Towards practical free-space quantum communication

Pedro Mendes

QuLab
Quantum Photonics Laboratory

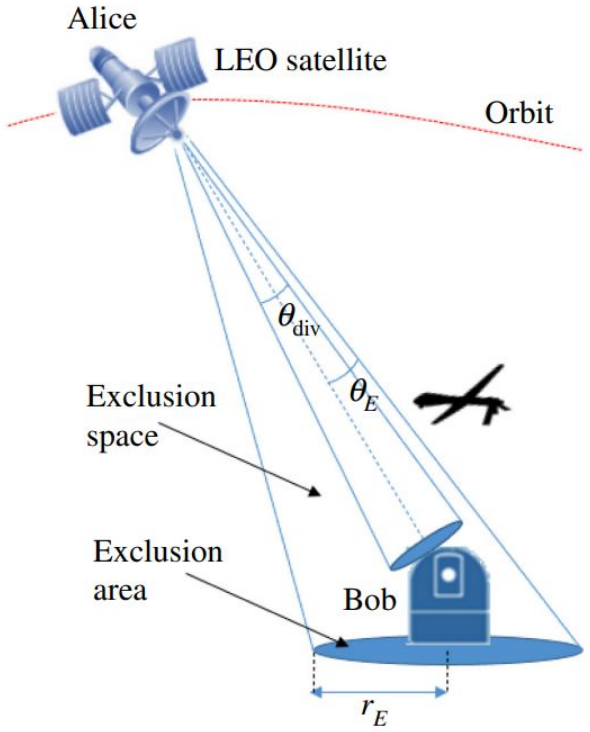
07/12/2023

TÉCNICO
LISBOA

instituto de
telecomunicações

Free-Space Quantum Communication

- Traditional cryptographic security relies heavily on computational assumptions, and this makes it vulnerable
- Free-Space: Long distance, airborne vehicles, new protocols
- QKD problems: distance/conditions limitation (satellites → night time only), experimental complexity…
- Can we do better? Yes, if we restrict Eve



Wiretap Model history

- 1949: Shannon
- 1975: Wyner
- 1978: Csiszár and Korner
- 2000: Long (QSDC)
- 2021: Vázquez-Castro, Rusca and Zbinden (QKPC)

γ - Channel degradation

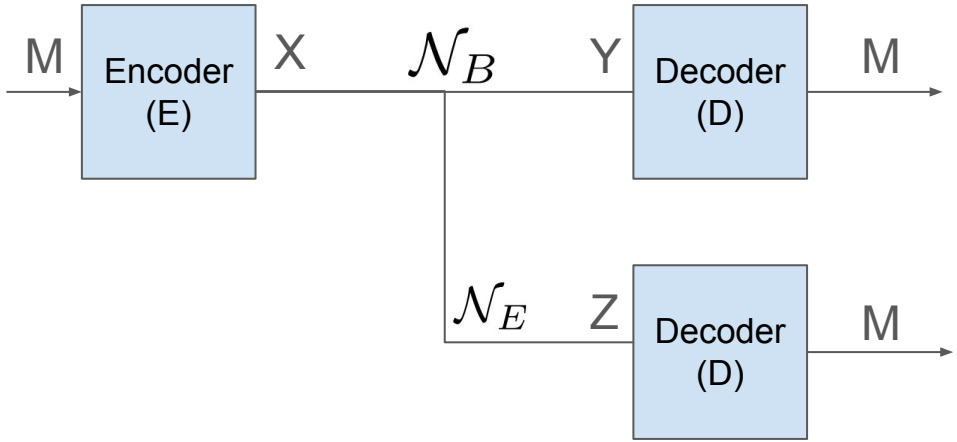
$I(X;Y)$ - Shannon mutual information using photon counting detectors

$I(X;Z|\gamma)$ - Shannon mutual information that Eve can physically detect

$$C_P(\gamma) = \max_q \{I(X;Y) - I(X;Z|\gamma)\},$$

Wiretap Model

- Alice communicates with Bob a message M subjected to N_B noise
- Eve intercepts the communication but with additional loss N_E
- For a given encoder and decoder, information-theoretic security can be proven
- Eve cannot extract useful information

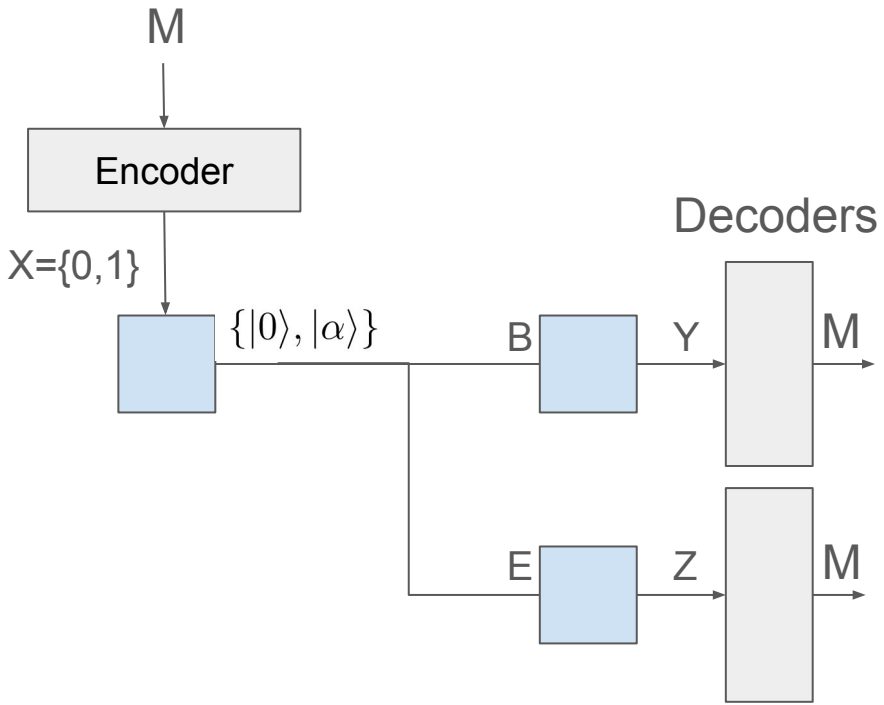


$$\mathcal{N}_B < \mathcal{N}_E$$

$$I(X;Z|\gamma) \to 0$$

Quantum Keyless Private Communication

1. **Encoding** - Alice, sends a stream of secret information bits to a stochastic public wiretap encoder
2. **State Preparation -** Alice prepares a coherent state modulated by the random variable $X \in X = \{0, 1\}$
3. **Measurement -** Bob receives B and Eve E. Bob estimates Y. Eve estimates Z.
4. **Decoding -** Bob and Eve send their estimated received states to the public known decoder.



Simplified QKD Protocol (2018)

- Alice sends two states in the Z basis and one state in the X basis
- Z basis exchanges the secret key, while X basis estimates information leakage
- Bob measures in the Z basis or only one state in the X basis, considering the potential no-detection
- No-detection event ($|\varnothing\rangle$) represents possible loss in the channel or an adversary's interference.

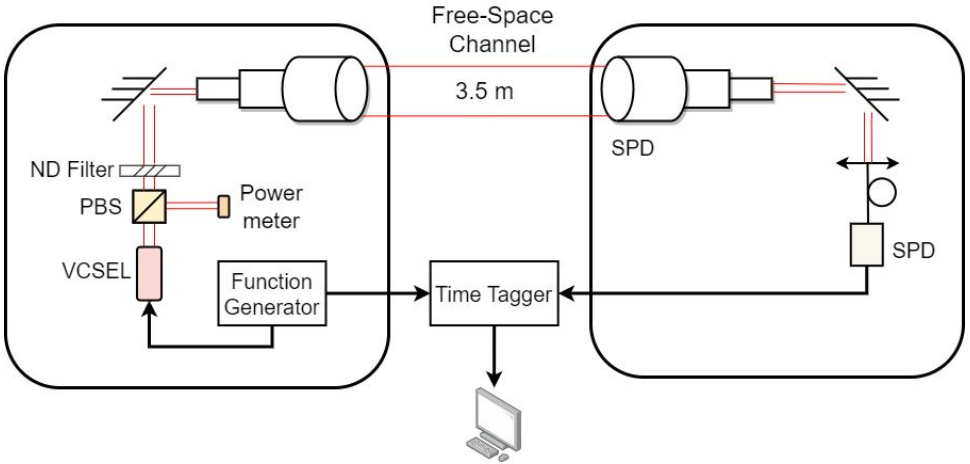
Alice states:

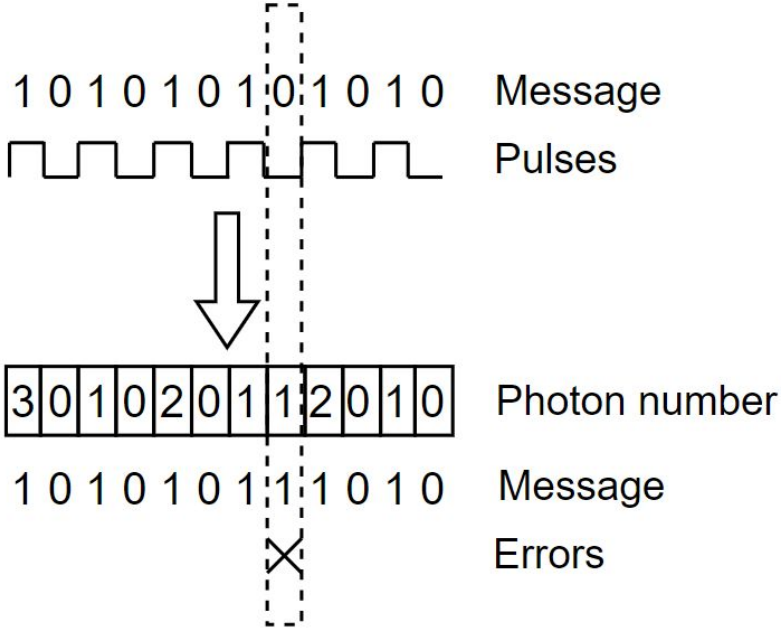
$$\{|H\rangle, |V\rangle, |D\rangle\}$$

Bob projections:

$$\{|H\rangle, |V\rangle, |A\rangle, |\emptyset\rangle\}$$

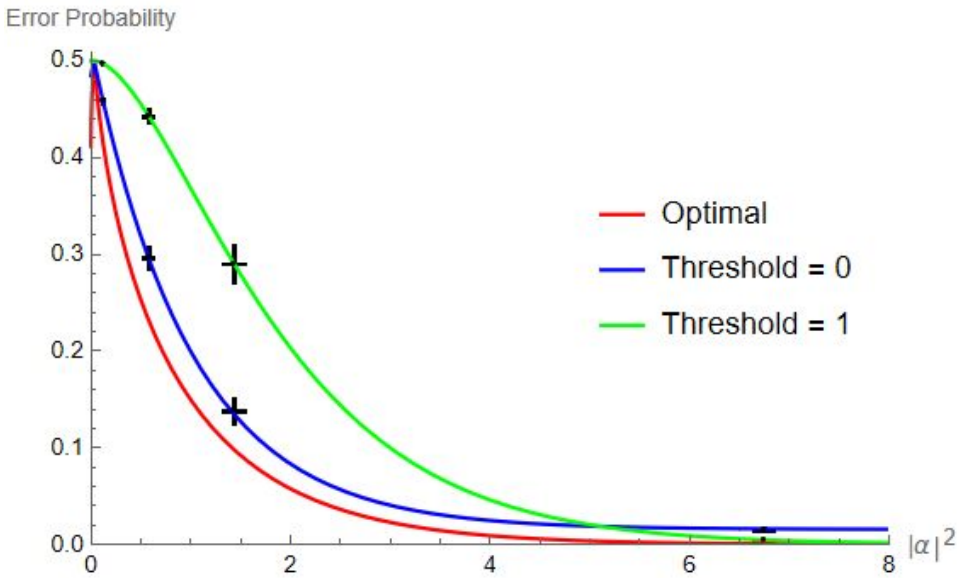
Experimental Setup - QKPC



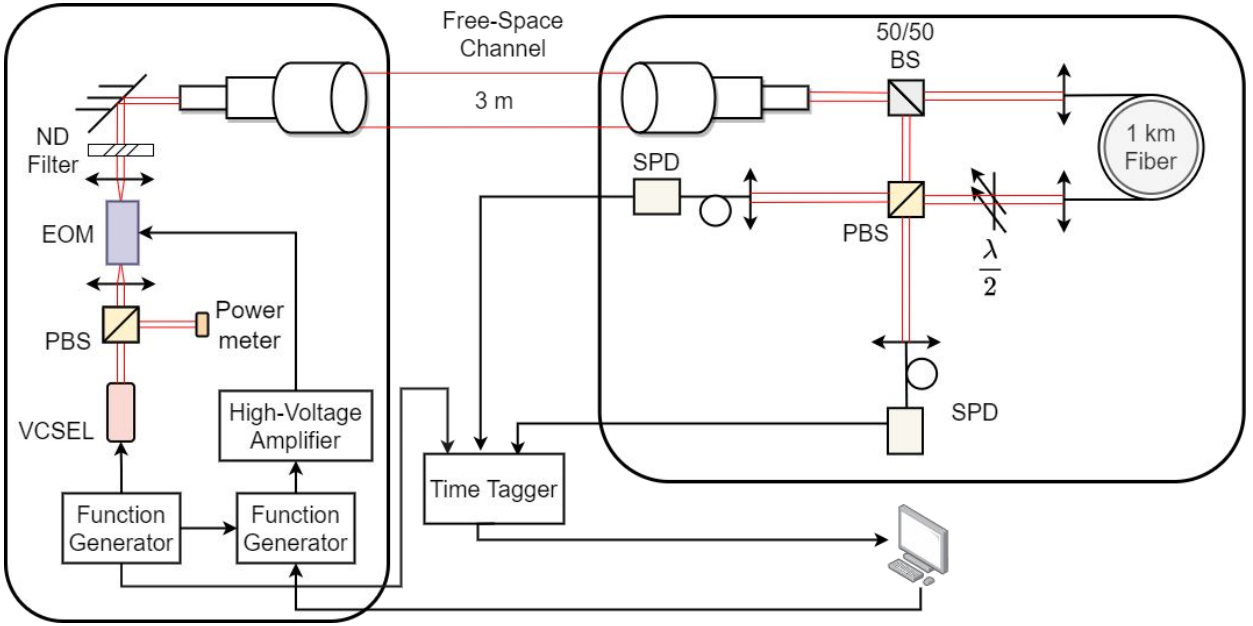


Results - QKPC

- The plots show the error probability in the recovered string as a function of the average number of photons of the state sent
- Different colours represent different threshold chosen
- The measured data matches well with the simulated plots

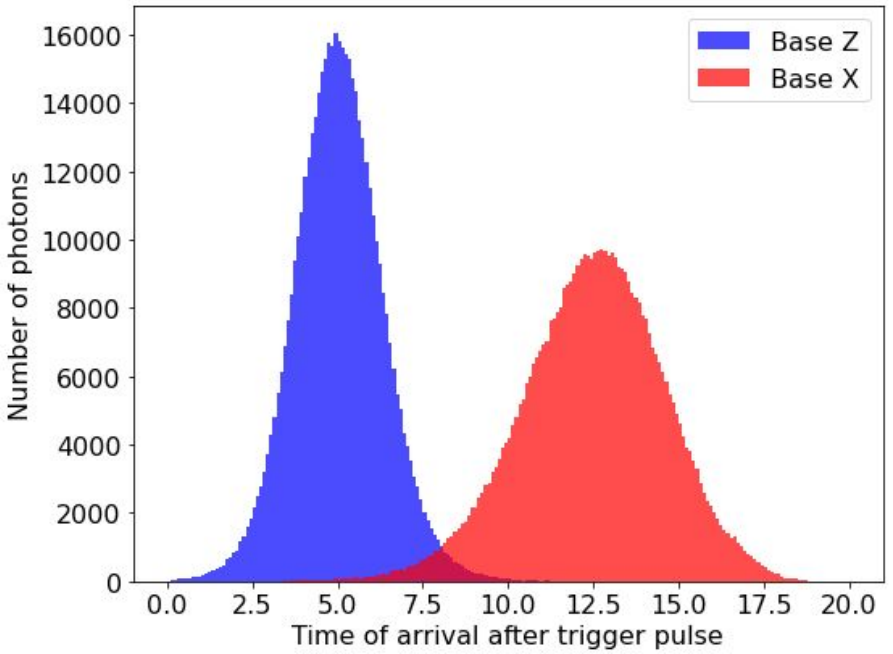


Experimental Setup - Simplified



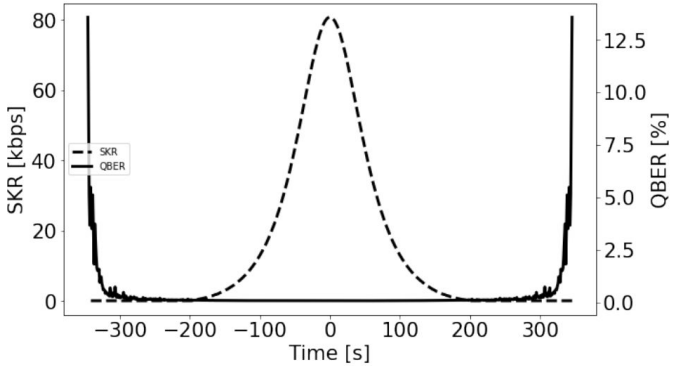
Results - Simplified

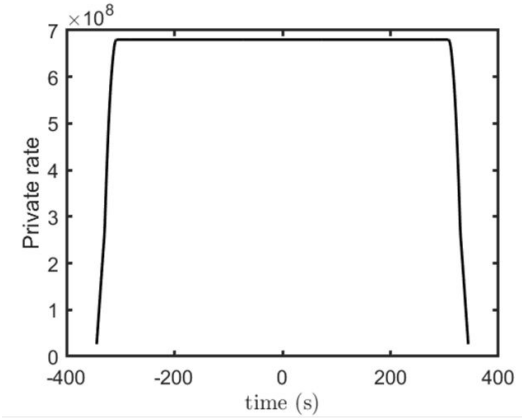
- Verification of time multiplexing with a fiber-delay.
- Estimation of the quantum state fidelity:
  - 0.999 ± 0.024 |H⟩,
  - 0.998 ± 0.024 |V⟩,
  - 1.000 ± 0.024 |D⟩
- QBER of 2.5% in Z basis and 2.1% in X basis.



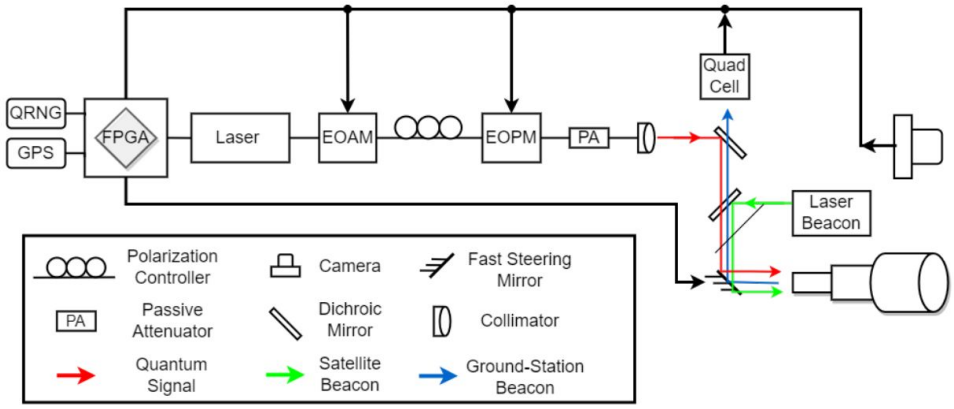
QKD vs QKPC

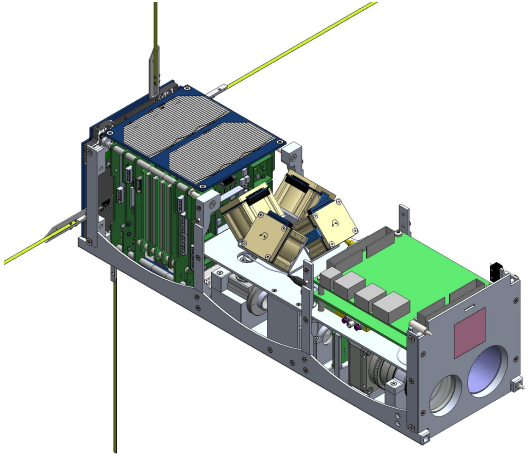
- Most practical QKD protocols:
  - Efficient BB84
  - Simplified BB84
- SatQuMA => Efficient BB84 results in low rates for satellite
- Us => Simplified BB84 is better for higher loss but still low rates
- QKPC's private rate is around 700 Mb/s during the overpass
- QKD's secret key rate is at most 80 Kb/s during zenith

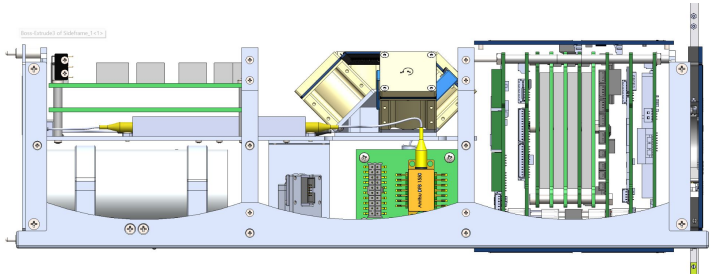




Satellite design

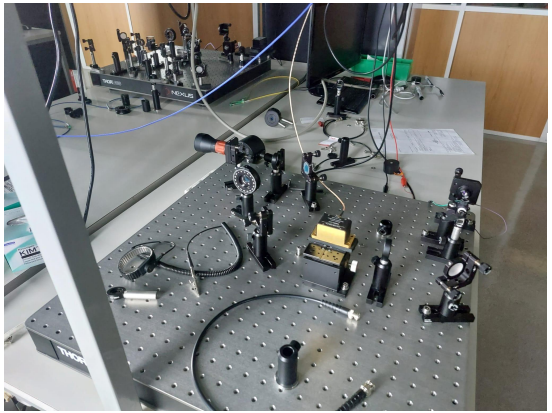


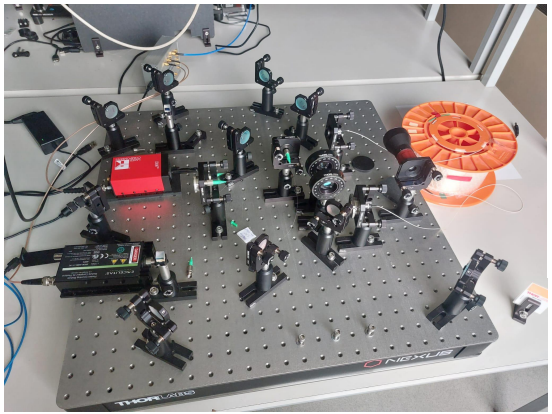


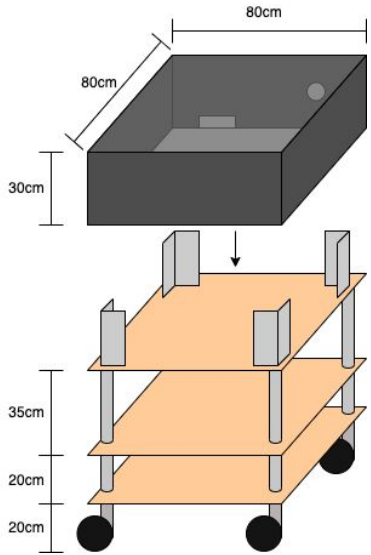


Conclusion and Outlook

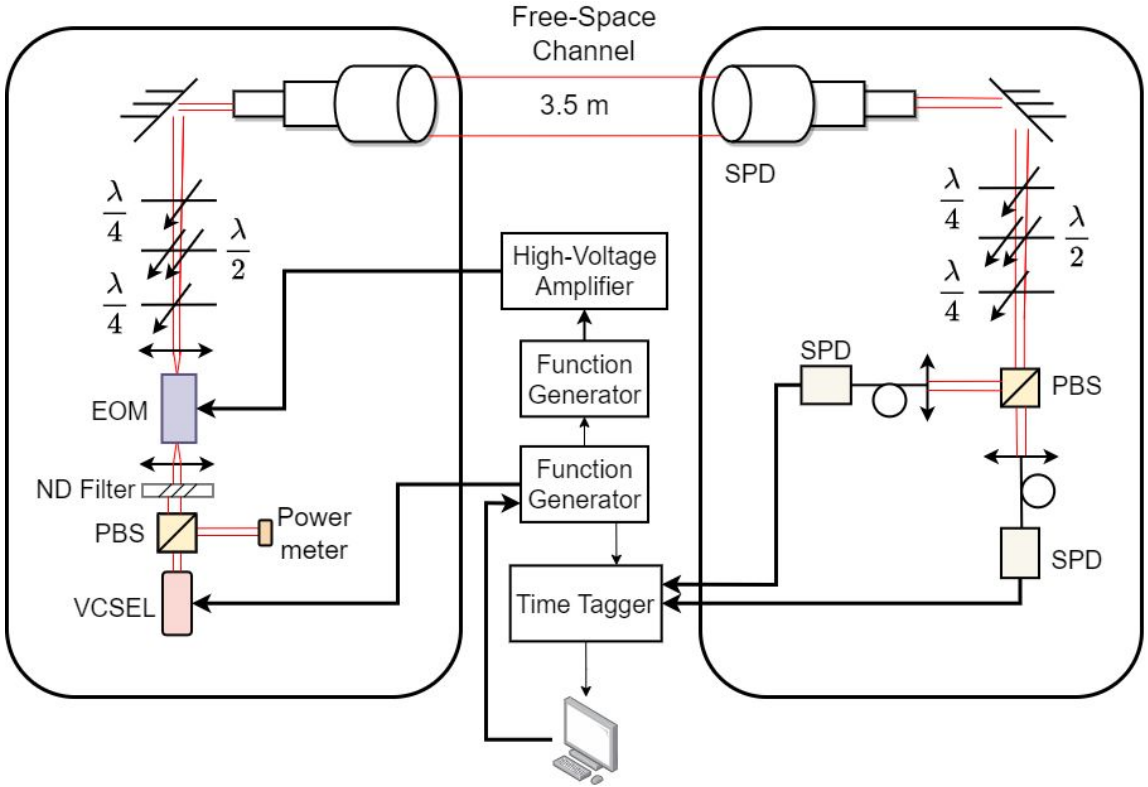
- Portable/Compact Setup useful for airborne applications and more practical quantum communication
- New protocols (Polarization Multiplexing) already being explored in the lab
- New types of Q.C. (Prepare and measure, Entanglement Assisted, Contextuality?)







Experimental implementation: Setup



$$|\alpha_1\rangle = e^{-\frac{1}{2}|\alpha_1|^2} \sum_{n=0}^{\infty} \frac{\alpha_1^n}{(n!)^{1/2}} |n\rangle$$