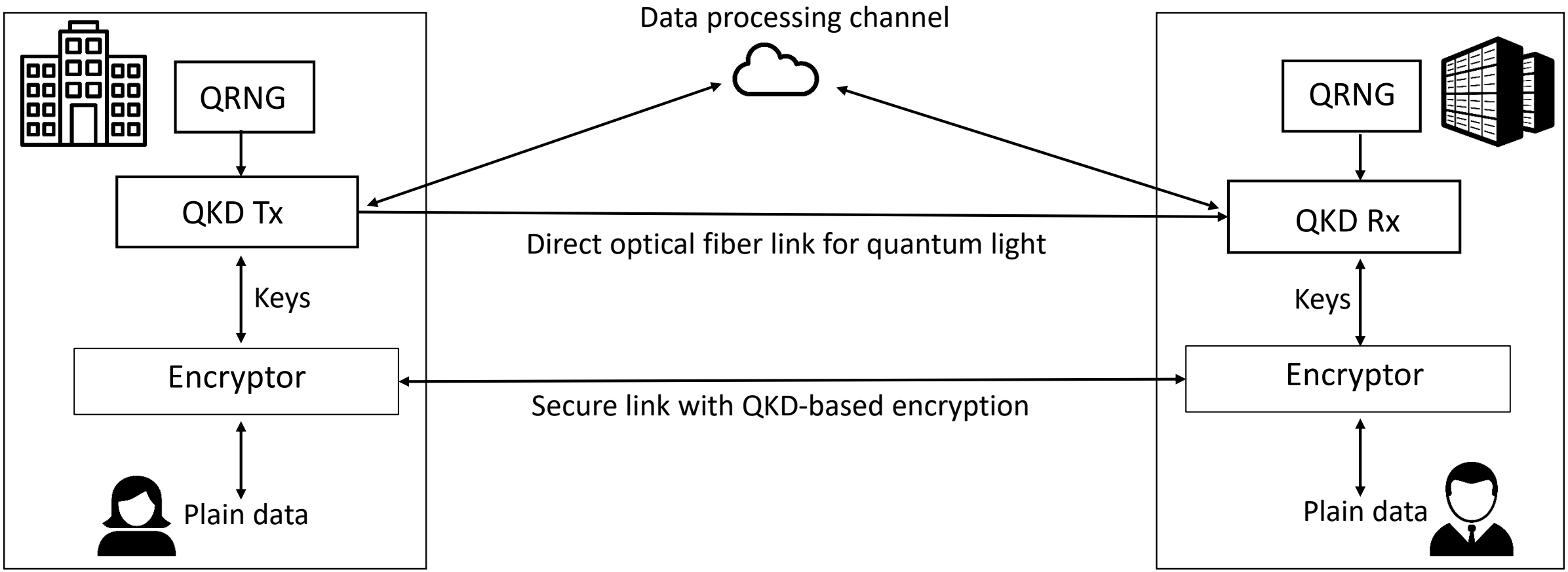
QRNG and QKD using classical hardware

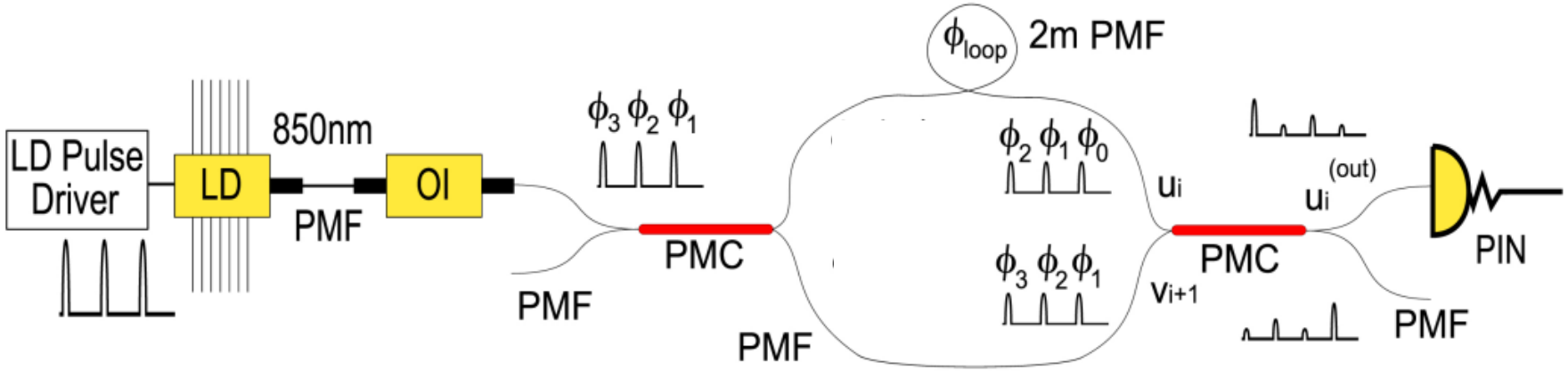
Valerio Pruneri

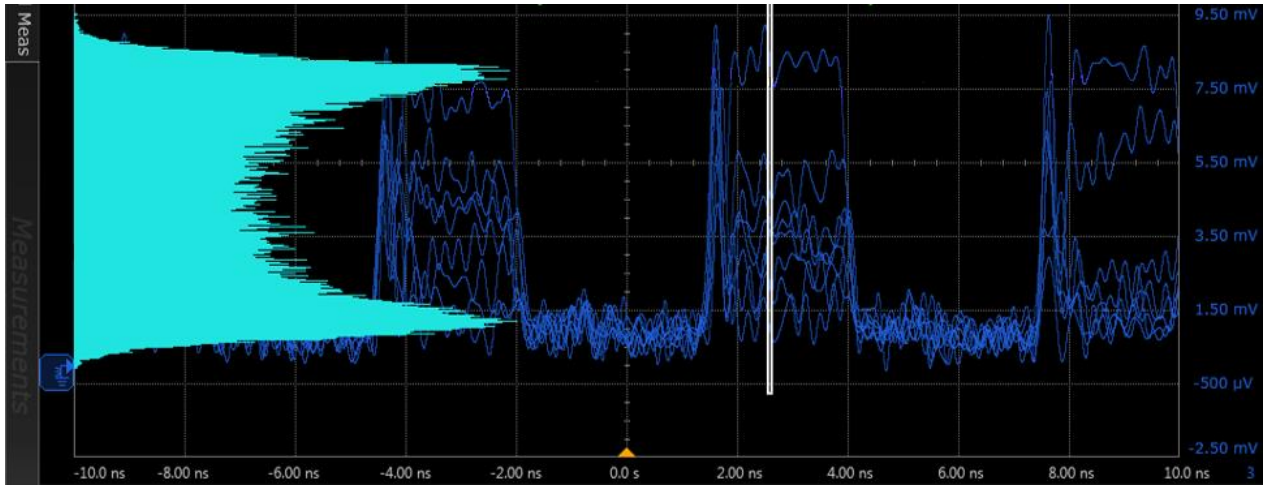
valerio.pruneri@icfo.eu

QRNG and QKD in cybersecurity

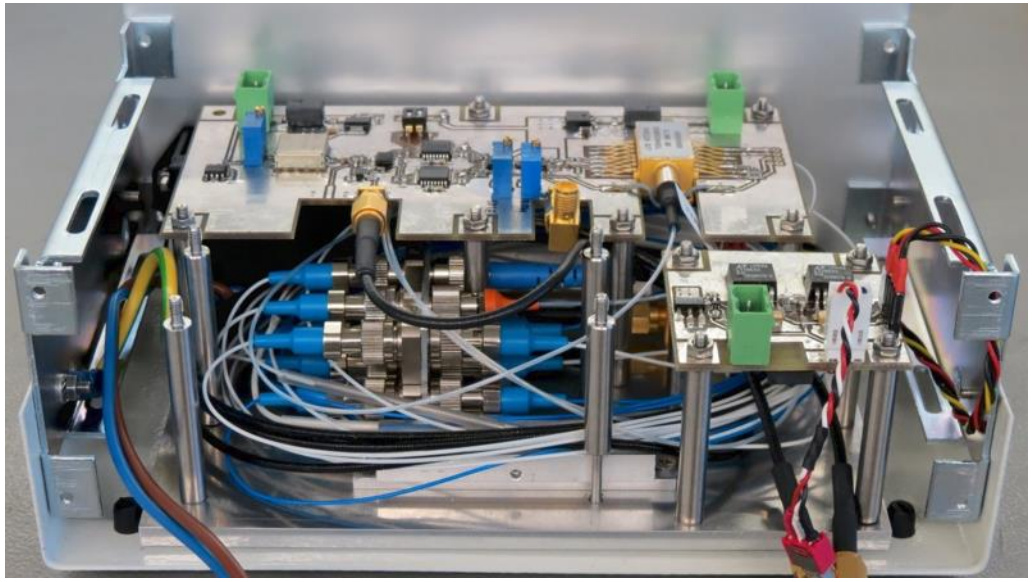


QRNG via phase diffusion of a laser

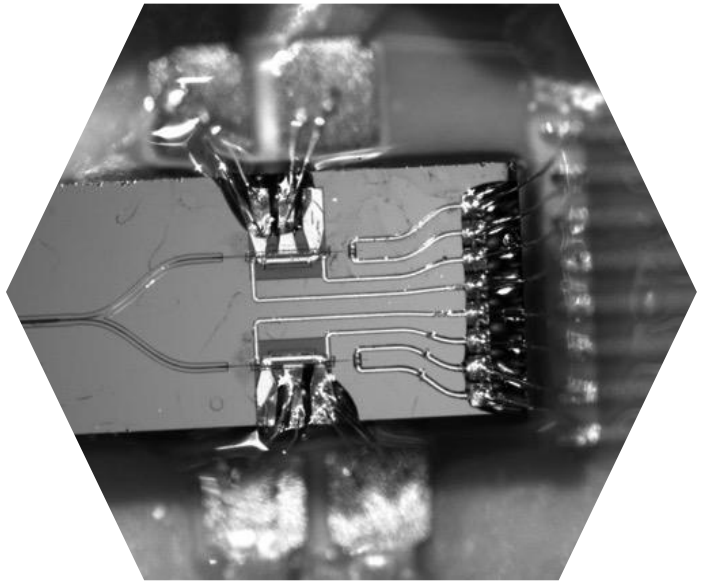




QRNG: from discrete to PIC

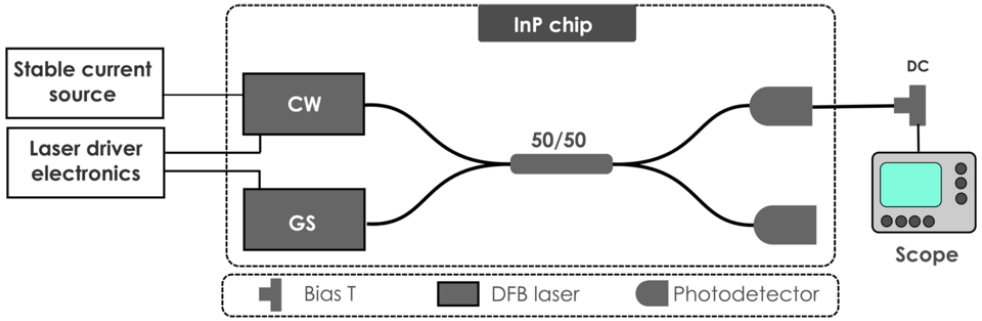


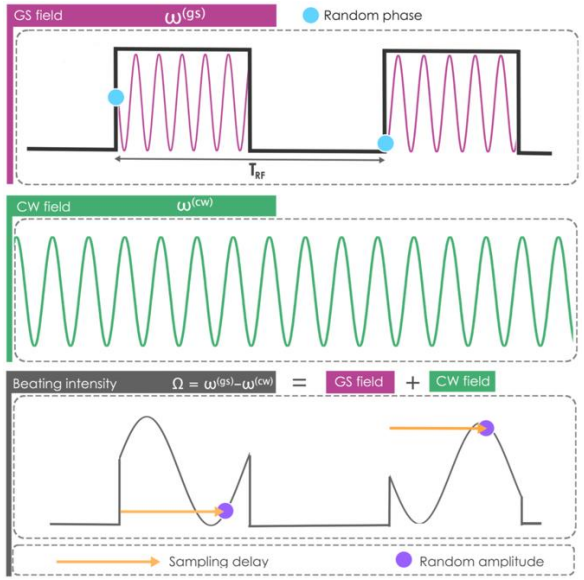
2015 loophole free Bell test experiments

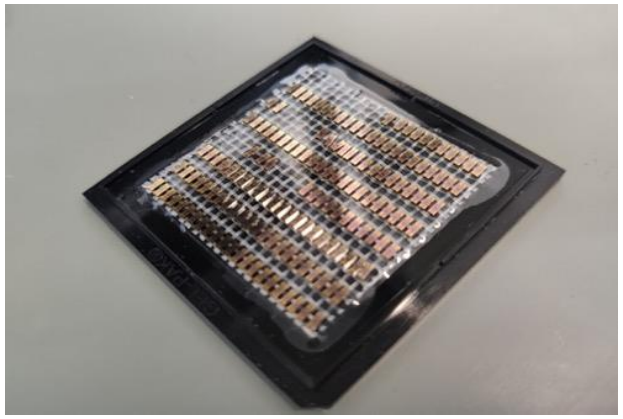


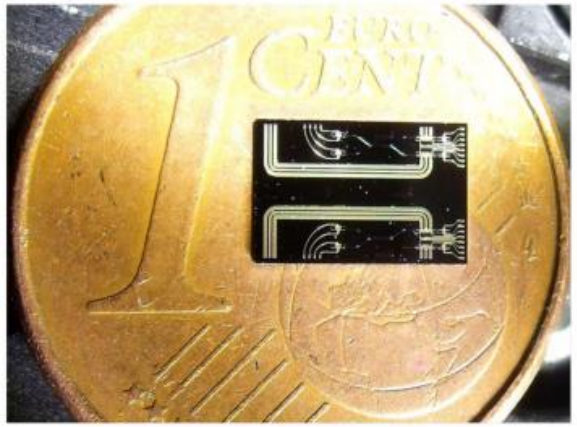
SiP & InP during 2014 – 2016

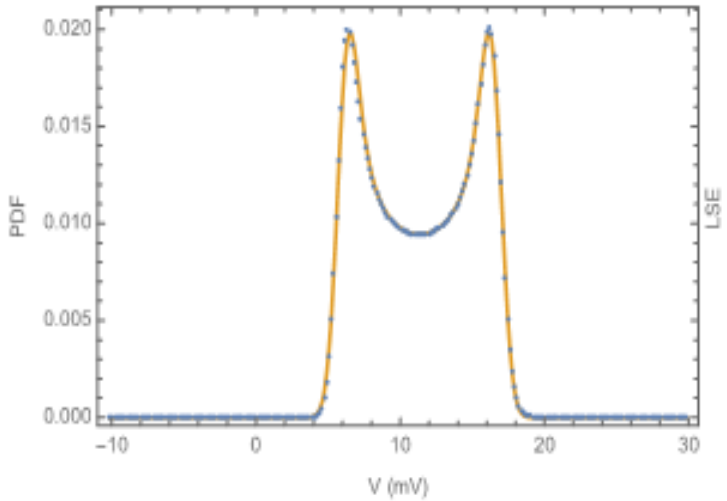
QRNG – PIC


InP chip
Stable current source
Laser driver electronics
CW
GS
50/50
DC
Scope
Bias T
DFB laser
Photodetector


GS field
ω(gs)
Random phase
T_RF
CW field
ω(cw)
Beating intensity
Ω = ω(gs)−ω(cw)
=
GS field
+
CW field
Sampling delay
Random amplitude






0.020
0.015
0.010
0.005
0.000
PDF
LSE
−10
0
10
20
30
V (mV)

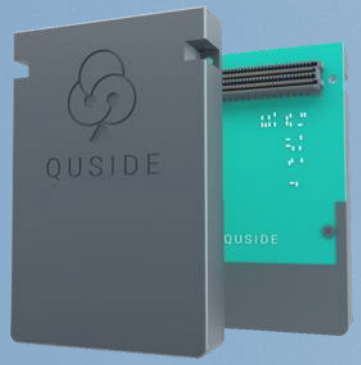
QRNG: Products

Quside™ Randomness **Generation & Processing**

QRNG / Chipsets / QN 100

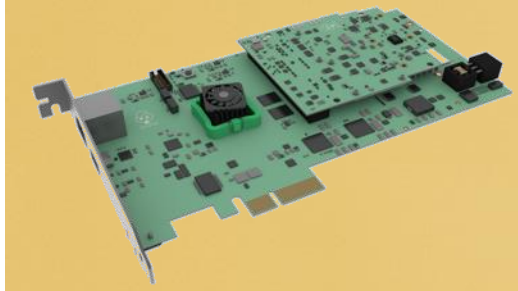
Quside™ unique QN 100 chipset is a fully integrated quantum entropy source enabling ultrafast performances and form factors.

QRNG / Embedded / FMC 400



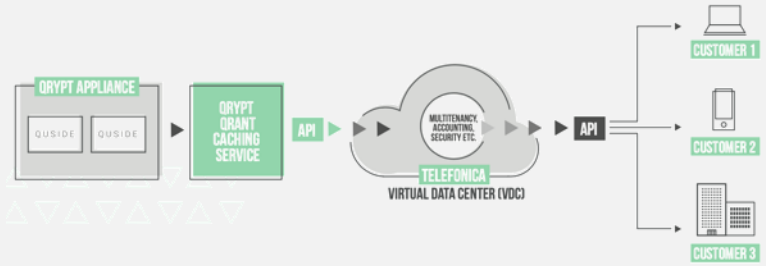
The Quside™ FMC 400 product is available for shipping today and available with advanced Randomness Metrology™.

Compute / Launch in 2023



Boost the performance of your randomized workloads by up to 10X and reduce energy consumption by up to 20X.

QRNG: Use cases

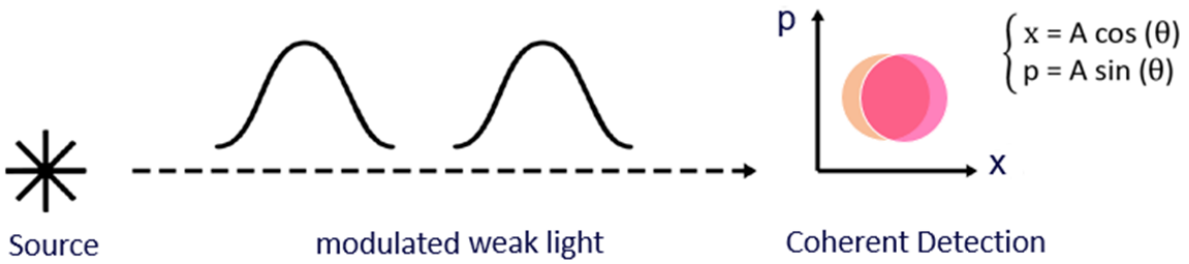
Telefónica Tech	LUXQUANTA	Qrypt
Delivering Entropy-as-a-Service within Telefonica's Virtual Data Center	**Continuous-variable quantum key distribution (QKD)**	**Unexploitable quantum-secure encryption services**
 **In a nutshell:** Validated multiple use cases and integration within Telefonica's infrastructure	• QRNGs are used to generate high-rate, randomized quantum states. • By distribution of quantum signals, LuxQuanta can detect an intruder. • LuxQuanta devices can be easily embedded in telecom networks.	• QRNGs are used to generate high-rate random streams for users. • Qrypt create identical keys at multiple endpoint enabled by quantum entropy. • As keys are never distributed, they can't be intercepted.

CV-QKD: principle

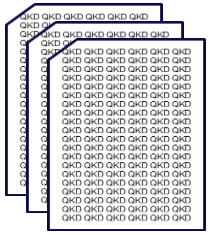
CV-QKD
(Continuous variable Quantum Key Distribution) **=** **Telecom technology + quantum security proofs**

$$A\sin(\omega t+\theta) = \underbrace{A\cos(\theta)}_{x}\sin(\omega t) + \underbrace{A\sin(\theta)}_{p}\cos(\omega t)$$

x and p are non-commuting observables



+



- Quantum-security proofs
- Shot-noise limited operation
- Digital signal processing (DSP) adapted to quantum security proofs
- …

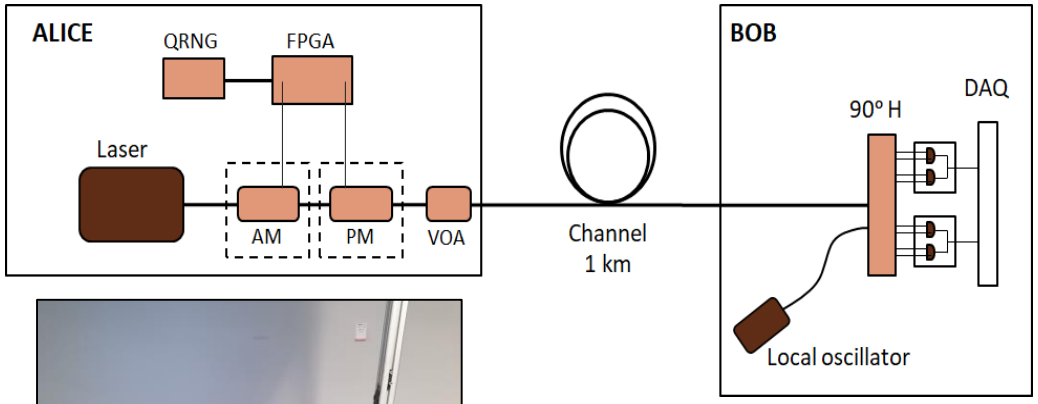
Uses coherent pulses and coherent detection

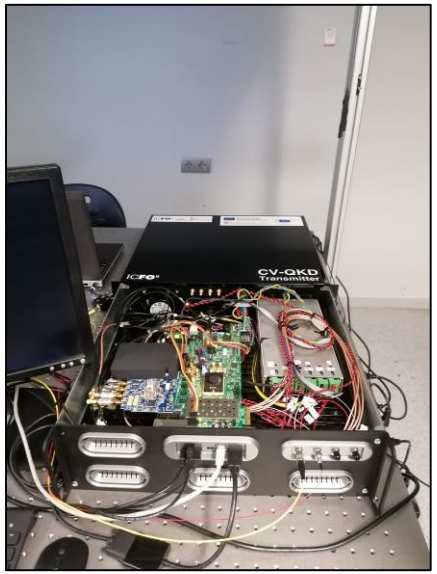
No need of single-photon technology

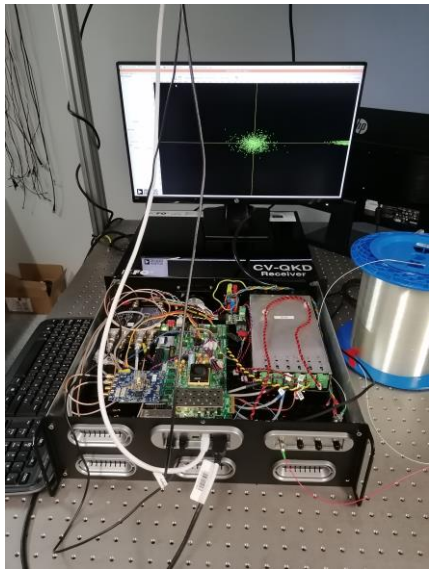
Chip-level integration

Compatible with modern optical telecommunication

CV-QKD: GG02 protocol and hardware





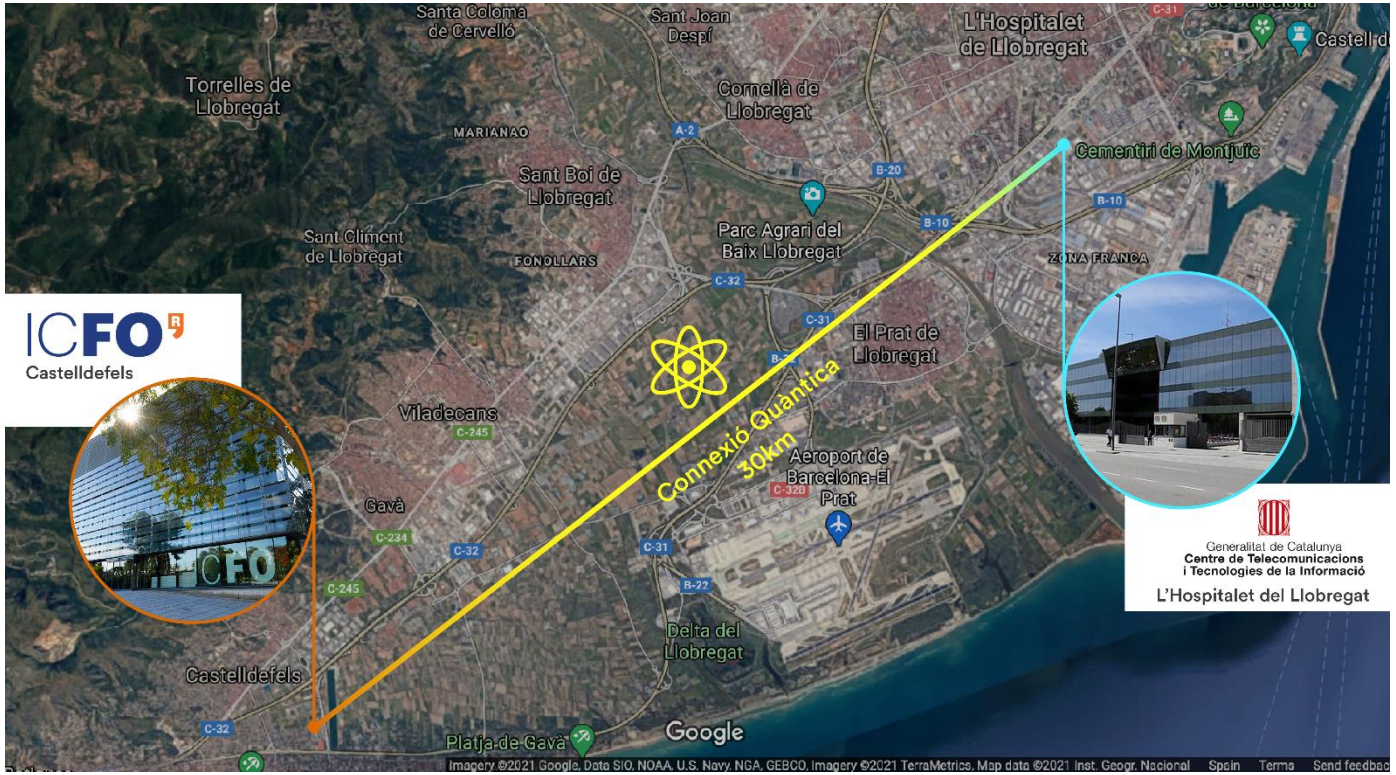


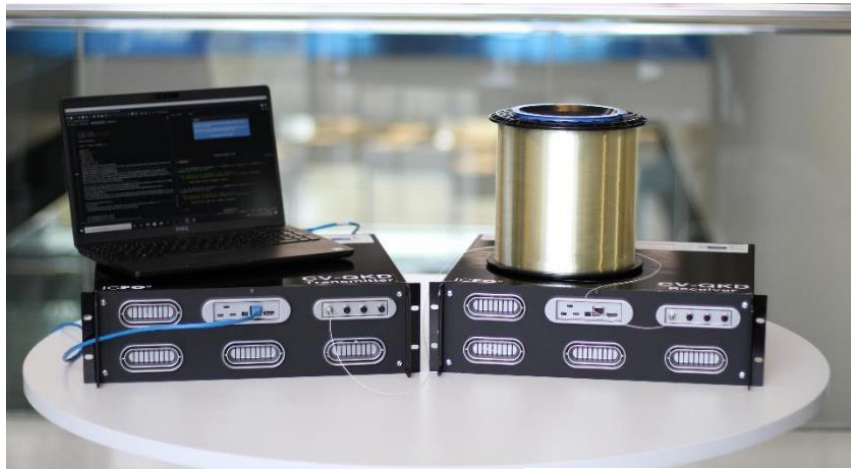
- Alice sends Bob coherent states with Gaussian modulated quadratures.
- Bob measures them by shot-noise limited homodyne or heterodyne detection
- Alice and Bob share **Gaussian correlated data**

Public channel

Noise estimation	Key reconciliation
Detecting intruder	Error correction, privacy amplification

CV-QKD: use case





LUXQUANTA

cellnex driving telecom connectivity

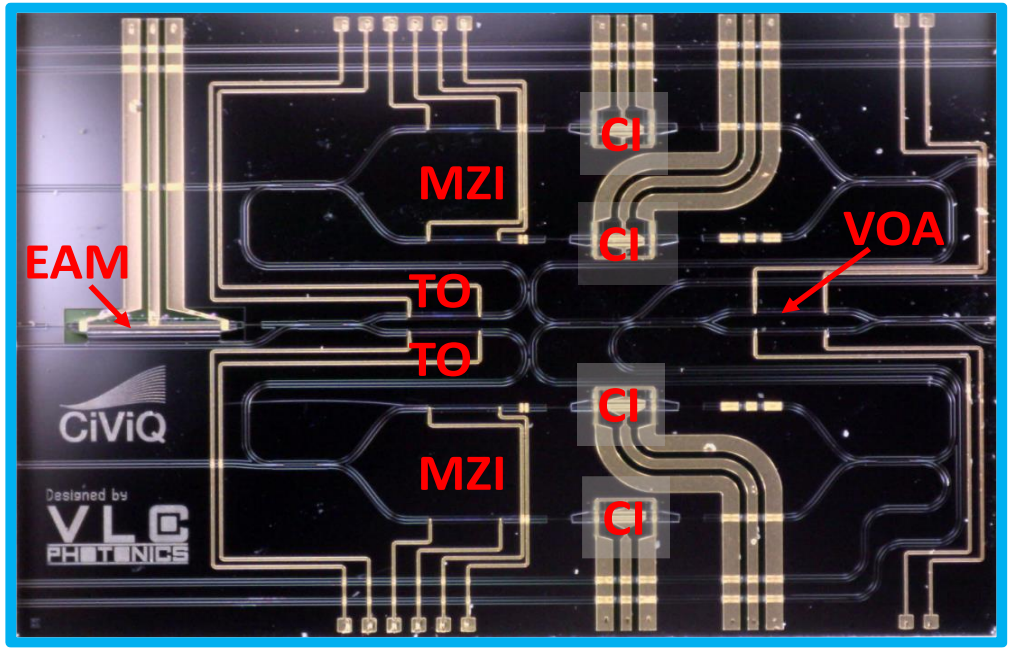
Secure teleconference

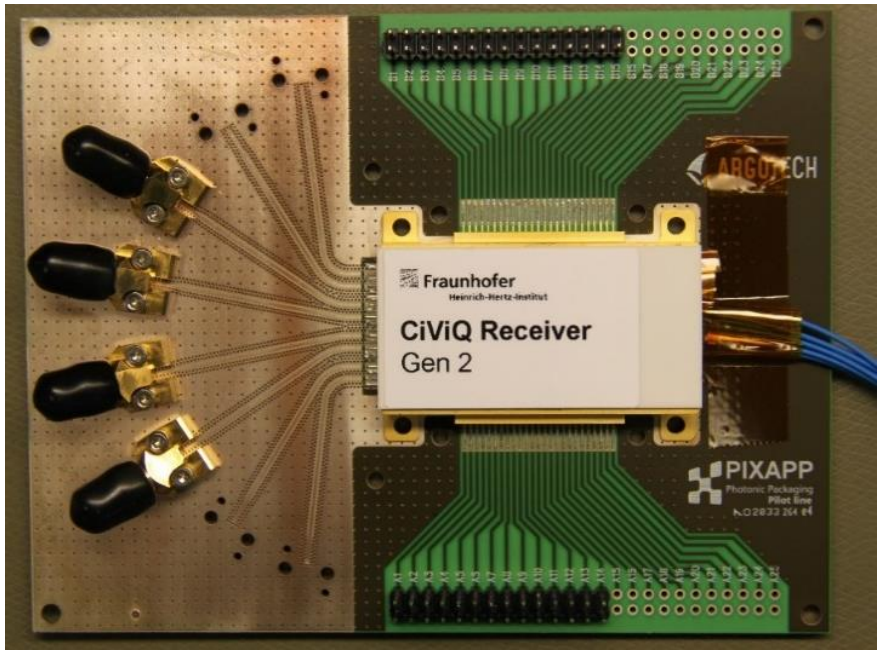
SmartCatalonia

OPEN QKD

CiViQ

QKD in InP-PIC





VLC, HHI, CNRS, ICFO, MPL

The technology team

Quantum part of OptoGroup

QUSIDE

+ 6 new employees

LUXQUANTA