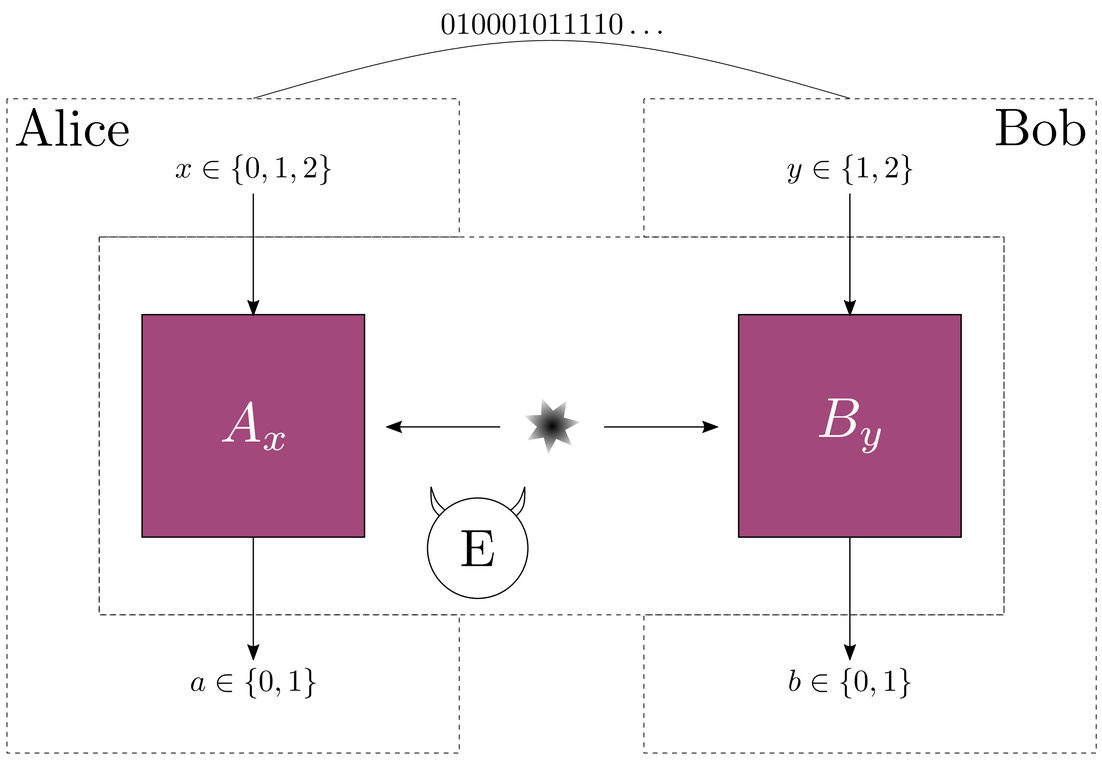
Automated design of photonic implementations for device-independent quantum key distribution

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 and share an authenticated classical channel of communication.
They don't trust their devices (measurement and state preparation).



DIQKD Protocol [1]

1. Alice and Bob randomly pick up a measurement.
2. In case A0 was picked by Alice, Alice indicates it to Bob so he will measure B1. These outputs will constitute the raw key.
3. Alice and Bob measures and store outputs a,b.
4. After a few repetitions, they share relevant information to compute the CHSH score:

$$\mathrm{CHSH} = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle$$

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

Key rate

Number of secure bit that can be extracted per round

$$r = H(B_1|E) - H(B_1|A_0)$$

$H(B_1|E)$: Secrecy — $H(B_1|A_0)$: Correctness

Lower bound (using noisy-preprocessing [2])

$$r \leq 1 - f_p(\mathrm{CHSH}) - H(\hat{B}_1|A_0)$$

Photonic circuit as the implementation of choice

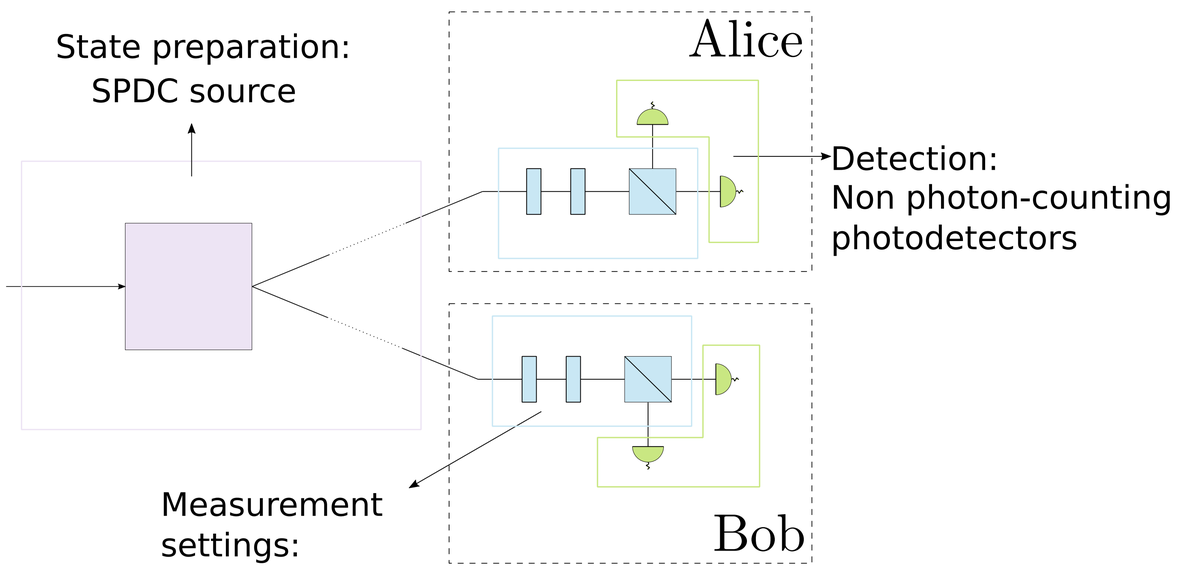
Advantages:

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

Incovenient:

- 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

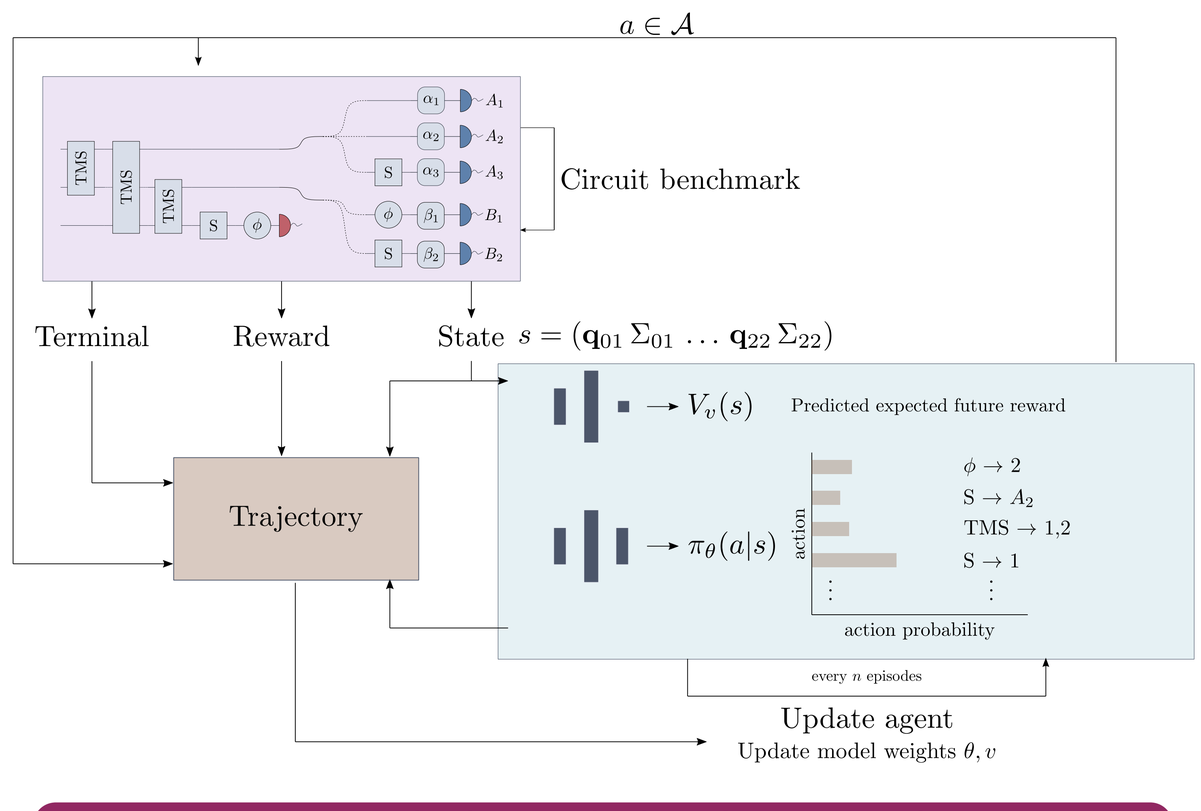
Heralded detection → Weighted sum of Gaussian state

→ QuantumOpticalCircuits.jl [4]

Exploring and learning

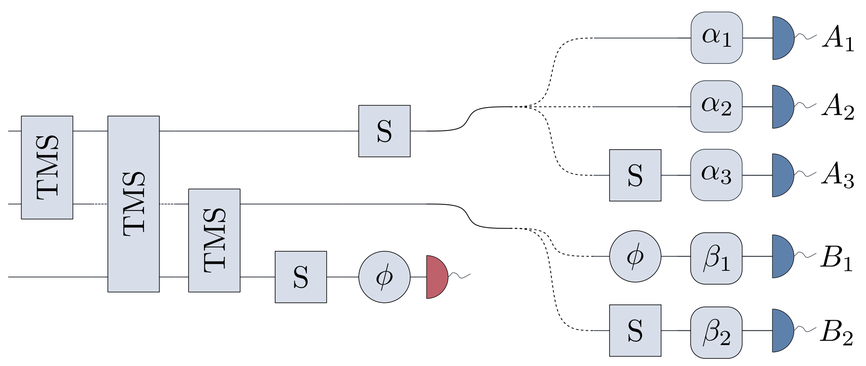
Reinforcement Learning (PPO) [5]

Teaching an agent how to solve tasks by trial and error.

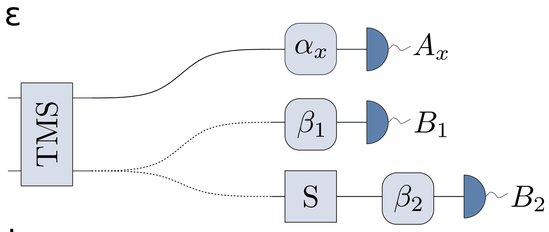


Proposed photonic implementation

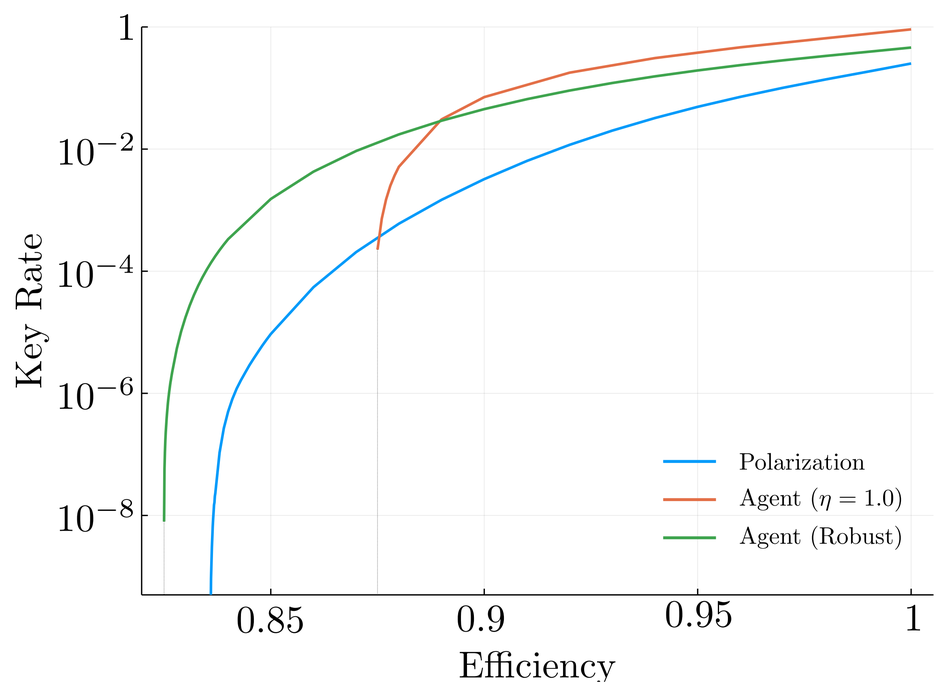
Task: Design circuit reaching the highest key rate in a perfect scenario



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