Polarization-Multiplexed Quantum Keyless Private Communication for Free-Space Applications

Pedro Neto Mendes[1,2], Davide Rusca[3], Hugo Zbinden[4] and Emmanuel Zambrini Cruzeiro[1,2]

1 - DEEC, Instituto Superior Técnico, Universidade de Lisboa, Avenida Rovisco Pais 1, 1049-001, Lisboa, Portugal
2 – Quantum Photonics Laboratory, Instituto de Telecomunicações, Avenida Rovisco Pais 1, 1049-001, Lisboa, Portugal
3 - AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain
4 - Group of Applied Physics, Univeristy of Geneva, Rue de l'Ecole-de-Médecine 20, CH-1211, Genève, Switzerland

Introduction

Background: Quantum Key Distribution (QKD) has become the standard for secure communication. However, it requires complex infrastructure and significant resources, limiting its practical implementation.

Objective: Introduce and validate a novel polarization-multiplexed Quantum Keyless Private Communication (QKPC) protocol that can achieve information-theoretic security with simpler setups, in high noise regimes, particularly suitable for free-space space-based applications [1, 2].

QKPC

- Information encoded directly on the quantum states (weak coherent pulses).
- No keys required.
- Eve only receives a part of the signal (γ), based on the Wiretap model [3].

Steps: Encoding; State preparation; Measurement; Decoding.

On-Off Keying (OOK) encoding:

- Information encoded on the number of photons:

$$|\psi_0\rangle = |0\rangle,$$
$$|\psi_1\rangle = |\alpha\rangle.$$

Polarization encoding:

- Information encoded also on the polarization:

$$|\psi_0\rangle = |\alpha\rangle_H |0\rangle_V$$
$$|\psi_1\rangle = |\cos\theta\beta\rangle_H |\sin\theta\beta\rangle_V$$

Eve: Can discriminate the states optimally (Helstrom Bound). Modeled by a symmetric binary channel with mutual information, I_E.

Bob: Uses practical detection schemes. Modeled by an asymmetric binary channel with mutual information, I_B.

Quantum Bit Error Rate (QBER): Given by the error probability in discriminating the states

Private Capacity (C_p): $C_p(\gamma) = \max_{q_0} [I_B - I_E]$

Δ: Average number of background photons

Experimental Setup

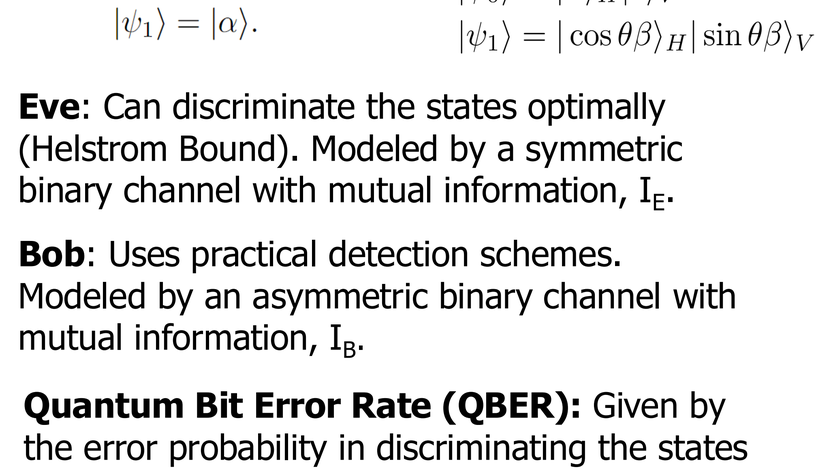

Figure 1: A portable setup capable of implementing both implementations of the QKPC protocol. PBS: polarizing beam splitter. EOPM: electro-optic polarization modulator. PA: passive attenuator. SPD: single photon detector. λ4 : quarter-waveplate. λ2 : half-waveplate. The black arrows are electrical connections.

QBER

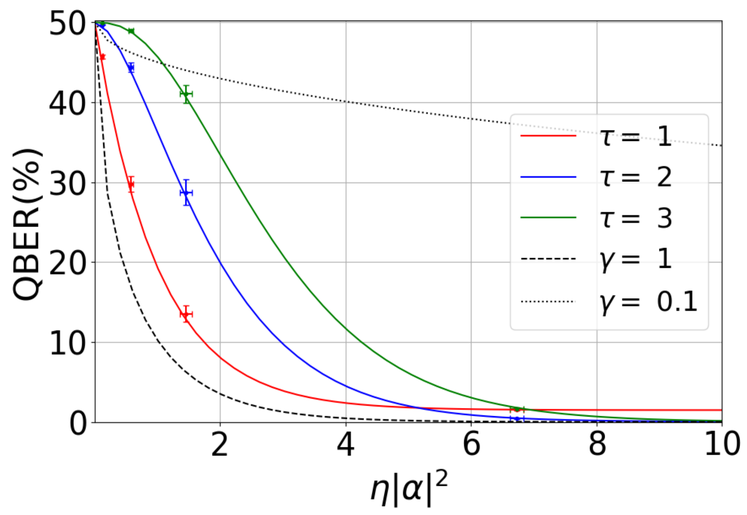

Figure 2: Bob's QBER as a function of the number of received photons for different estimation techniques (solid). Eve's QBER for two γ values (dashed).

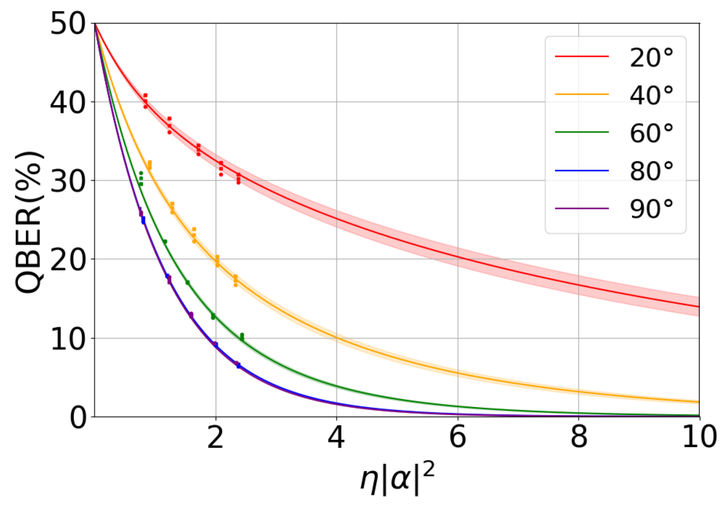

Figure 3: Bob's QBER as a function of the number of received photons for various polarization angles.

Optimal Private Capacity

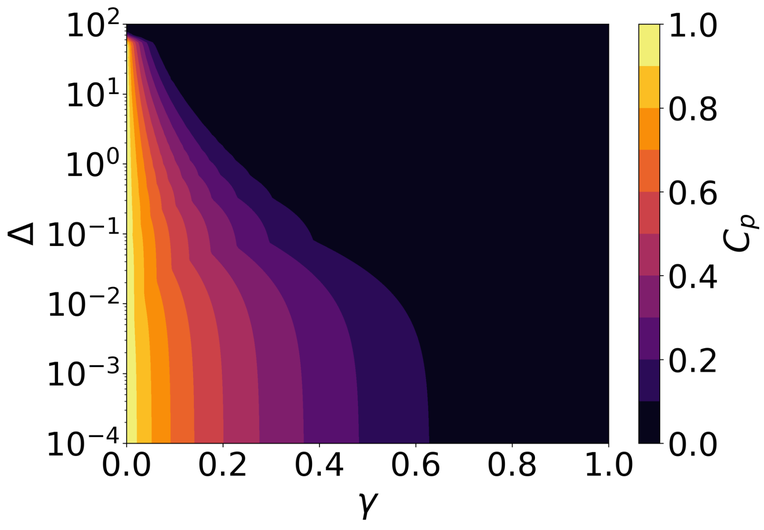

Figure 4: Heatmap of the optimal private capacity for diferente values of Δ and γ using OOK implementation.

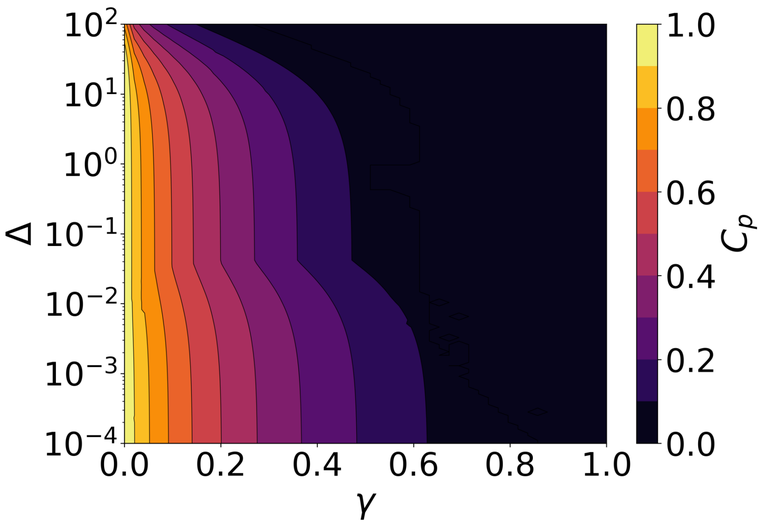

Figure 5: Heatmap of the optimal private capacity for diferente values of Δ and γ using the polarization implementation.

Free-space daylight quantum communication

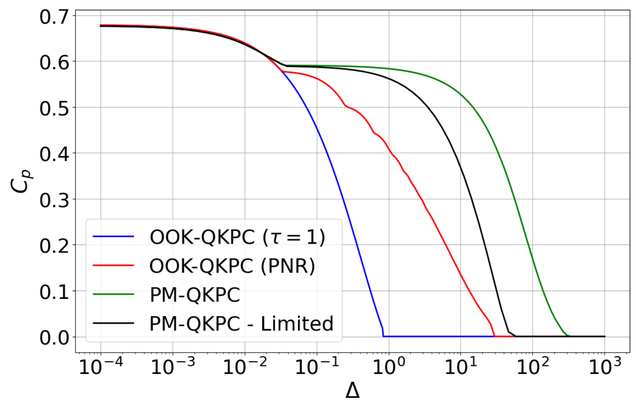

Figure 6: Plot of the maximum private capacity as a function of the photon noise, Δ, for γ = 0.1, for different protocol implementations.

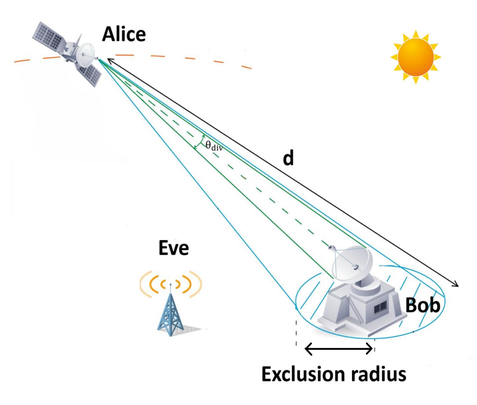

Figure 7: Free-space satellite downlink scenario during daylight, illustrating the QKPC security concept.

Conclusion

- QKPC is promising for free-space quantum communication applications, including space-based links.
- The use of polarization encoding improves the resilience, enabling daylight operation of QKPC
- It enables quantum secure high rate data transfer with moderate experimental requirements, making quantum communication more practical.

References

[1] - A. Vázquez-Castro, et al. Quantum keyless private communication versus quantum key distribution for space links, Physical Review Applied 16, 014006.

[2] - Mendes, P.N., et al. Optical payload design for downlink quantum key distribution and keyless communication using CubeSats. EPJ Quantum Technol. 11, 48 (2024)

[3] - Aaron D Wyner. The wire-tap channel. Bell system technical journal, 54(8):1355–1387, 1975.

Acknowledgements

The authors thank the support from Instituto de Telecomunicações.
P.N.M. acknowledges the support of FCT through scholarship 2024.01717.BD.
E.Z.C. acknowledges funding by FCT/MCTES - Fundação para a Ciência e a Tecnologia (Portugal) - through national funds and when applicable co-funding by EU funds under the project UIDB/50008/2020. E.Z.C. also acknowledges funding by FCT through project 021.03707.CEECIND/CP1653/CT0002. The authors thank the support from the European Commission (EC) through project PTQCI (DIGITAL-2021-QCI-01).