Quantum keyless private communication under intense background noise

Pedro Neto Mendes

PTQCI Workshop in Lisbon

09/09/2024

TÉCNICO LISBOA

instituto de telecomunicações

Motivation

We live in a highly connected world

- Every day, we exchange thousands of messages.
- Secure communication is essential for our modern lifestyle.

Classical Security Today

- Current security protocols rely on hard-to-solve problems.
- Even the best computers today would take 1,000 years to crack these codes.

The Quantum Threat

- Quantum computers will soon be able to break today's encryption much faster than classical computers.
- Your data can be recorded today and decrypted in the future.

The Solution: Quantum Communication

- A security system based on the laws of physics, not computational assumptions

Quantum Communication Protocols

Quantum Key Distribution (QKD)

- Uses quantum properties to create secure keys.
- Well established (satellites, metropolitan network tests, commercial products…).
- Limited distance, complex and expensive.

Quantum Keyless Private Communication (QKPC)

- No key used, message communicated directly.
- More practical and simple.
- Requires extra assumptions on the channel and still in development.

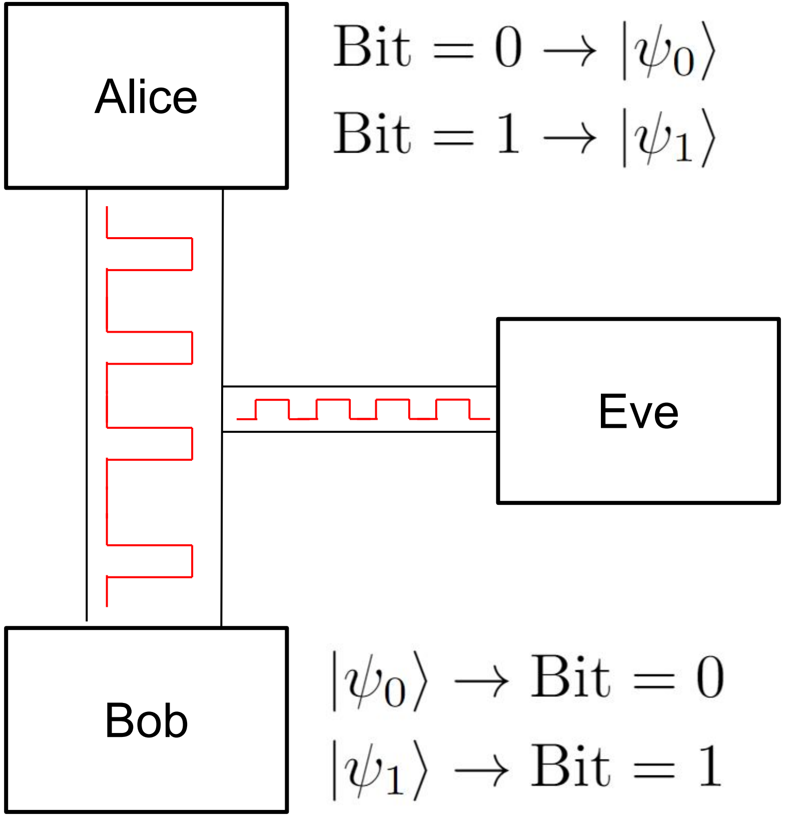
The Wiretap model

- **Communication:**
  - Alice sends a message to Bob.
  - Eve is listening.
- **Noisy channels:**
  - (Alice → Bob) - Noisy.
  - (Alice → Eve) - Noisier.
- **Private Capacity:**
  - Message can only be decoded with enough information.
  - Information-Theoretic Security.

$$C_p(\gamma) = \max_{q_0} \left[I_B - I_E \right]$$

QKPC protocol

- Alice encrypts her message and encodes it in non-orthogonal quantum states (Coherent States).
- Eve captures a fraction of these quantum states.
- Bob measures and discriminates the states and decrypts the message.
- The Quantum Bit Error Rate (**QBER**) measures the amount of error in the discrimination.



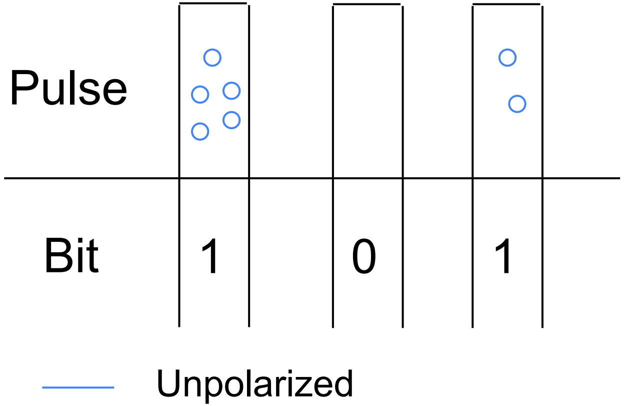
$$\text{Bit} = 0 \rightarrow |\psi_0\rangle$$
$$\text{Bit} = 1 \rightarrow |\psi_1\rangle$$

$$|\psi_0\rangle \rightarrow \text{Bit} = 0$$
$$|\psi_1\rangle \rightarrow \text{Bit} = 1$$

Encodings

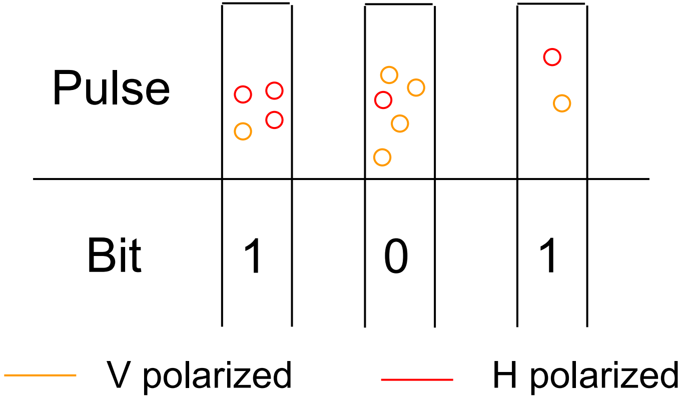
On-Off Keying

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



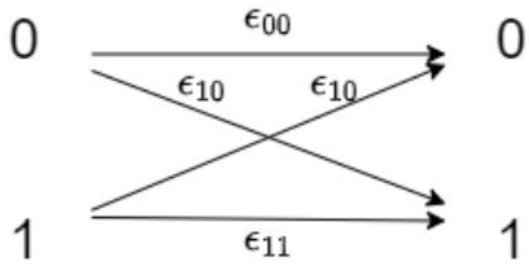
Polarization

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



Discrimination OOK

- When Bob receives 0 photons, Alice most likely sent nothing.
- If Bob measure something, could Alice have sent nothing?
- **Δ** - Photon noise (Dark counts, background radiation…).
- **τ** - Threshold choice.



$$\epsilon_{00} = \sum_{i=0}^{\tau-1} e^{-\Delta}\frac{\Delta^i}{i!}.$$

$$\epsilon_{01} = \sum_{i=0}^{\tau-1} e^{-(|\alpha|^2+\Delta)}\frac{(|\alpha|^2+\Delta)^i}{i!}.$$

Discrimination Polarization

- For bit = 0 maximize the number of photons to one detector.
- For bit = 1 maximize the number of photons to the other detector.
- Check which detector clicked more often.
- $\boldsymbol{\Delta}$ - Photon noise (Dark counts, background radiation…).

$$P(m|0) = e^{-|\alpha|^2} \sum_{l=0}^{\infty} \frac{(|\alpha_H|^2)^{l+m}(|\alpha_V|^2)^l}{(l+m)!l!},$$

$$P(m|1) = e^{-|\beta|^2} \sum_{l=0}^{\infty} \frac{(|\beta_H|^2)^{l+m}(|\beta_V|^2)^l}{(l+m)!l!},$$

$$\epsilon_{00} = P(m \geq 0|0) = \sum_{m=0}^{\infty} P(m|0).$$

$$\epsilon_{01} = P(m \geq 0|1) = \sum_{m=0}^{\infty} P(m|1).$$

Discrimination Eve

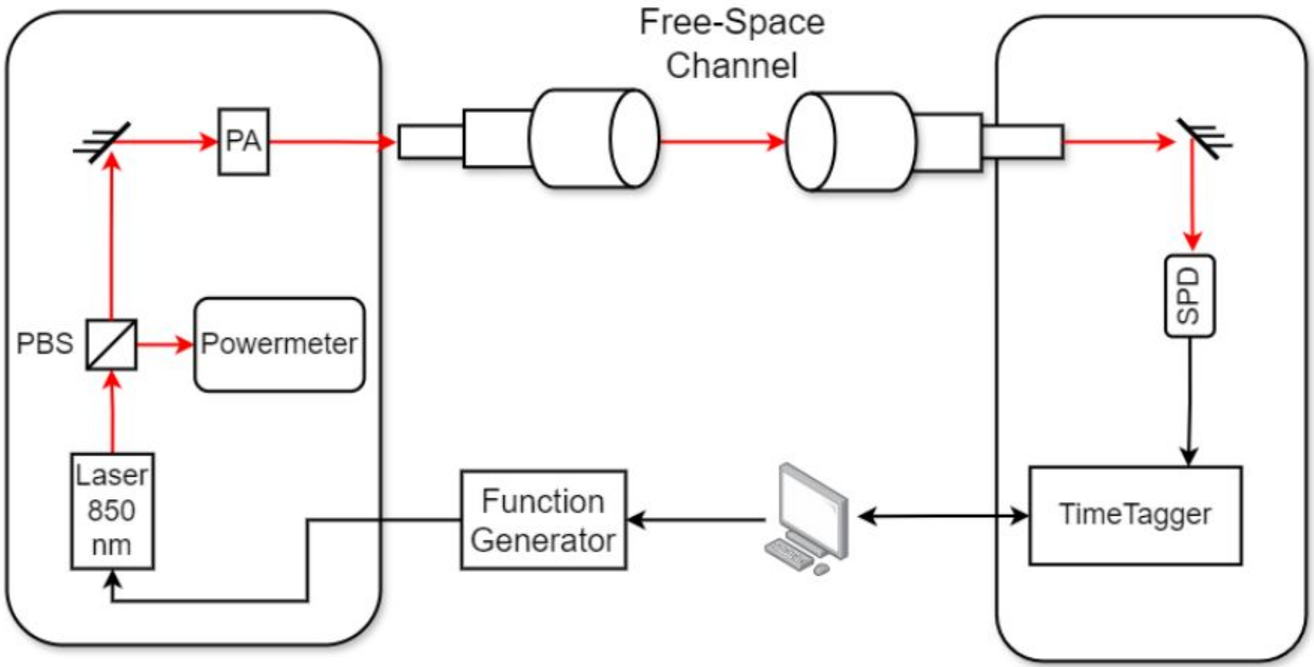
- Eve is assumed to have unlimited computing power.
- Optimal discrimination - Helstrom bound.
- Physical disadvantage, noisier channel.
- γ - Eve’s intercepted signal.

$$\epsilon_\gamma = \frac{1}{2}\left(1 - \sqrt{1 - 4q_0q_1|\langle\psi_0|\psi_1\rangle|^2}\right),$$

$$\langle\psi_0|\psi_1\rangle = e^{-\gamma\frac{|\alpha|^2}{2}}.$$

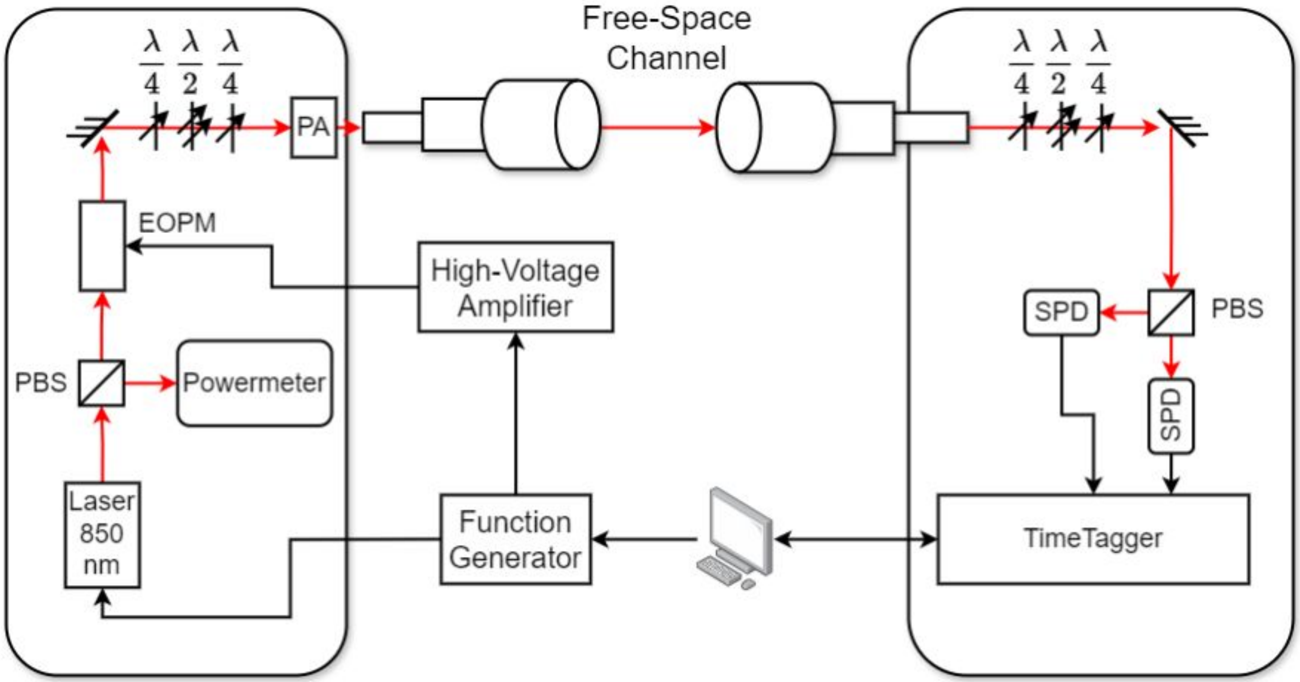
$$\langle\psi_0|\psi_1\rangle = e^{-\gamma\frac{|\alpha|^2+|\beta|^2}{2}}e^{\gamma\cos(\theta)|\alpha||\beta|},$$

Experimental setup - OOK



PBS: Polarizing Beam Splitter; PA: Passive Attenuator
SPD: Single Photon Detector.

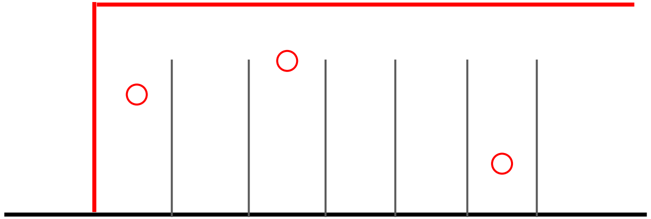
Experimental setup - Polarization

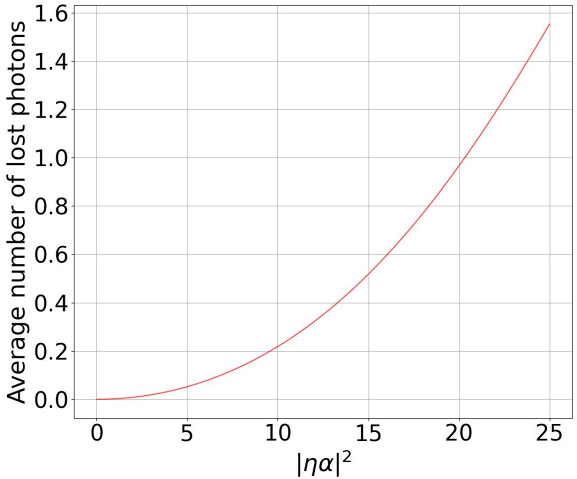

Free-Space Channel
$\frac{\lambda}{4}$ $\frac{\lambda}{2}$ $\frac{\lambda}{4}$
PA
EOPM
High-Voltage Amplifier
PBS
Powermeter
Laser 850 nm
Function Generator
$\frac{\lambda}{4}$ $\frac{\lambda}{2}$ $\frac{\lambda}{4}$
SPD
PBS
SPD
TimeTagger

PBS: Polarizing Beam Splitter; PA: Passive Attenuator; SPD: Single Photon Detector; EOPM: Electro-Optic Polarization Modulator.

Experimental setup - Photon counting

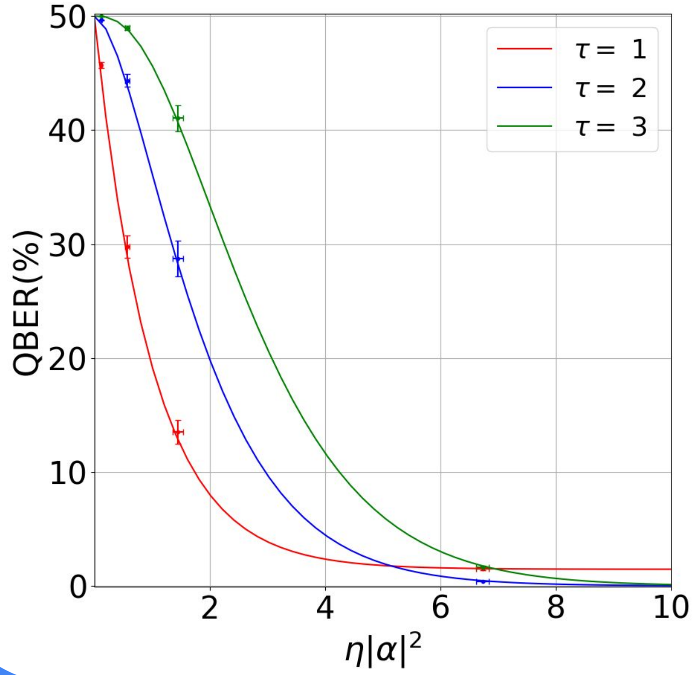
- Time multiplex the threshold single photon detector to count the number of photons.
- Detector dead time = 40 ns.
- Pulse width = 10000 ns.
- There are 250 time bins.
- Low probability of miscount.



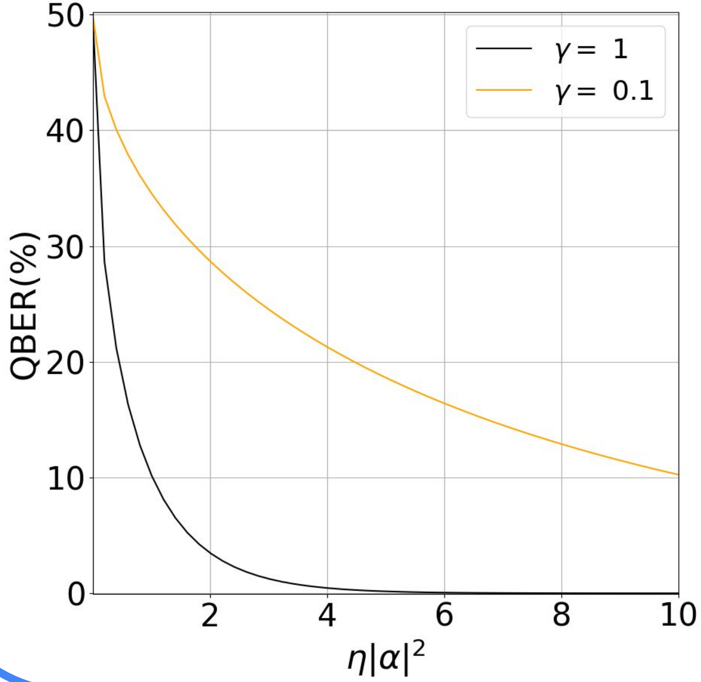


QBER OOK

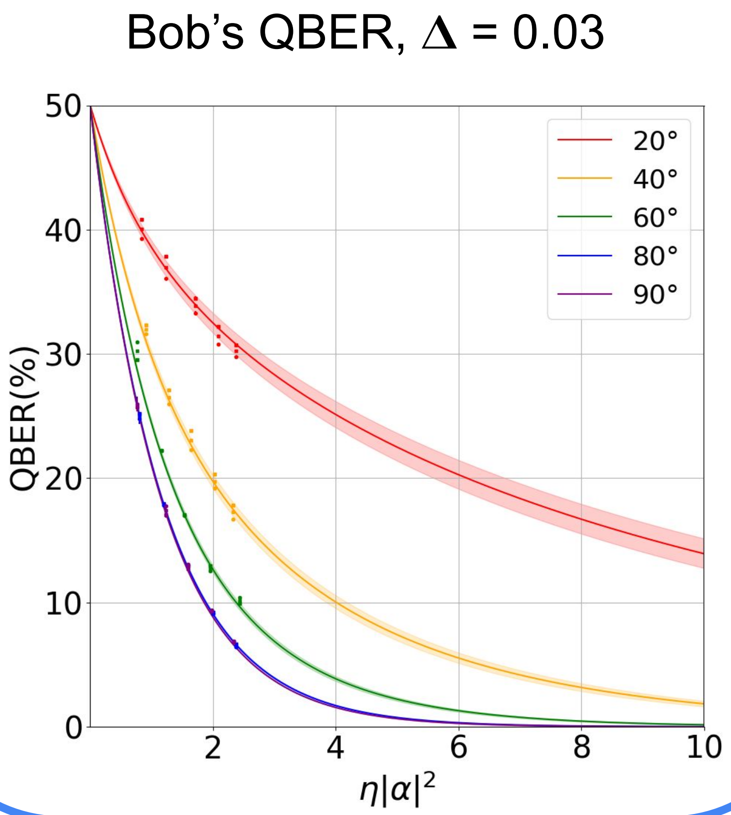
Bob’s QBER, Δ = 0.03



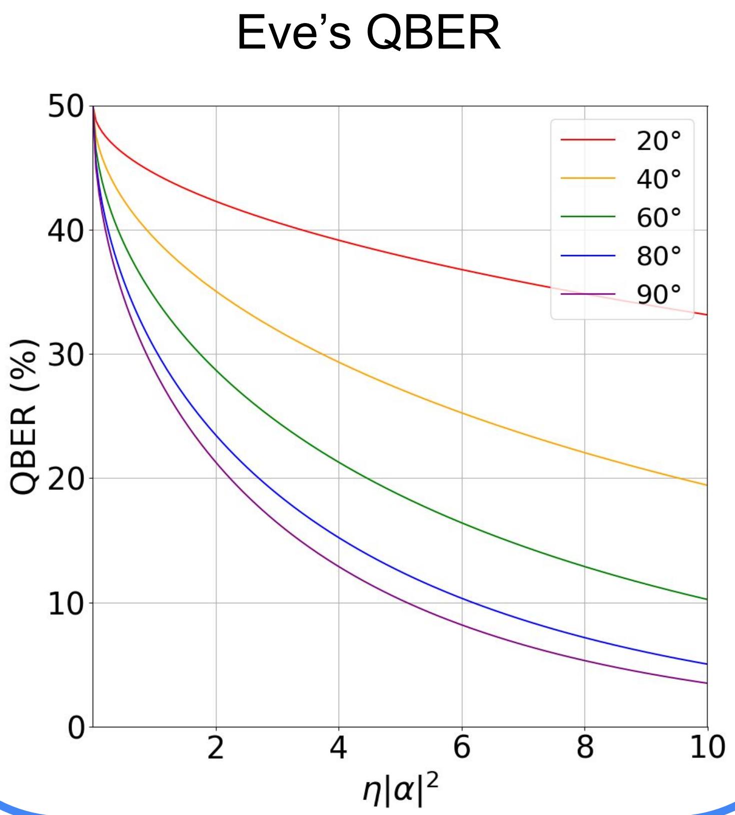
Eve’s QBER



QBER Polarization



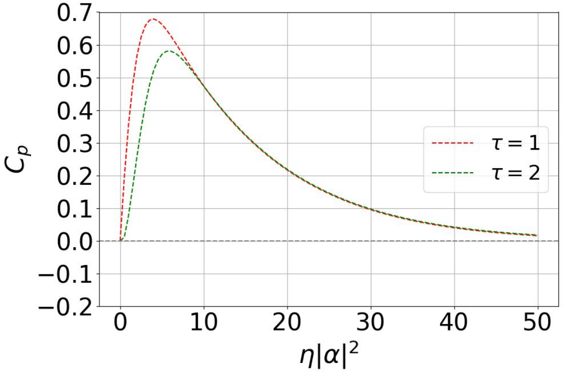
Bob's QBER, $\Delta = 0.03$



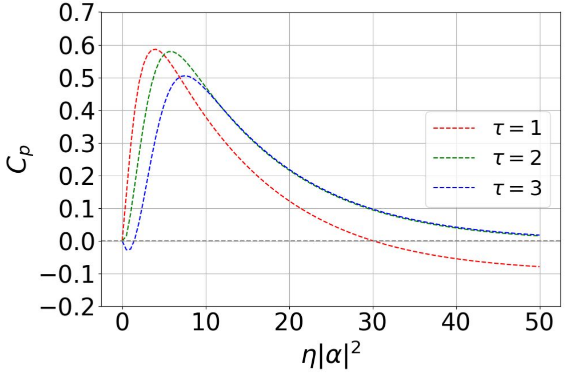
Eve's QBER

Private Capacity - OOK - $\gamma = 0.1$

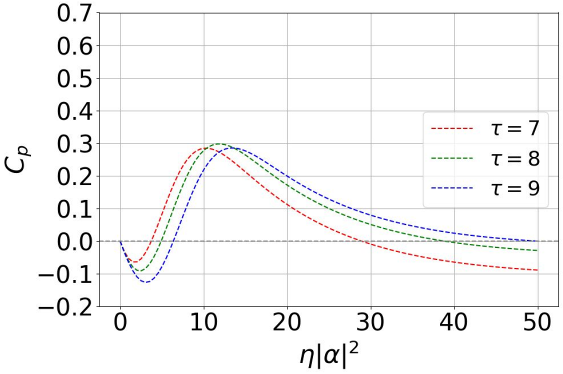
Δ = 0.0003



Δ = 0.03



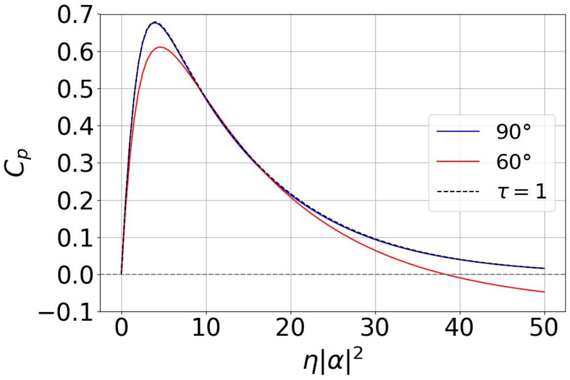
Δ = 3



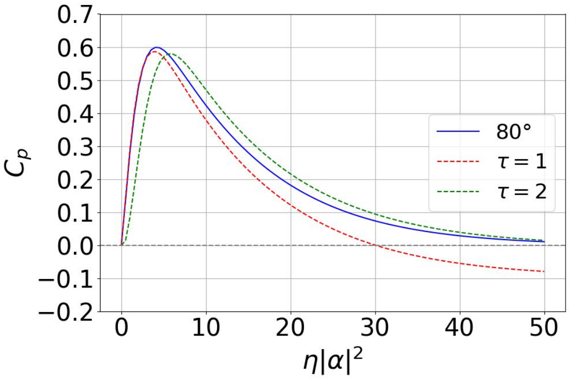
- The maximum C_p decreases with increasing photon noise, **Δ.**
- Changing the threshold allows for a higher C_p for high photon noise.

Private Capacity - Polarization - $\gamma = 0.1$

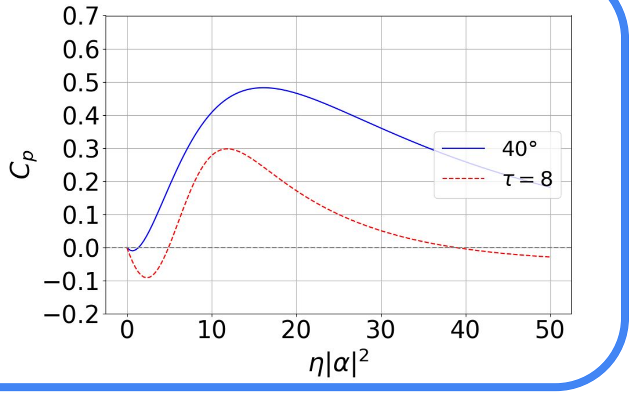
Δ = 0.0003



Δ = 0.03

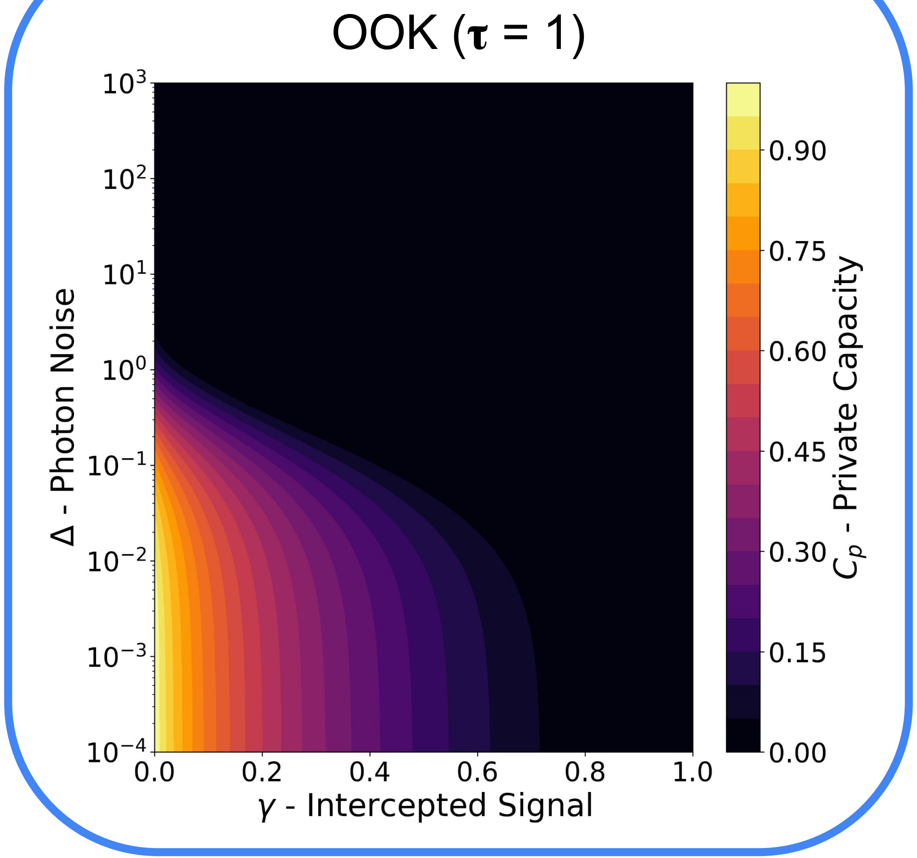


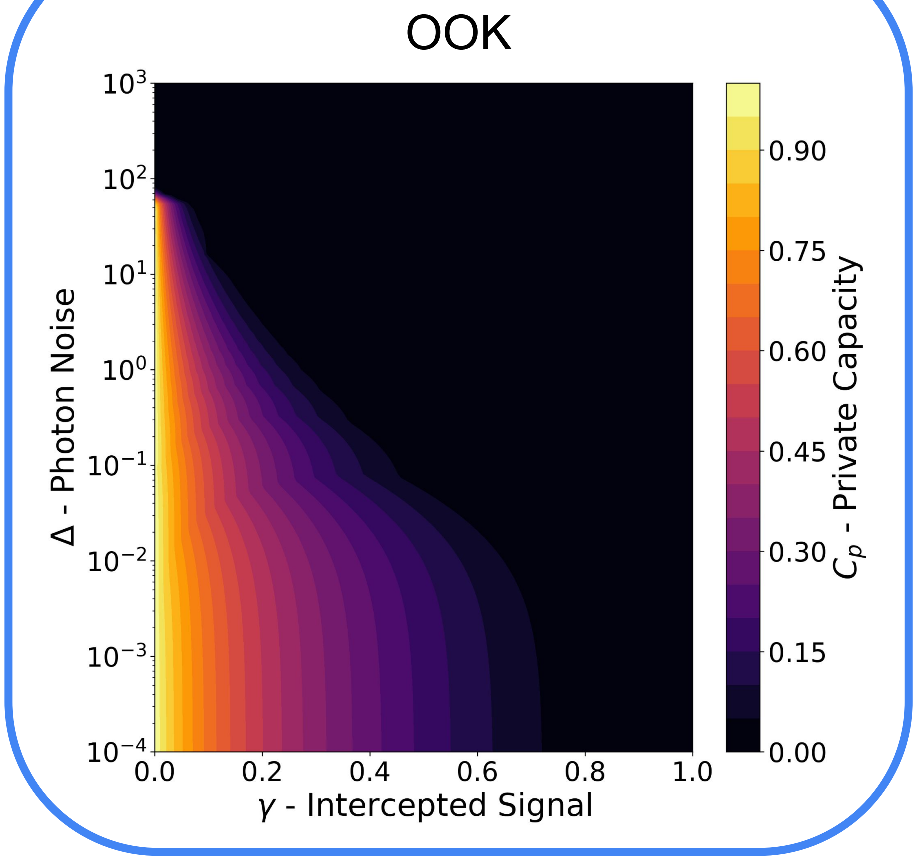
Δ = 3



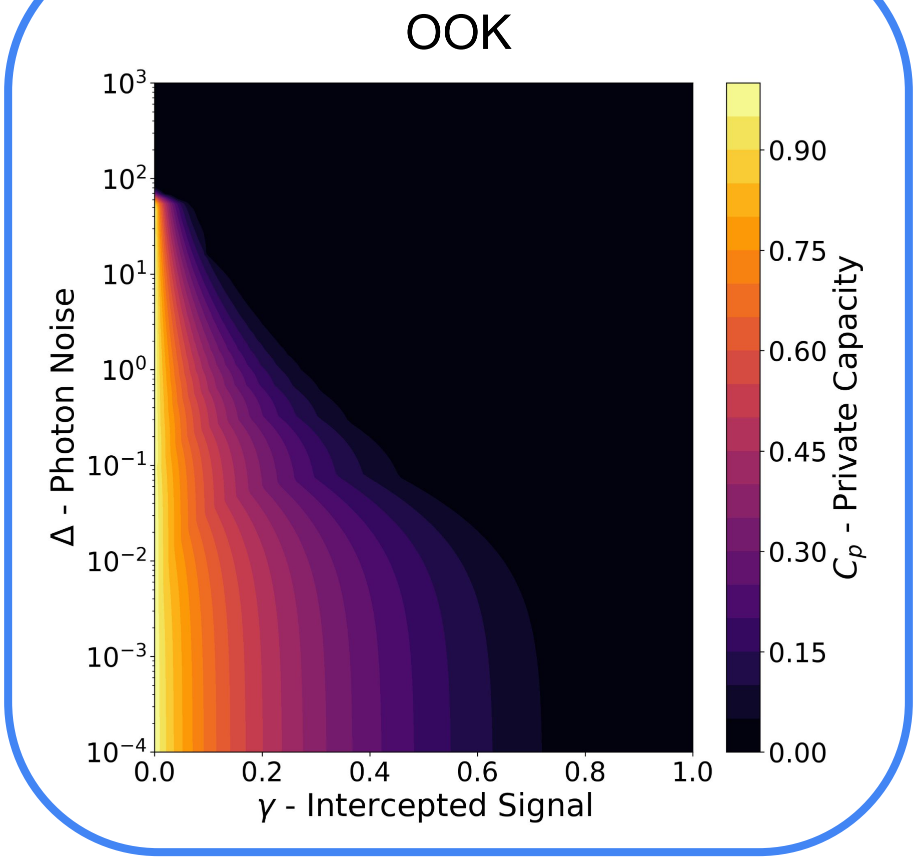
- For low photon noise, there is no advantage in using polarization encoding.
- For high photon noise the polarization encoding allows for higher private capacities.

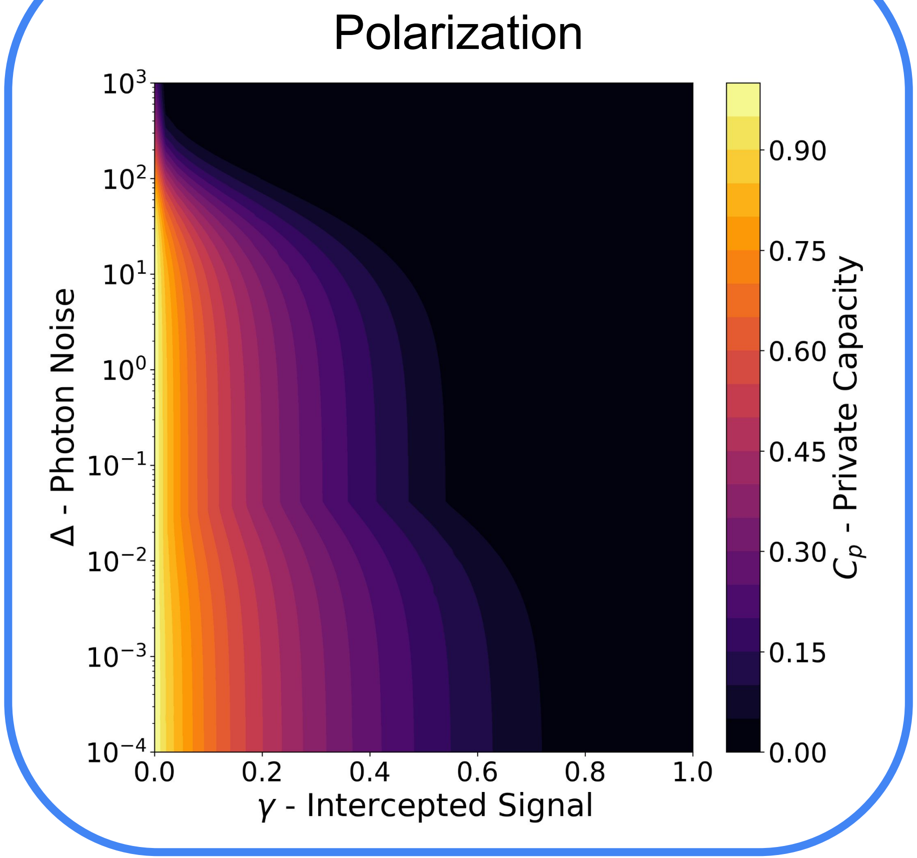
Optimal Private Capacity





Optimal Private Capacity





Conclusions

- The use of threshold choices in the discrimination step can increase the resistance to photon noise.

- Polarization encoding provides equal or better private capacities, depending on photon noise levels.

- Polarization encoding is even more resilient to photon noise, allowing for efficient communication in high photon noise regimes.

Questions?

Setup Photos