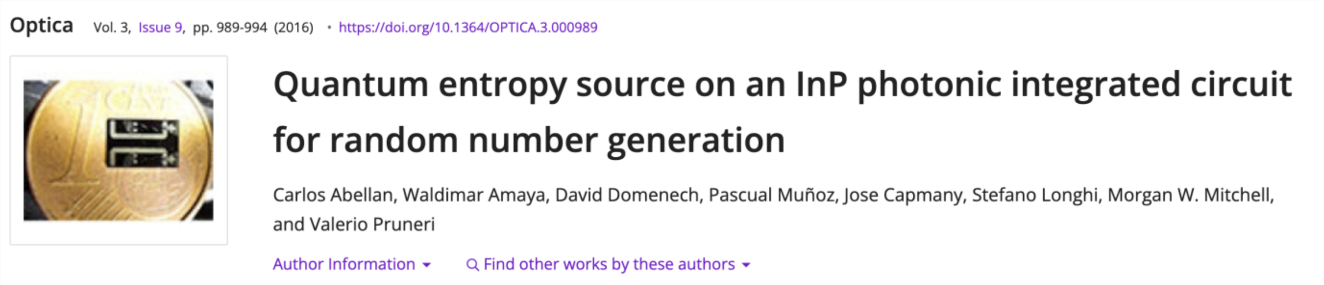


$$i_{PD}(t) = i_{L1}(t) + i_{L2}(t) + 2\sqrt{i_{L1}(t)i_{L2}(t)}\cos(\Omega_b t + \Delta\theta)$$

$$\Omega_b(\mathrm{t}) = \omega_1(t) - \omega_2(t)$$

Tunable

Quantum random phase

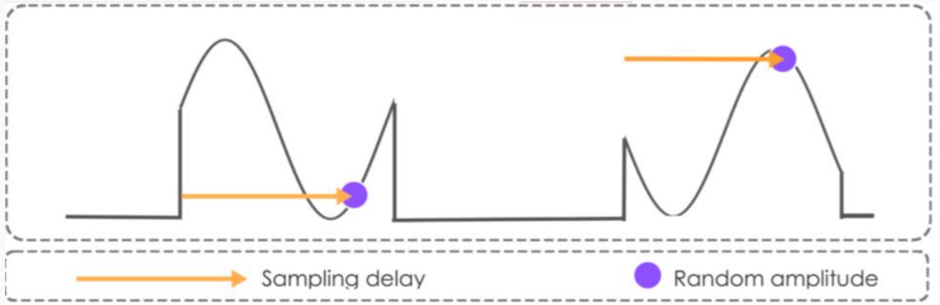


Optica Vol. 3, Issue 9, pp. 989-994 (2016) • https://doi.org/10.1364/OPTICA.3.000989

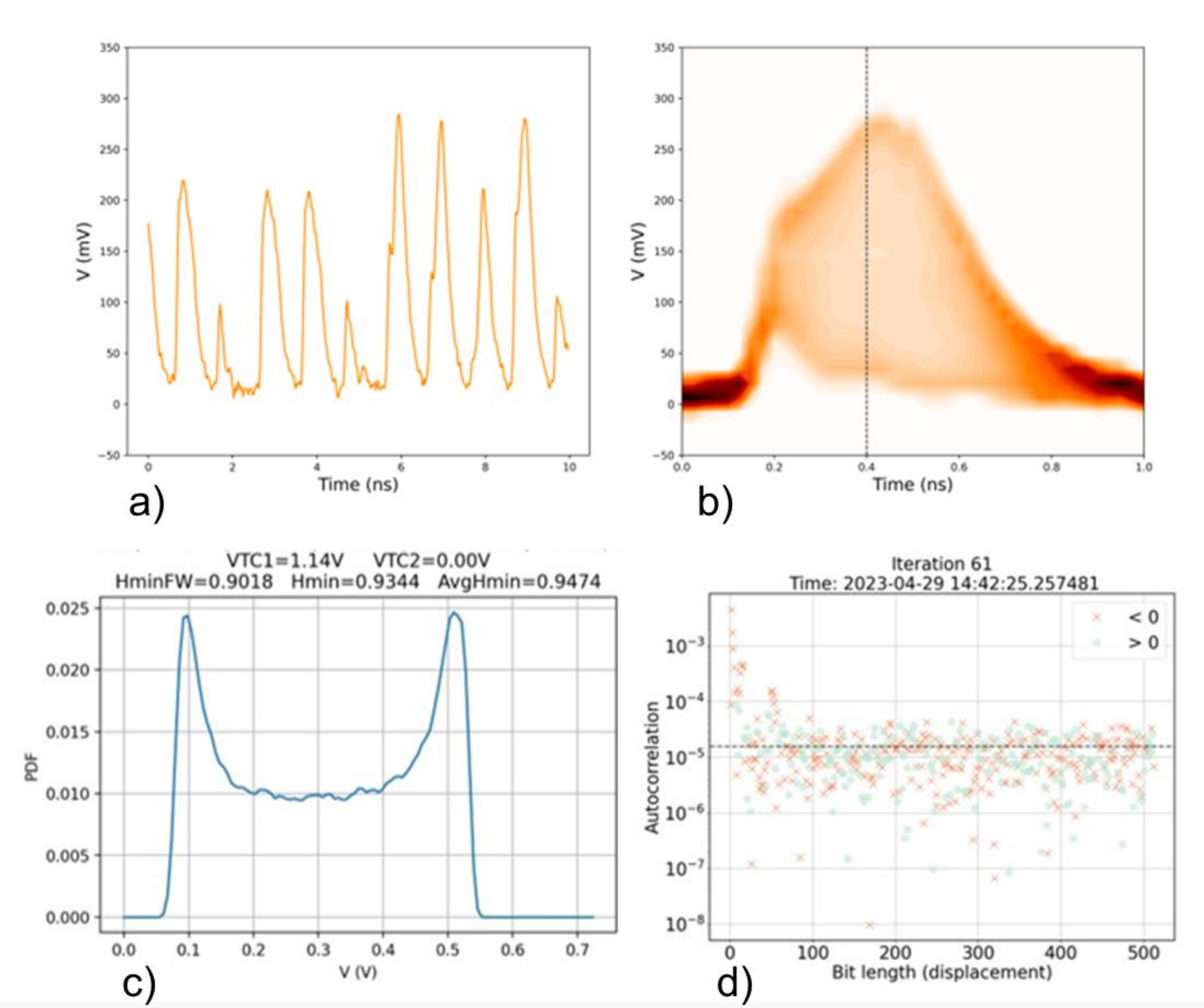
Quantum entropy source on an InP photonic integrated circuit for random number generation

Carlos Abellan, Waldimar Amaya, David Domenech, Pascual Muñoz, Jose Capmany, Stefano Longhi, Morgan W. Mitchell, and Valerio Pruneri

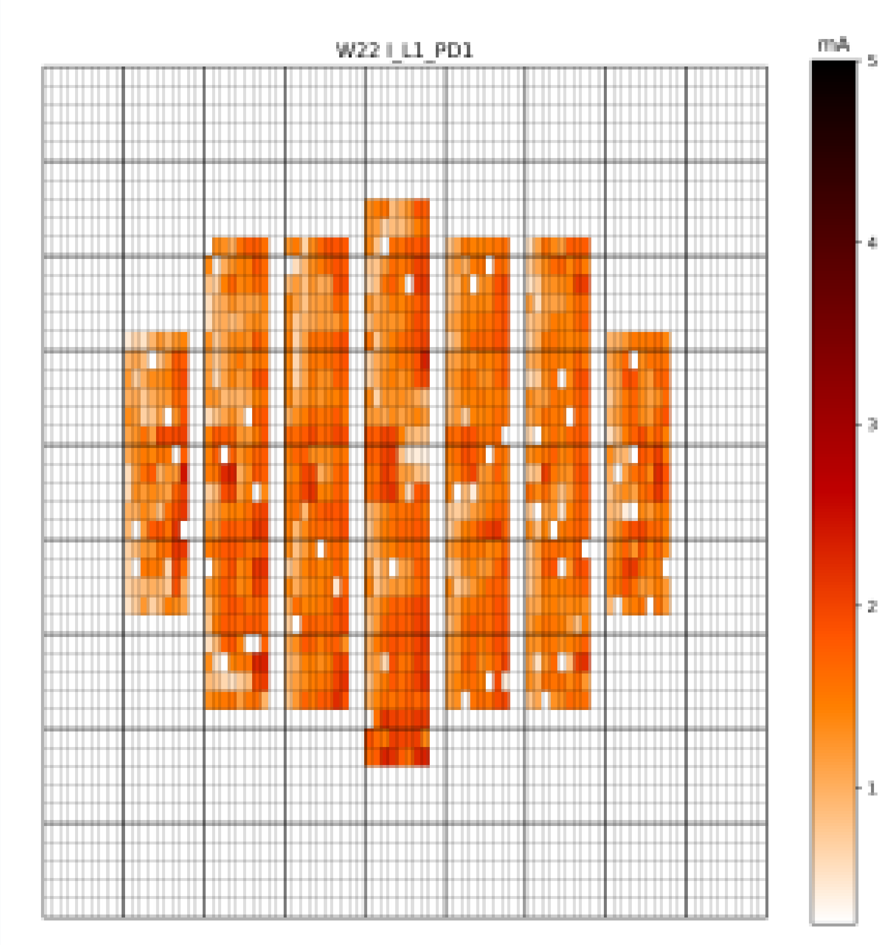
Author Information ▾ Find other works by these authors ▾



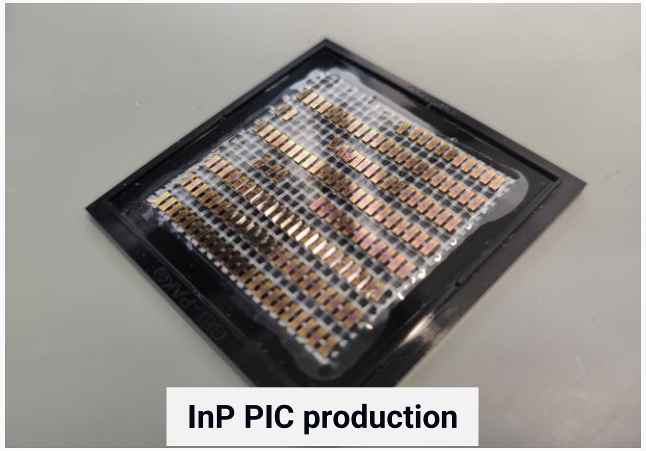
QN100 - Accelerated Phase Diffusion Scheme



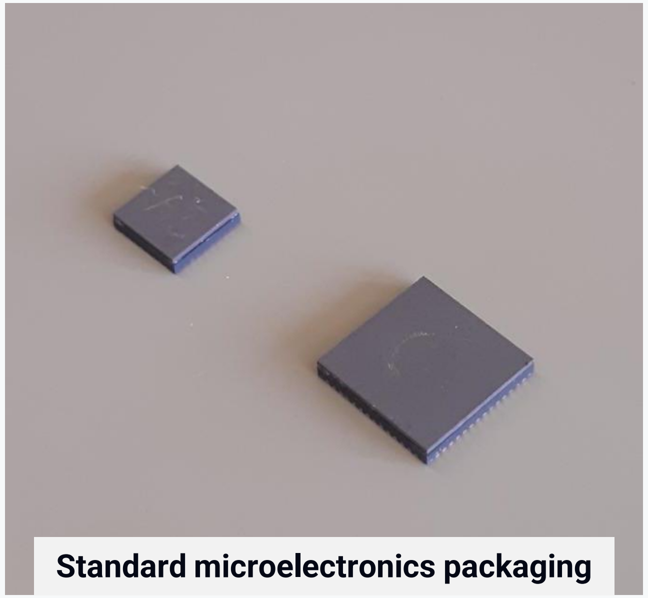
Scalable Processing



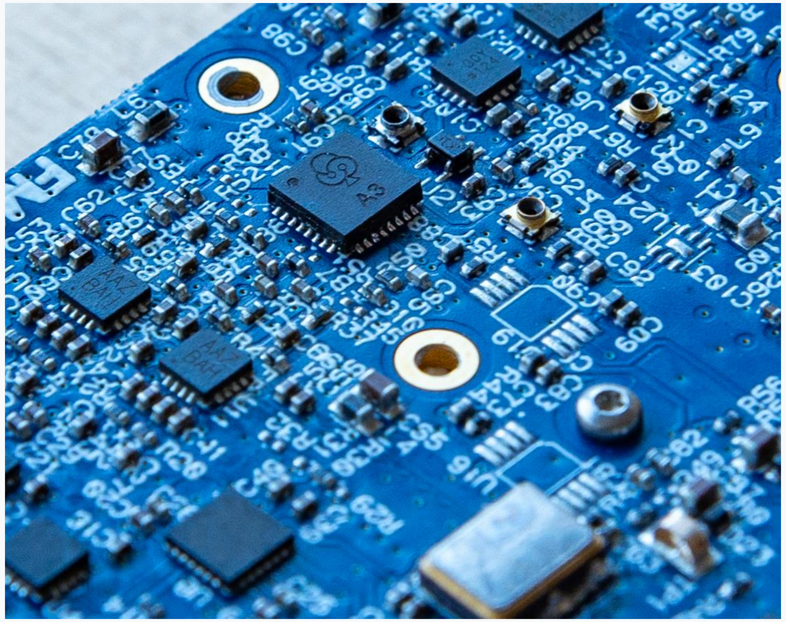
Wafer Level Testing



InP PIC production



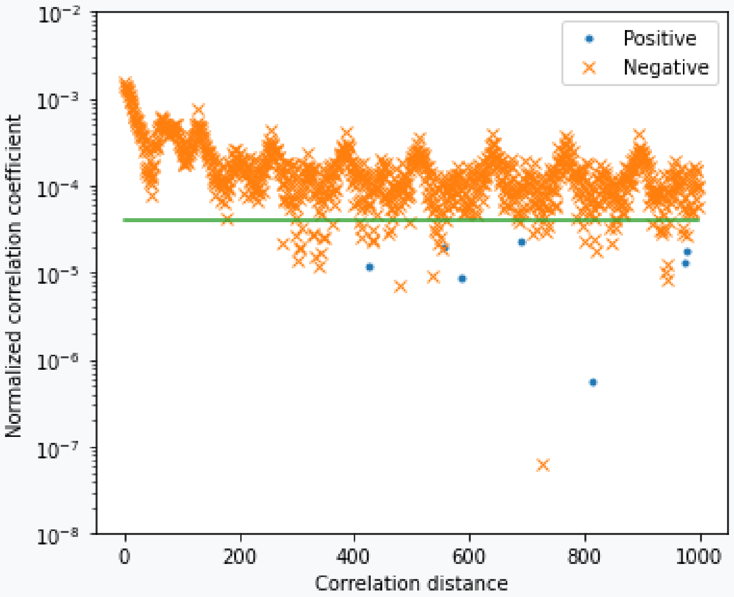
Standard microelectronics packaging



FMC-One

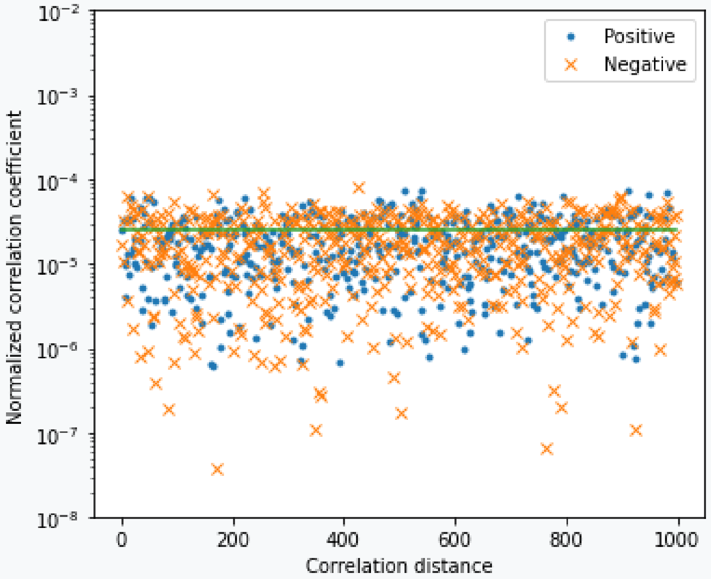
Use case examples: enhancing entropy generation

Using OS entropy sources only



- Statistically significant defects
- 6+ days to collect data

Using Quside quantum entropy



- Eliminated statistical defects
- 2 seconds to collect data **(+500.000X)**

Quside unveils **the world's first Randomness Processing Unit**

What's an RPU?

The RPU is a new hardware acceleration card for a richer heterogeneous compute landscape, providing faster performance lower energy consumption for intensive randomized workloads. A new addition for highly optimized servers.

(Link to video)

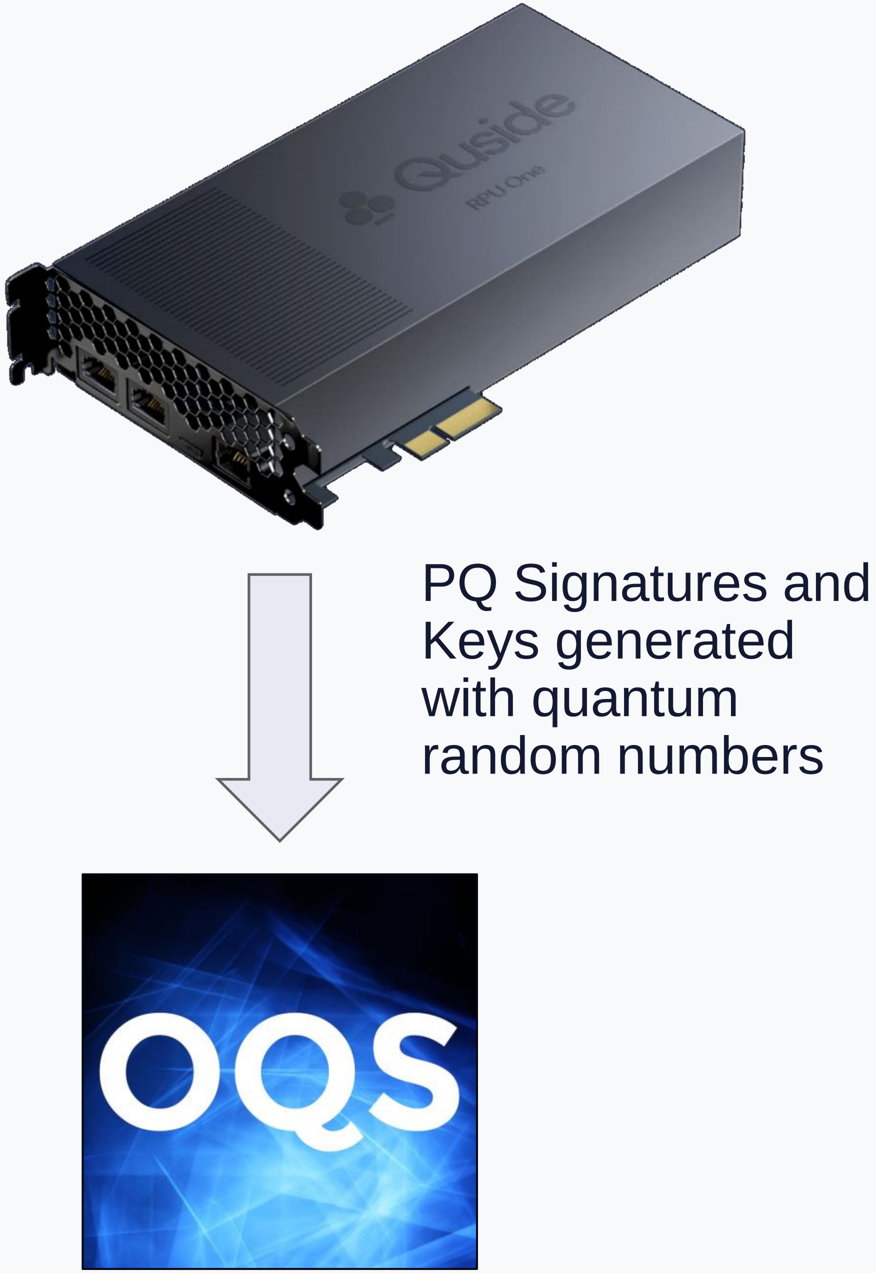
Award-winning technology

Quside wins the EUSPA myEUspace competition *with their hardware acceleration to empower randomness-intensive algorithms for route optimization.*

EUSPA European Union Agency for the Space Programme

RPU integration in libOQS

- Development of PQC algorthims with quantum safe keys.
- Extra security layer to the transition to a quantum-safe cryptography.



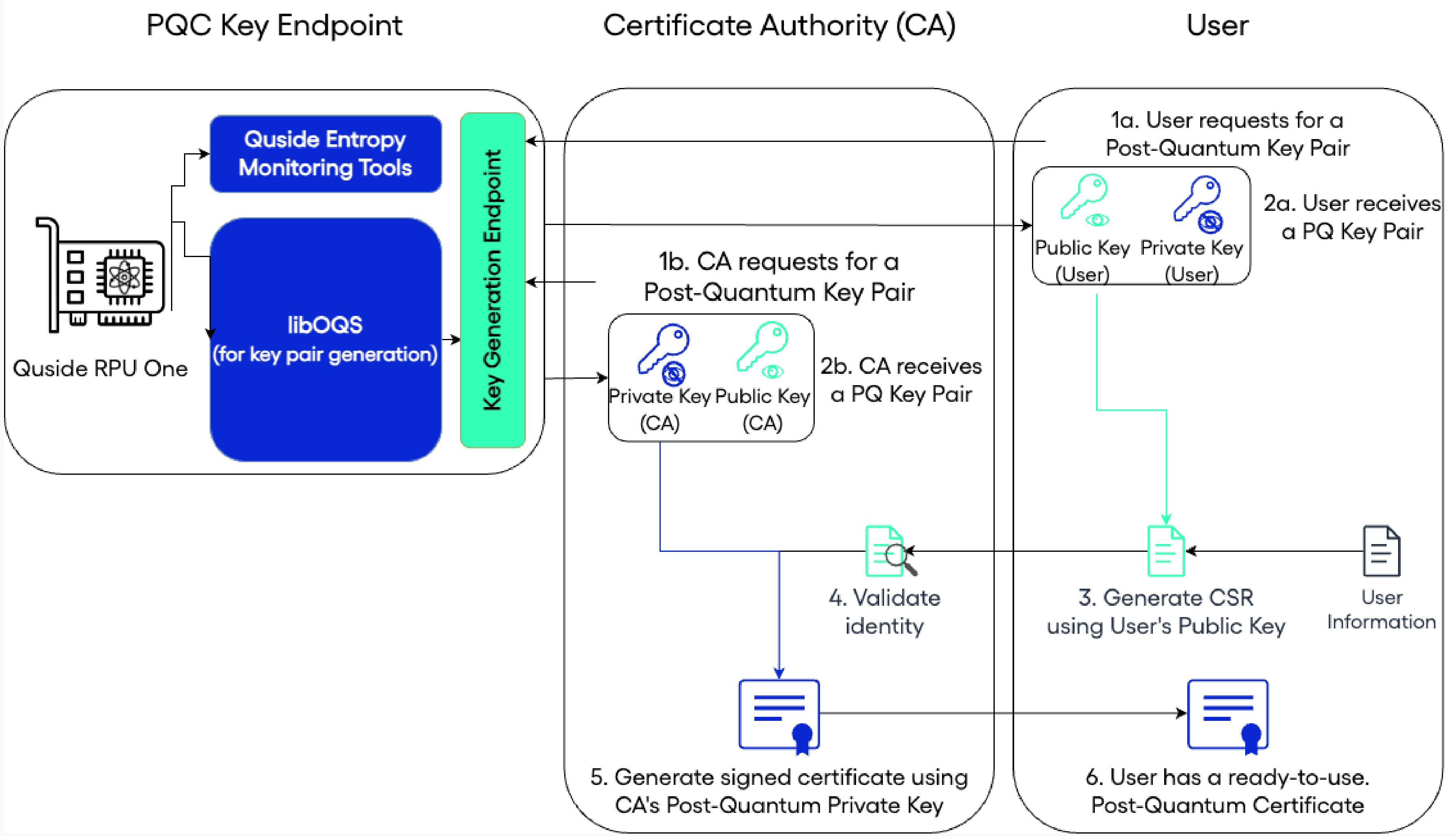
PQ Signatures and Keys generated with quantum random numbers

libOQS is a software library that provides a collection of quantum-resistant cryptographic algorithms.

Its main features are:

- **Open-source** library.
- Direct integration with cryptography libraries like OpenSSL and BoringSSL.
- Easy to integrate with network tools like OpenSSH, curl, Chromium, nginx, etc.
- Strongly aligned with **NIST PQC Standardization Process** including the recently published drafts.

Envisioned Architecture

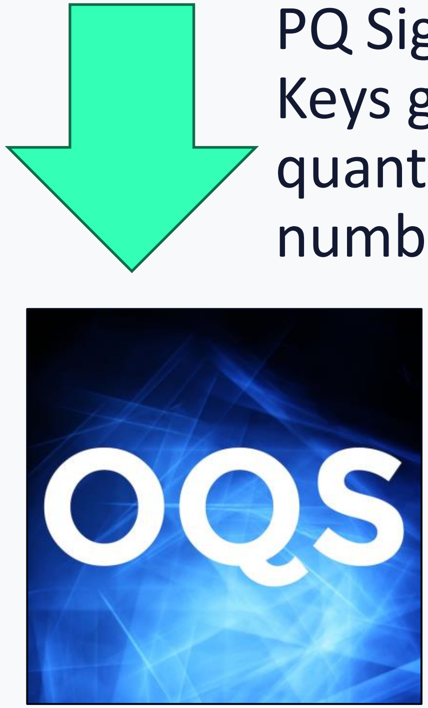

PQC Key Endpoint
Certificate Authority (CA)
User
Quside Entropy Monitoring Tools
libOQS
(for key pair generation)
Key Generation Endpoint
Quside RPU One
1a. User requests for a Post-Quantum Key Pair
Public Key (User)
Private Key (User)
2a. User receives a PQ Key Pair
1b. CA requests for a Post-Quantum Key Pair
Private Key (CA)
Public Key (CA)
2b. CA receives a PQ Key Pair
4. Validate identity
3. Generate CSR using User's Public Key
User Information
5. Generate signed certificate using CA's Post-Quantum Private Key
6. User has a ready-to-use. Post-Quantum Certificate

Next steps

- The **RPU platform**, allows to get fast and safe random numbers.
- Designed to allow customers to offload their randomness workloads, including cryptographic primitives.

- The **offloading of post-quantum primitives** is in the roadmap for the development of this product.

- This would **improve the performance of libOQS** which would have a huge positive impact on the final product that relies on this library.



PQ Signatures and Keys generated with quantum random numbers

Take-home Message

Why QRNGs?

- Random numbers are at the foundational base of any crypto system.
- In the absence of truly random numbers, any cryptographic software is vulnerable to attacks.
- **QRNGs** guarantee that the quantum realm is where your numbers are coming from.

Why now?

- The market is transitioning to a new type of cryptography with high quality entropy demands
- **Now** is the time to embed the strongest cryptographic foundation to cope with the current and future requirements of it.
- QRNGs are **interoperable** devices which can be already integrated.

Why Quside?

- +10 years building QRNG technology.
  - tested in the most demanding scenarios including experiments that lead to the 2022 Nobel prize winning
  - peer reviewed in the most exigent scientific publications.
- Advanced, ready to deploy in production, randomness solutions.
- **Quside** products provide measurable quality, high-speed entropy in a scalable way

hello@quside.com

www.quside.com

C/Esteve Terradas 1, Of. 304
08860 Castelldefels
Barcelona, Spain

Quside