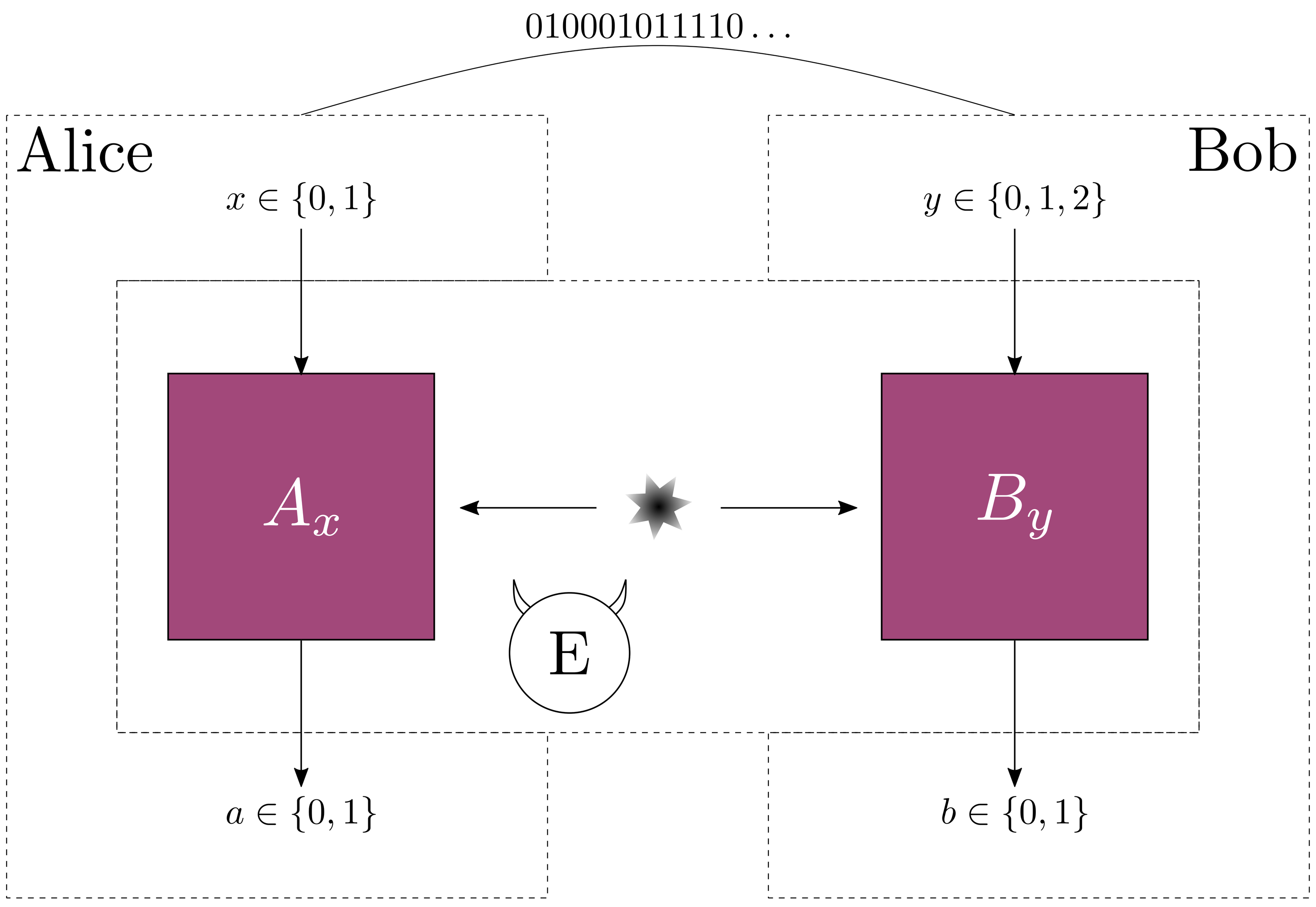
Automated design of photonic experiments for device-independent quantum key distribution

Xavier Valcarce[1], Pavel Sekatski[2], Elie Gouzien[1], Jean-Daniel Bancal[1], Nicolas Sangouard[1]

[1] Université Paris-Saclay, CEA, CNRS, Institut de Physique Théorique, 91191, Gif-sur-Yvette, France
[2] Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

Device-independent Quantum Key Distribution

Alice and Bob want to generate a secret key.
They trust quantum mechanics, their classical devices and share an authenticated channel.
They don't trust their devices (measurement and state preparation).



DIQKD Protocol [1]

1. Alice and Bob randomly pick up a measurement.
2. They collect statistics from their measurements outputs a,b.
   Test rounds: $x = \{0,1\}$ and $y = \{0,1\}$
   Key generation rounds: $x = 0$ and $y = 2$
3. After a few repetitions, they compute the CHSH score:

$$\mathrm{CHSH} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$$

4. Post-processing steps (error-correction, privacy amplificiation,...)

Key rate

Number of secure bit that can be extracted per round

$$r = \underbrace{H(A_0|E)}_{\text{Secrecy}} - \underbrace{H(A_0|B_2)}_{\text{Correctness}}$$

Lower bound (using noisy-preprocessing [2])

$$r \leq 1 - f_p(\mathrm{CHSH}) - H(A_0|B_2)$$

Photonic circuit as the implementation of choice

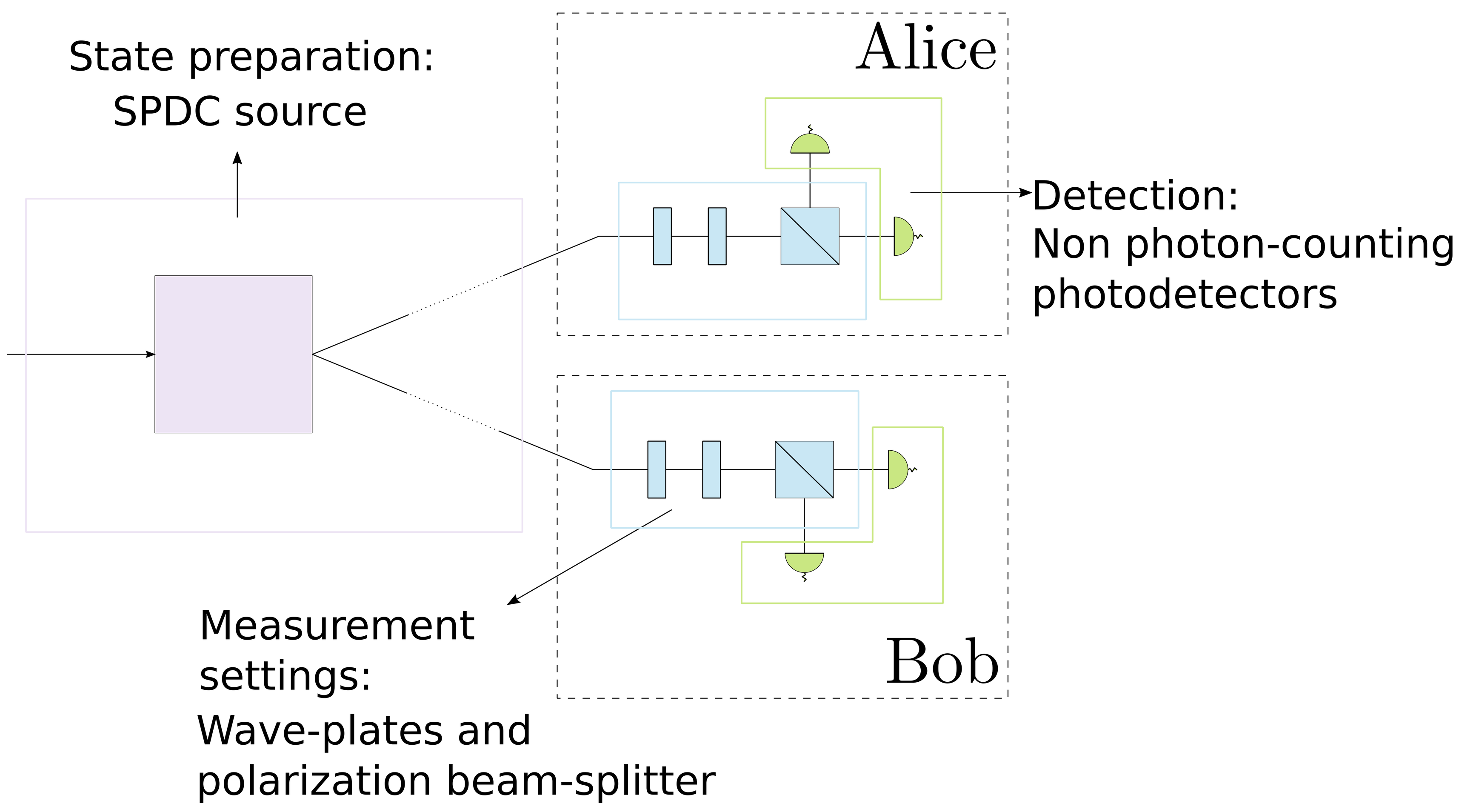
Advantages:

- High repetition rate
- Detection loophole-free Bell tests already implemented

Challenge:

- Poor efficiency (susceptible to losses)

Reference setup: Photons entangled in polarization [2,3]



Automated design

Fast and reliable simulation of quantum circuit

Squeezers, Displacements, Phase shifters, Beam splitters, ... → Gaussian processes

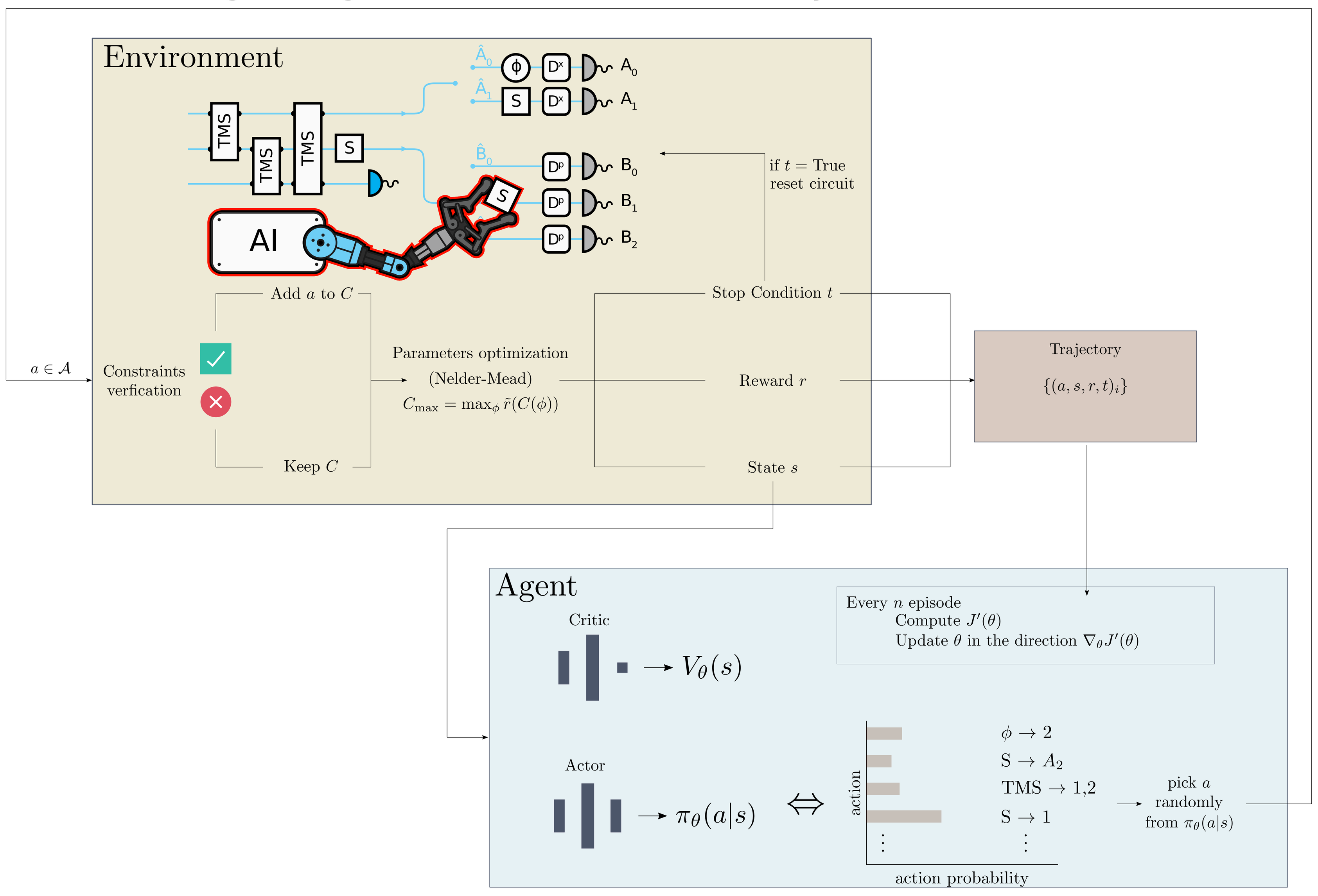
Heralded detection → Weighted sum of Gaussian states

→ QuantumOpticalCircuits.jl [4]

Exploring and learning

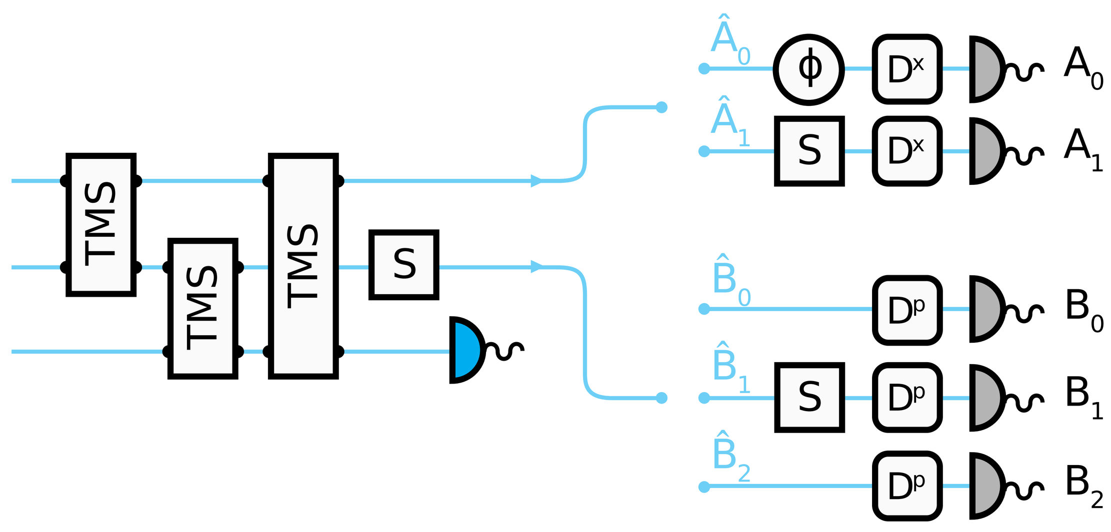
Reinforcement Learning (PPO) [5]

Teaching an agent how to solve tasks by trial and error

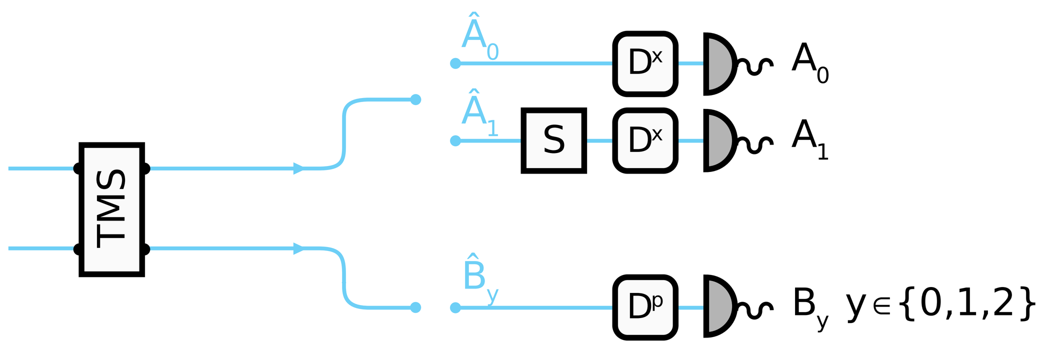


Proposed photonic implementations

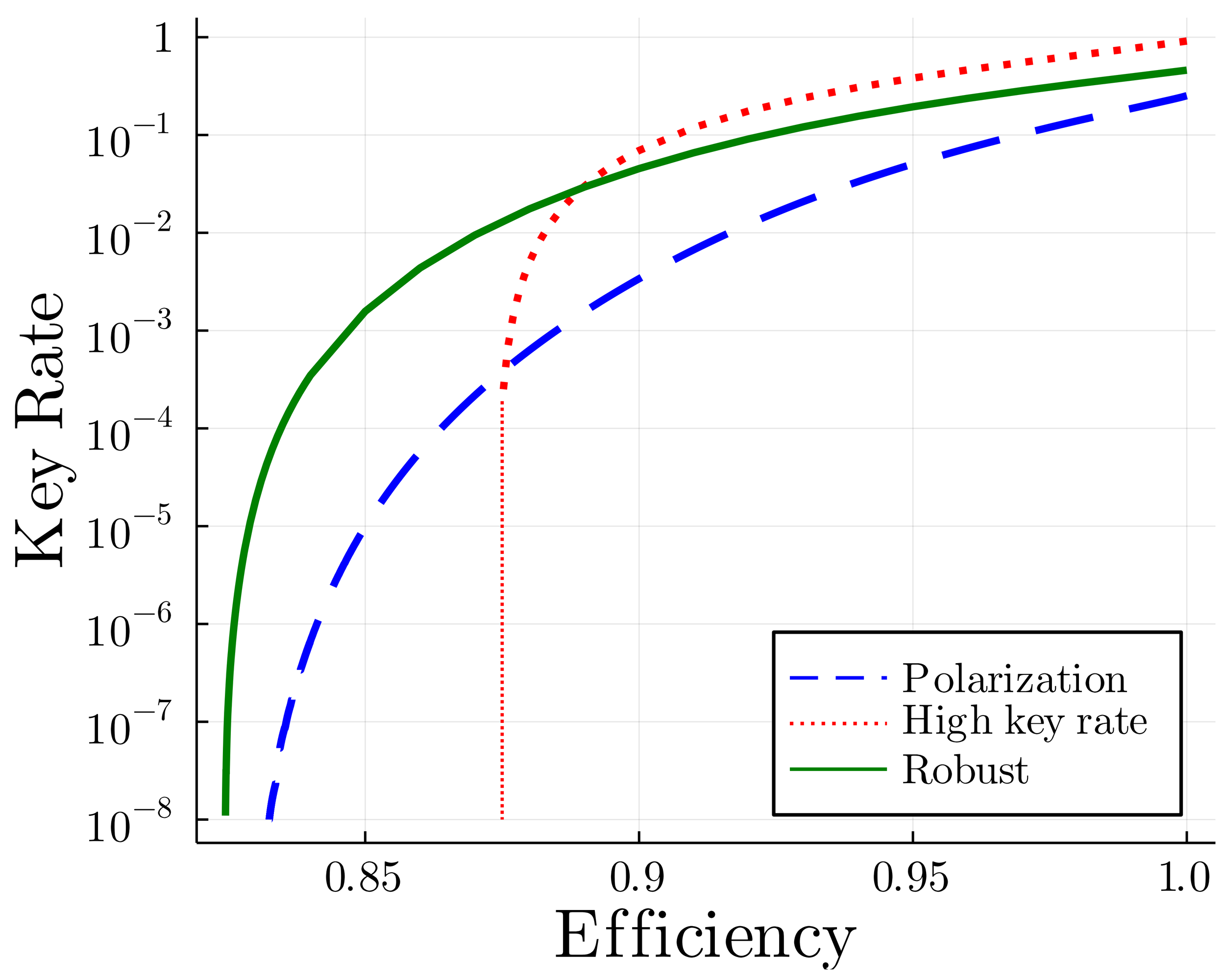
Task: Design circuit reaching the highest key rate in a lossless scenario



Task: Design circuits that tolerate the highest loss while having a key rate higher than ε



DIQKD benchmark



[1] Ekert A. (1991), **PRL** 67, 661
[2] Ho M. et al. (2020), **PRL** 124, 230502
[3] Caprara Vivoli V. et al. (2015), **PRA** 91, 012107
[4] https://gitlab.com/plut0n/QuantumOpticalCircuits.jl
[5] Schulman J., et al. (2017), arXiv:1707.06347
[6] Valcarce X. et al., to be published