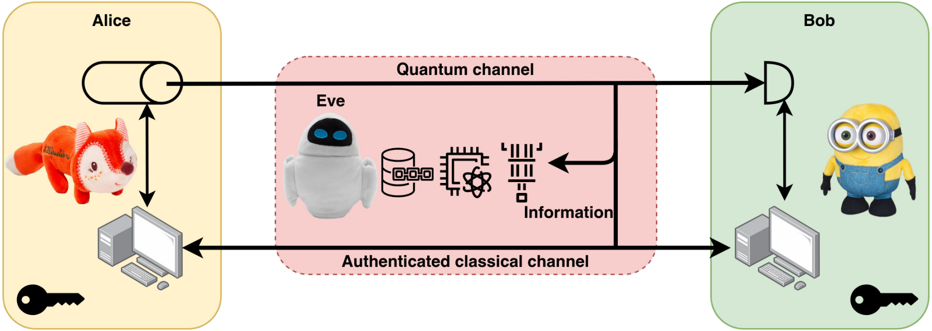
QOSST: Quantum Open Software for Secure Transmissions

A Highly Modular Open Source Platform for Continuous Variable Quantum Key Distribution Applications

Yoann Piétri

02/10/2024

Quantum Key Distribution (QKD)



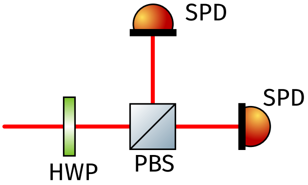
Alice, Bob: **trusted** users

Eve: **unbounded adversary**

Goal: exchange **cryptographic key** with **information-theoretic and long-term** security.

QKD does not directly encrypt the data. It has to be combined with an encryption mechanism (such as One-Time-Pad for instance).

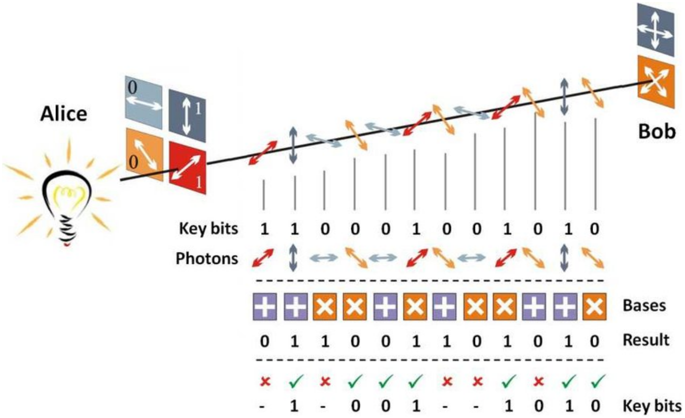
Conjugate bases



		HV $\|\leftrightarrow\rangle$	HV $\|\updownarrow\rangle$	DA $\|\nwarrow\!\!\searrow\rangle$	DA $\|\swarrow\!\!\nearrow\rangle$
HV	$\leftrightarrow$	1	0	1/2	1/2
	$\updownarrow$	0	1	1/2	1/2
DA	$\nwarrow\!\!\searrow$	1/2	1/2	1	0
	$\swarrow\!\!\nearrow$	1/2	1/2	0	1

Measuring a HV qubit in DA gives you no information $\Rightarrow$ HV and DA are conjugate bases.

BB84


Alice
0
1
0
1
Bob
Key bits 1 1 0 0 0 1 0 0 1 0 1 0
Photons
Bases
Result 0 1 1 0 0 1 1 0 1 0 1 0
Key bits - 1 - 0 0 1 - - 1 0 1 0

Secret key rate

Usual step of a QKD protocol:

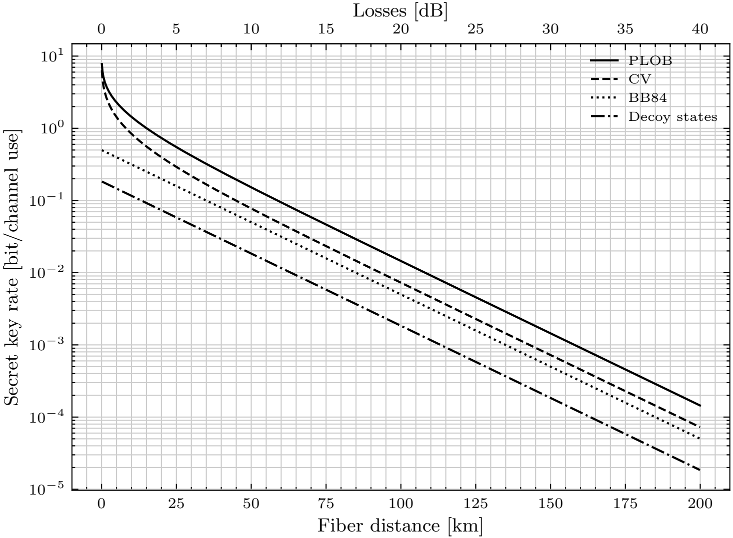
1. Quantum Information exchange;
2. Advantage distillation;
3. Parameter estimation;
4. Error correction
5. Privacy amplification.

Number of bits exchanged: n
Number of secret bits: l
Secret key rate $r = l/n$
Multiply by the rate to get the detection rate in bit/s.

General formula in the asymptotic case:

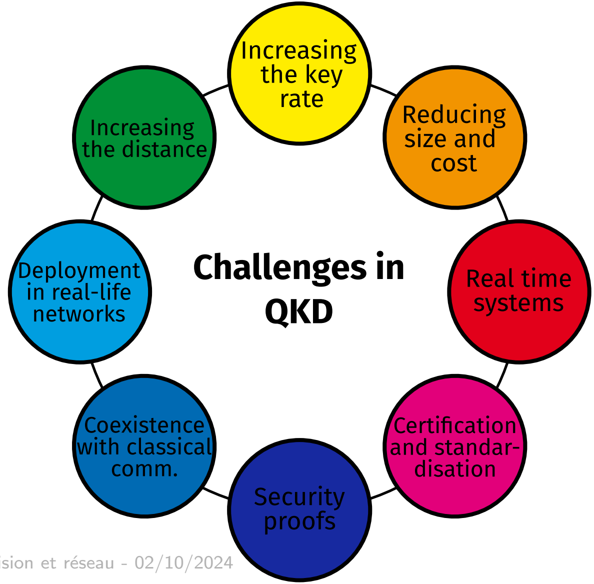
$$r = I_{AB} - I_E \tag{1}$$

The distance issue

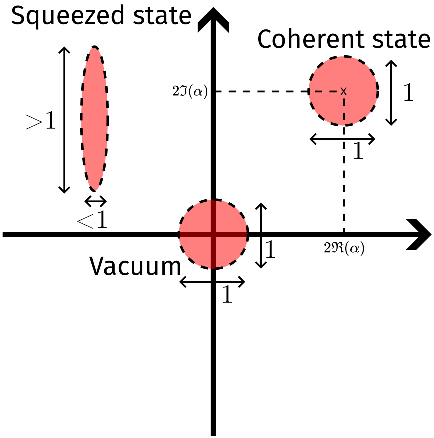


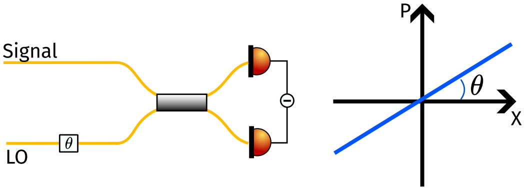
- Fundamental problem: exponential loss of photons in the fiber.
- Noise will also reduce the key rate.

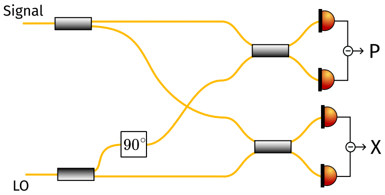
Challenges in QKD



Gaussian Quantum Information







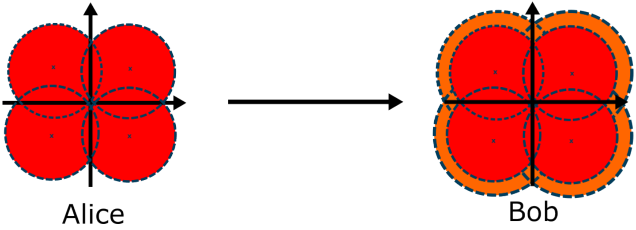
$$\Delta X \Delta P \geq 1$$

$\Rightarrow$ quadratures can encode quantum information.

$\Rightarrow$ conjugate variables.

CV-QKD: An intuition

Quadrature Phase Shift Keying (QPSK) modulation is used for representation purposes.



Uncertainty principle at Alice's side

Uncertainty principle at Bob's side

$$\Delta X \Delta P \geq \frac{\hbar}{2} = 1 \text{ SNU (Shot Noise Unit)}$$

$$\Delta X^2 = \Delta P^2 = \frac{\hbar}{2}$$

(coherent states: symmetric and reach minimal uncertainty).

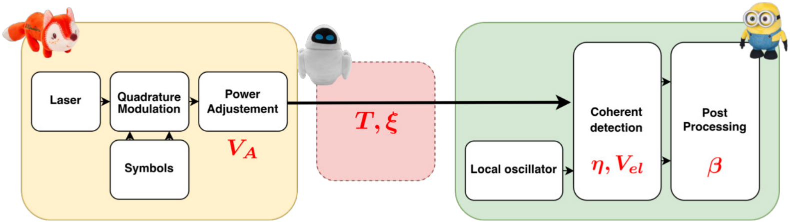
$$\Delta X^2 = \Delta P^2 = \frac{\hbar}{2}\left(1 + \frac{\xi}{2}\right)$$

ξ is called the excess noise and considers all the added noise in the transmission.

CV-QKD key rate

The excess noise ξ added in the channel allows to bound the amount of information of any eavesdropper with Holevo's bound χ_{BE} and find the secret key rate (per symbol):

$$K = \underbrace{\beta I_{ab}(V_A, T, \xi, \eta, V_{el})}_{\substack{\text{Shared information} \\ \text{between Alice and Bob}}} - \underbrace{\chi_{BE}(V_A, T, \xi, \eta, V_{el})}_{\substack{\text{Maximal information known} \\ \text{to an eavesdropper}}}$$



I_{ab} is the maximal shared information between Alice and Bob

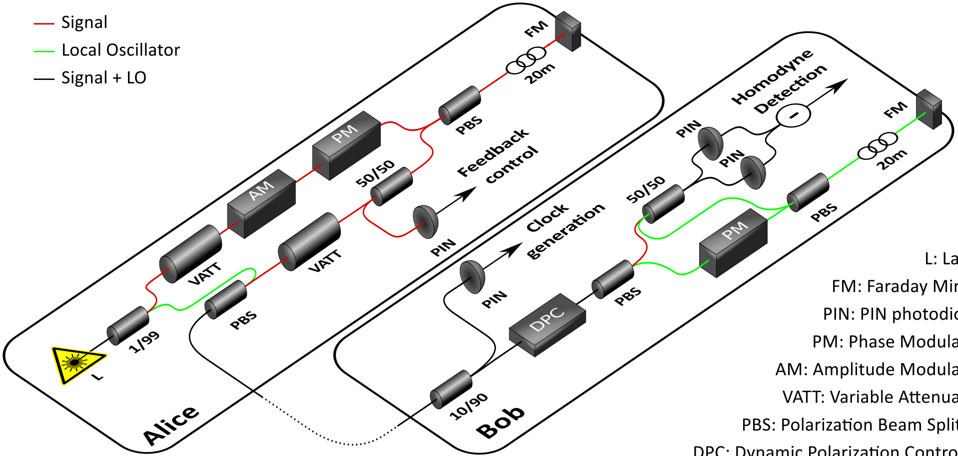
$$I_{ab} = log_2\left(1 + \frac{\frac{\eta T}{2} V_A}{1 + V_{el} + \frac{\eta T}{2}\xi}\right)$$

DV and CV Quantum Key Distribution

	Discrete Variable	**Continuous Variable**
Encoding	Single photons	Quadratures of the electromagnetic field
Hardware	Requires single photon detectors	Can use readily available telecom emitters and receivers
Secret key rate at metropolitan distance	10-1000 kbit/s	1-10 Mbit/s
Distance record	$\sim$400 km	$\sim$200 km
Post-processing	Light post-processing	Heavy post-processing
Integration	Hard integration of the single photon detector	Easier integration of emitter and receiver
Important parameters	QBER, detector efficiency, attenuation, reconciliation efficiency, dead time	Excess noise, detector efficiency attenuation, reconciliation efficiency detector noise, Alice's modulation strength, symbol rate

Performances for fiber communication and prepare-and-measure protocols.

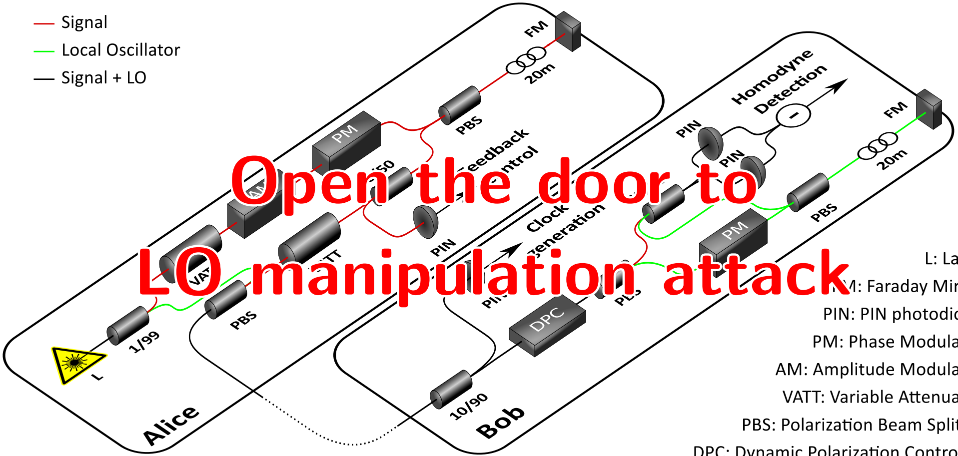
Historical implementations



L: Laser
FM: Faraday Mirror
PIN: PIN photodiode
PM: Phase Modulator
AM: Amplitude Modulator
VATT: Variable Attenuator
PBS: Polarization Beam Splitter
DPC: Dynamic Polarization Controller

Paul Jouguet, *et al*, Experimental demonstration of long-distance continuous-variable quantum key distribution

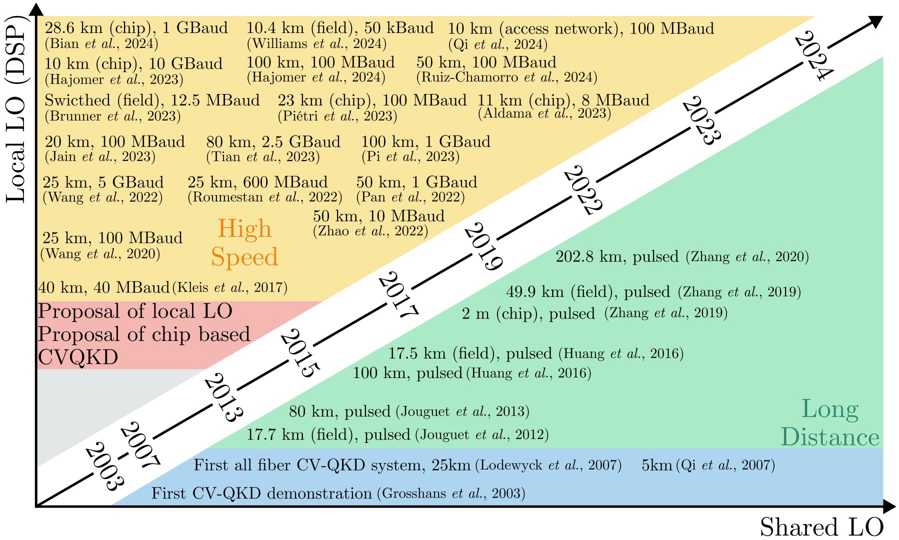
Historical implementations



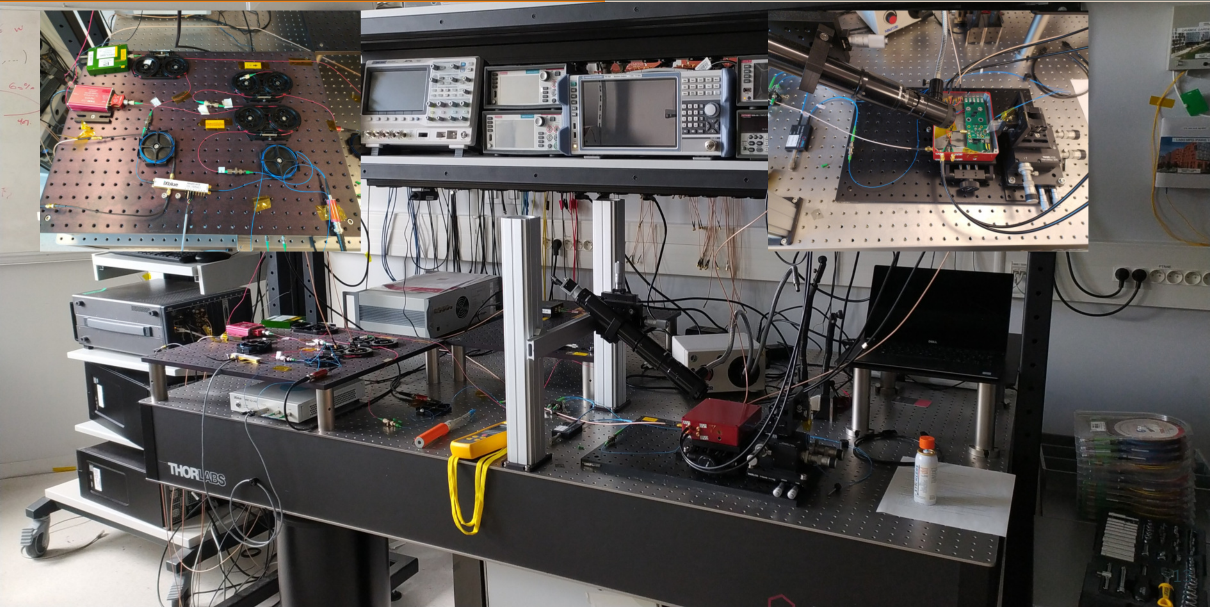
L: Laser
FM: Faraday Mirror
PIN: PIN photodiode
PM: Phase Modulator
AM: Amplitude Modulator
VATT: Variable Attenuator
PBS: Polarization Beam Splitter
DPC: Dynamic Polarization Controller

Paul Jouguet, *et al*, Experimental demonstration of long-distance continuous-variable quantum key distribution

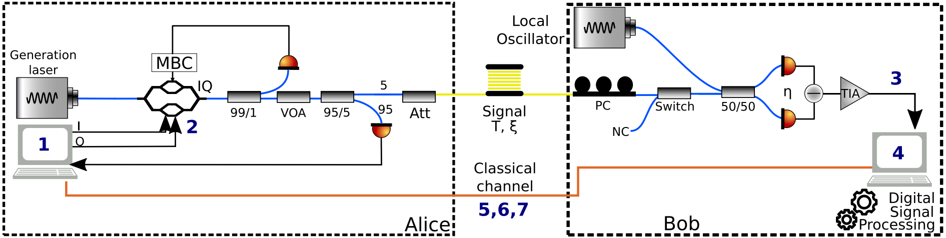
Historical implementations



The lab

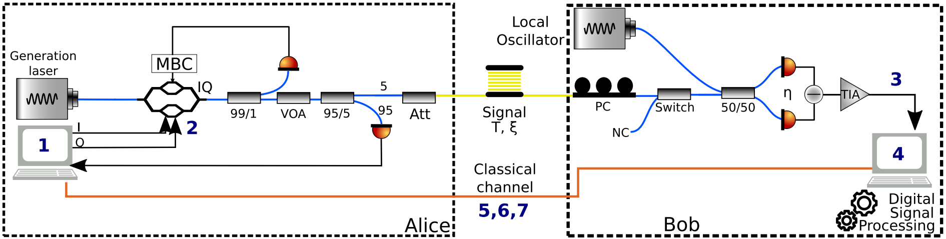


Experimental scheme



1	Alice's DSP
2	Generation of coherent states
3	Balanced detection
4	Bob's DSP
5	Parameters estimation
6	Error correction
7	Privacy amplification

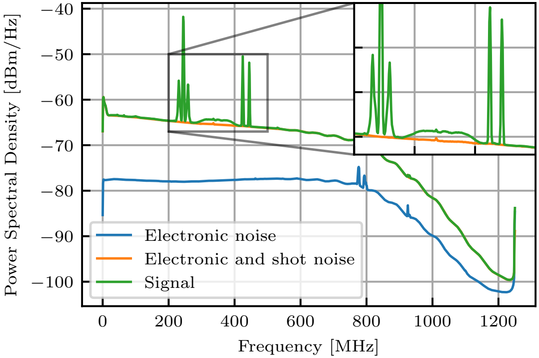
Experimental scheme



1	Alice's DSP
2	Generation of coherent states
3	Balanced detection
4	Bob's DSP
5	Parameters estimation
6	Error correction
7	Privacy amplification

⇒ **Clock, frequency and phase synchronizations are required.**

Phase, Frequency and clock recovery



- Clock

$$\Delta f = \frac{\tilde{f}^B_{pilot,2} - \tilde{f}^B_{pilot,1}}{f_{pilot,2} - f_{pilot,1}}$$

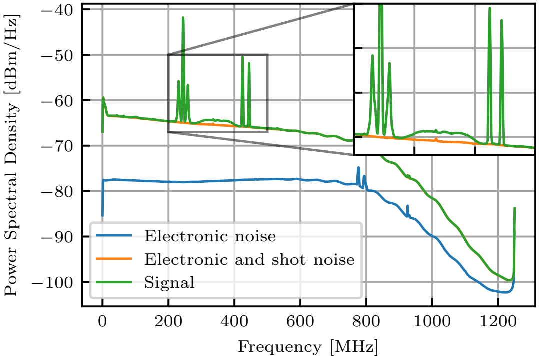
- Frequency

$$f_{beat} = f^B_{pilot,1} - f_{pilot,1}$$

- Phase

$$\Delta\theta(t) = s_{pilot,1}(t) \times e^{-2i\pi f^B_{pilot,1} t}$$

Phase, Frequency and clock recovery



- Clock

$$\Delta f = \frac{\tilde{f}^B_{pilot,2} - \tilde{f}^B_{pilot,1}}{f_{pilot,2} - f_{pilot,1}}$$

- Frequency

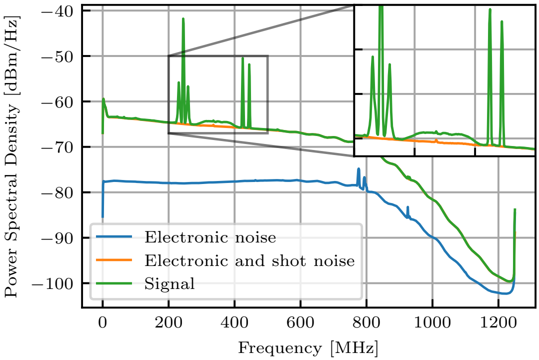
$$f_{beat} = f^B_{pilot,1} - f_{pilot,1}$$

- Phase

$$\Delta\theta(t) = s_{pilot,1}(t) \times e^{-2i\pi f^B_{pilot,1} t}$$

Proper recovery is crucial for good performance: any leftover impairment will be attributed to an eavesdropper.

Phase, Frequency and clock recovery



- Clock

$$\Delta f = \frac{\tilde{f}^B_{pilot,2} - \tilde{f}^B_{pilot,1}}{f_{pilot,2} - f_{pilot,1}}$$

- Frequency

$$f_{beat} = f^B_{pilot,1} - f_{pilot,1}$$

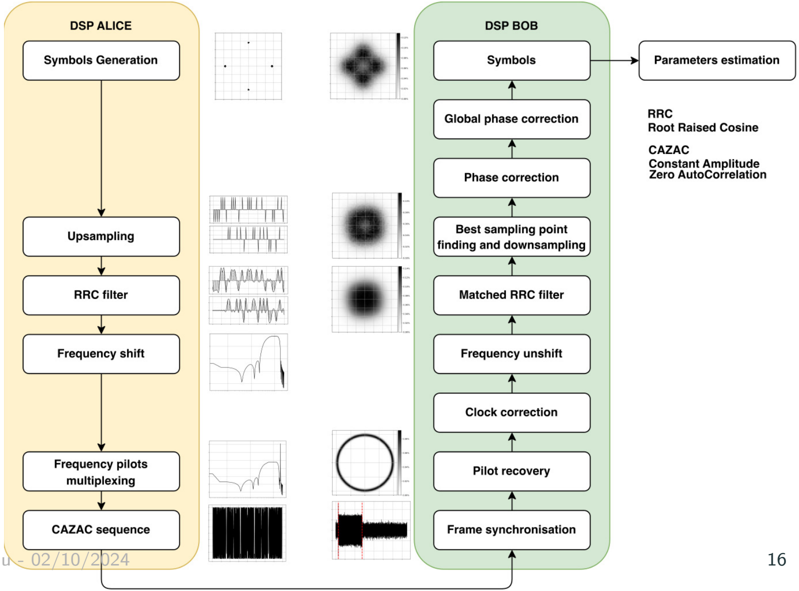
- Phase

$$\Delta\theta(t) = s_{pilot,1}(t) \times e^{-2i\pi f^B_{pilot,1} t}$$

Proper recovery is crucial for good performance: any leftover impairment will be attributed to an eavesdropper. Biggest source of noise is the phase noise.

Advanced Digital Signal Processing (DSP)

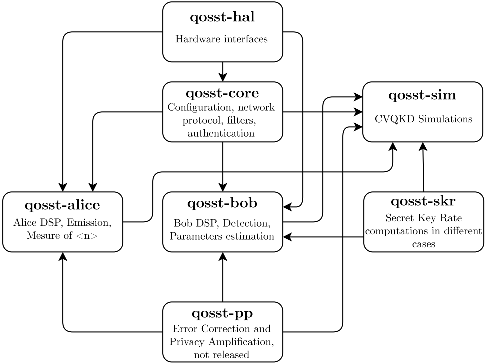
- Minimize hardware (no phase locking, no additional fiber or synchronisation channel required);
- Move corrections to digital processing.



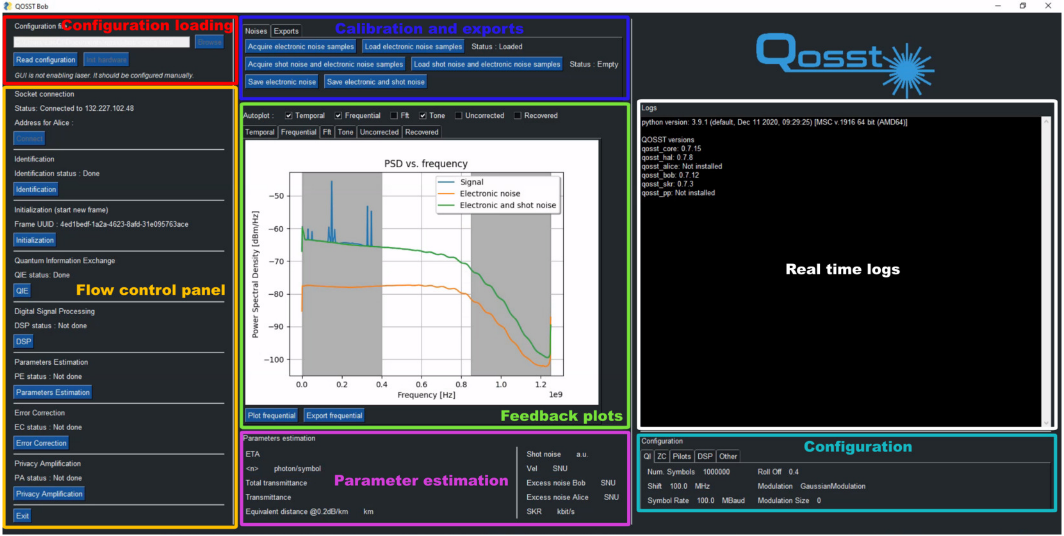
QOSST: An open source software for CV-QKD applications

- Full software suite for operating CV-QKD experiments, based on Python;
- Open source software (GPLv3 license);
- Includes DSP for Tx and Rx, hardware control and classical communication;
- Operates with built-in optimization subsystems over more than 10 DSP parameters, and calibration of Tx and Rx;
- Highly modular and hardware agnostic. Extensive documentation.

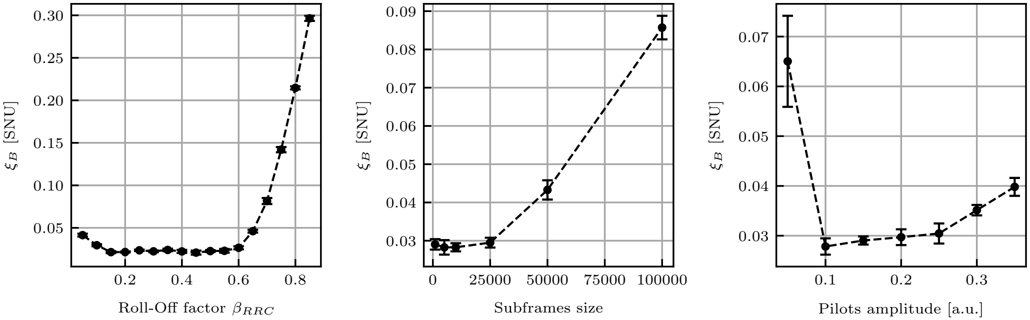
Quantum Open Software for Secure Transmissions



QOSST: An open source software for CV-QKD applications



Optimizing the DSP

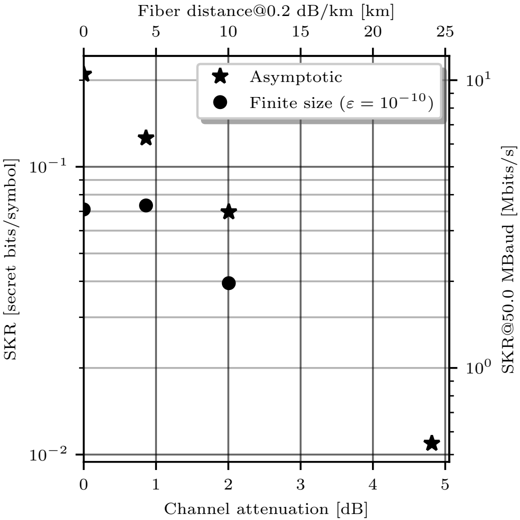


- Choice of parameters for the DSP is very important;
- Automated scripts to test every value of parameter and measure the excess noise;
- $\sim$10 DSP parameters can be optimized.

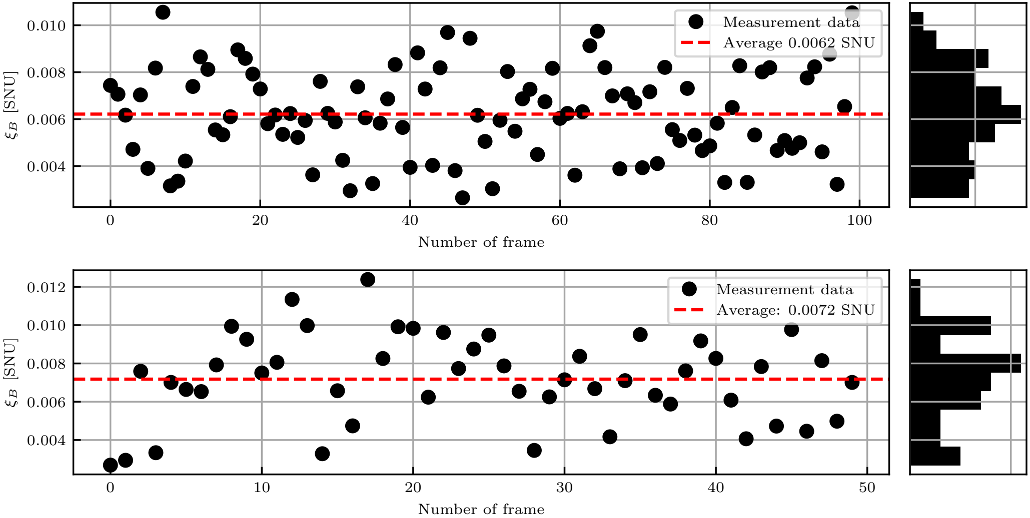
Benchmarking of the software

Distance	ξ_B	Key rate
0 km	0.0095 SNU	22.4 MBit/s
5 km (VOA)	0.0091 SNU	11.9 MBit/s
10 km (VOA)	0.0076 SNU	6.35 MBit/s
25 km (VOA)	0.0062 SNU	1.43 MBit/s
25 km (fiber)	0.0072 SNU	1.17 MBit/s

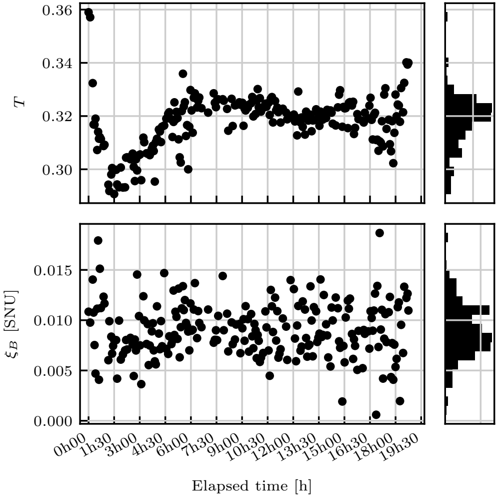
Parameter	**Value**	**Parameter**	**Value**
Modulation	Gaussian	f_{shift}	100 MHz
β_{RRC}	0.5	R_s	100 MBaud
$f_{\text{pilot},1}$	180 MHz	$f_{\text{pilot},2}$	200 MHz
L_{ZC}	3989	R_{ZC}	5
Acq. time	50 ms	β	0.95
DAC rate	2 GSa/s	ADC rate	2.5 GSa/s
η	55%	V_{el}	0.08 SNU

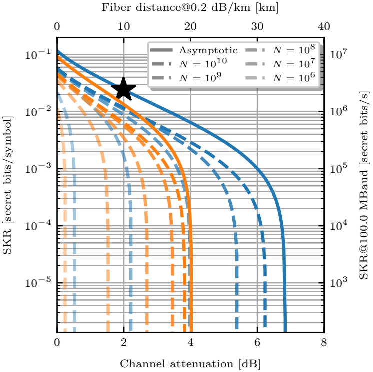


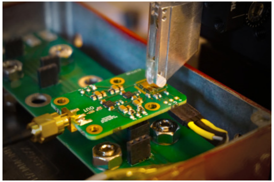
Benchmarking of the software



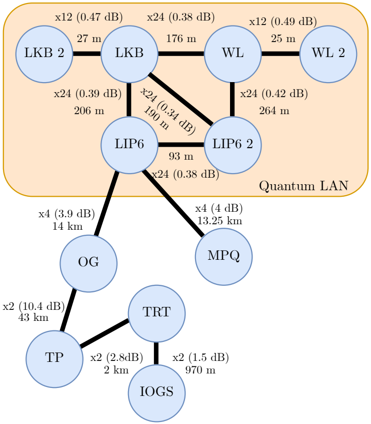
Benchmarking with a silicon PIC

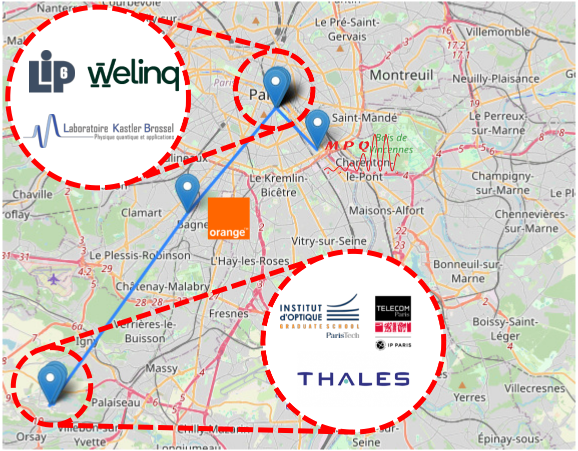




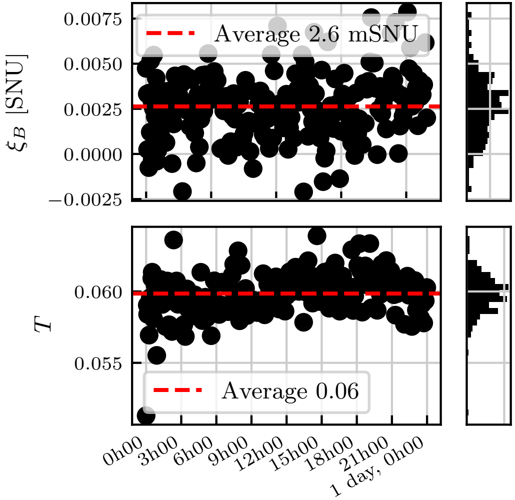


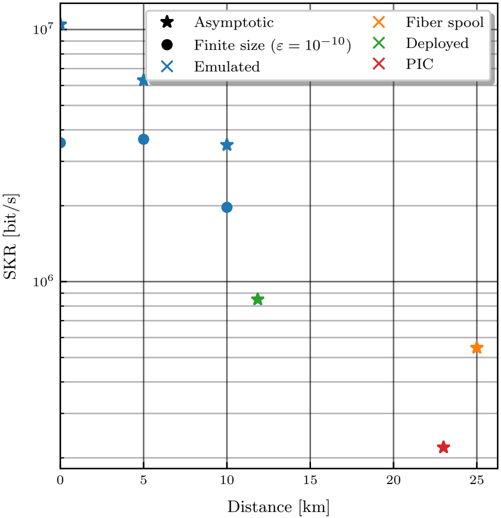
The Parisian Quantum Communication Infrastructure





Benchmark on the Parisian QCI





Conclusion

QOSST

- Open source suite for CV-QKD experiments. Released to the community;
- Hardware agnostic, with extensive documentation;
- Reaching state-of-the art key rates and excess noises;
- Other possible applications ?

Perspectives

- Error Correction and Privacy Amplification in QOSST;
- New integrated photonics devices (QSNP);
- Side channel attacks and certification (Nostradamus);
- CV-QKD satellite source (QUDICE) and atmospheric channel emulation.

We are open to collaborations with QOSST. Don't hesitate to reach out: Yoann.Pietri@lip6.fr !

arXiv:2404.18637

arXiv:2311.03978

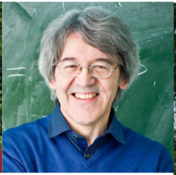
To appear in Optica Quantum

https://github.com/qosst

Thanks to the CV-QKD team in LIP6

Baptiste Gouraud

Philippe Grangier



Luis Trigo Vidarte

Valentina Marulanda Acosta

LIP6 Lab @ Sorbonne University in Paris
Quantum Information Team (~50 people)
Special thanks to the CV-QKD team