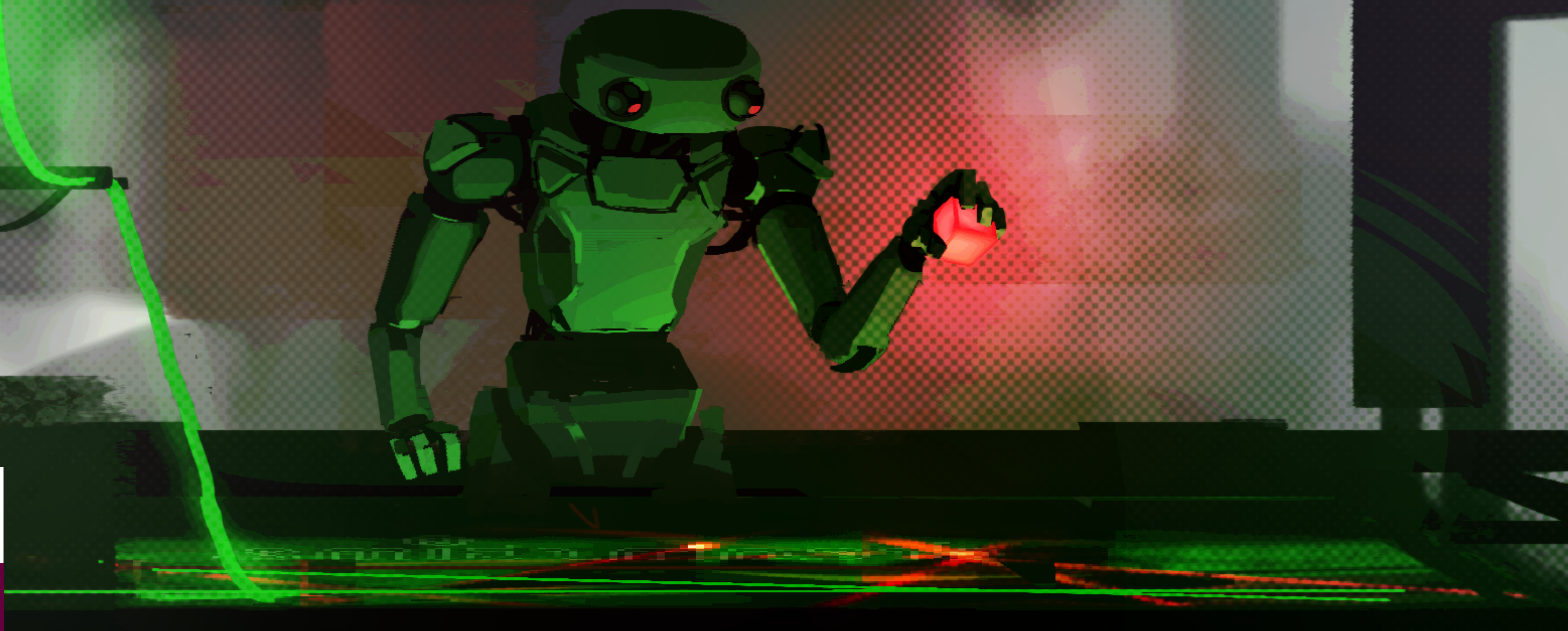
Automated design of photonic experiments for device-independent quantum key distribution

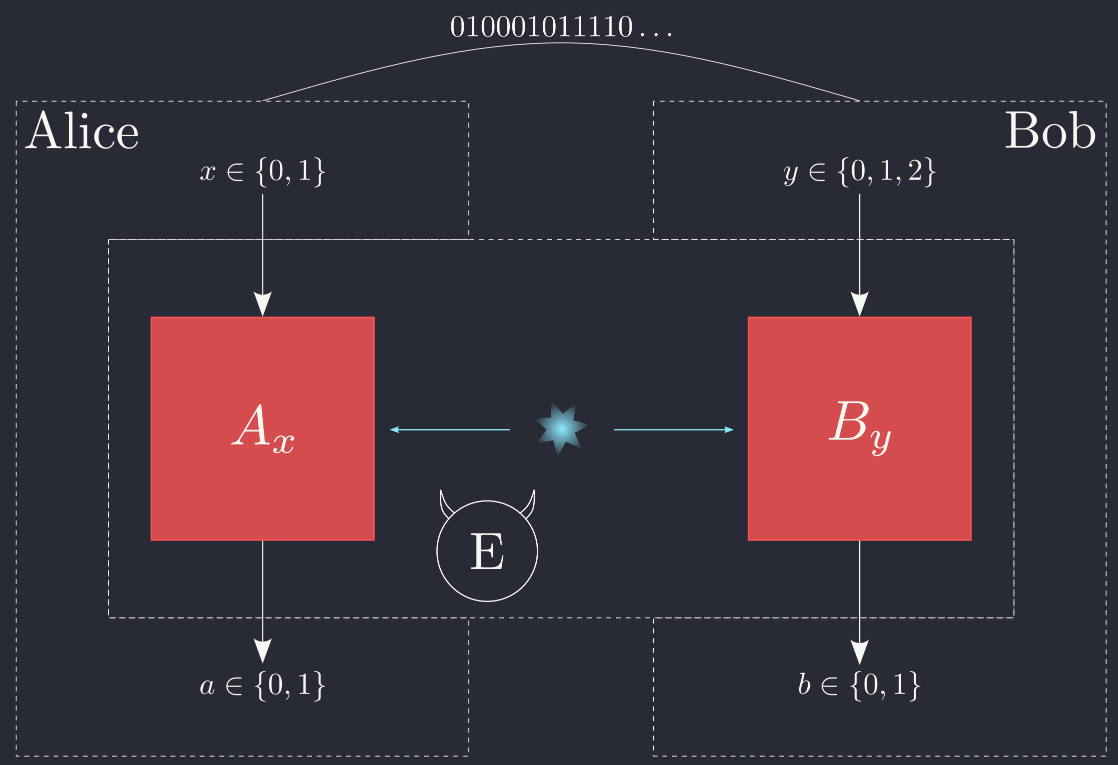
Xavier Valcarce[1], Pavel Sekatski[2], Elie Gouzien[1], Alexey Melnikov[3], Nicolas Sangouard[1]

[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
[3] Terra Quantum AG, 9000 St Gallen, Switzerland

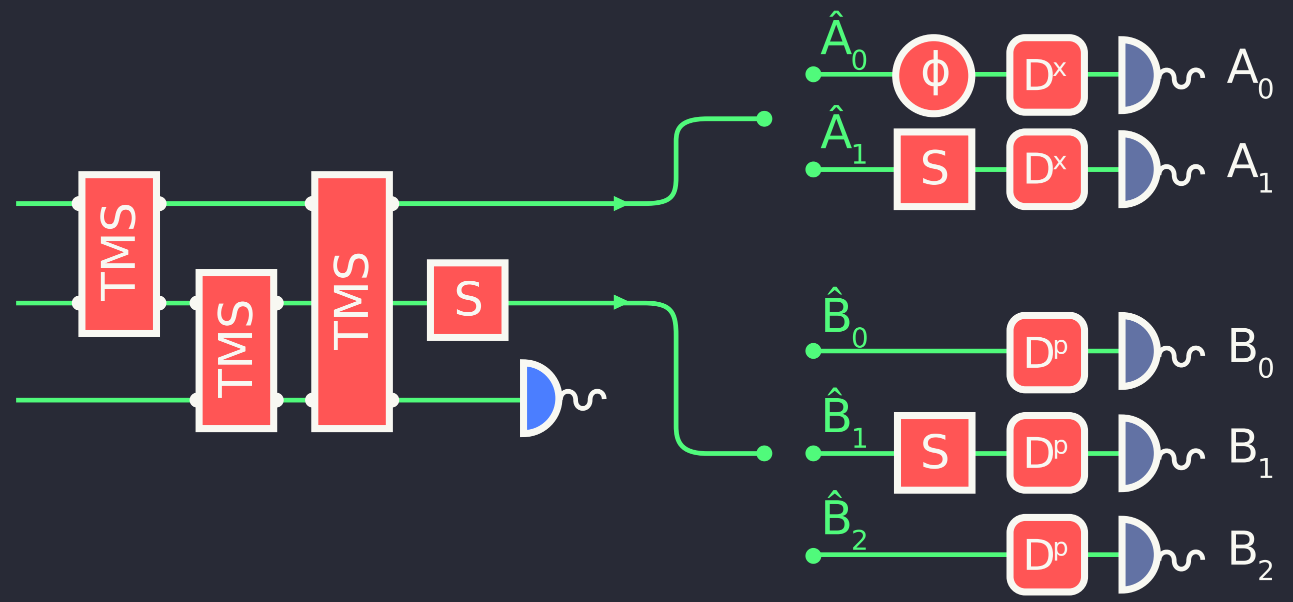


arXiv:2209.06468

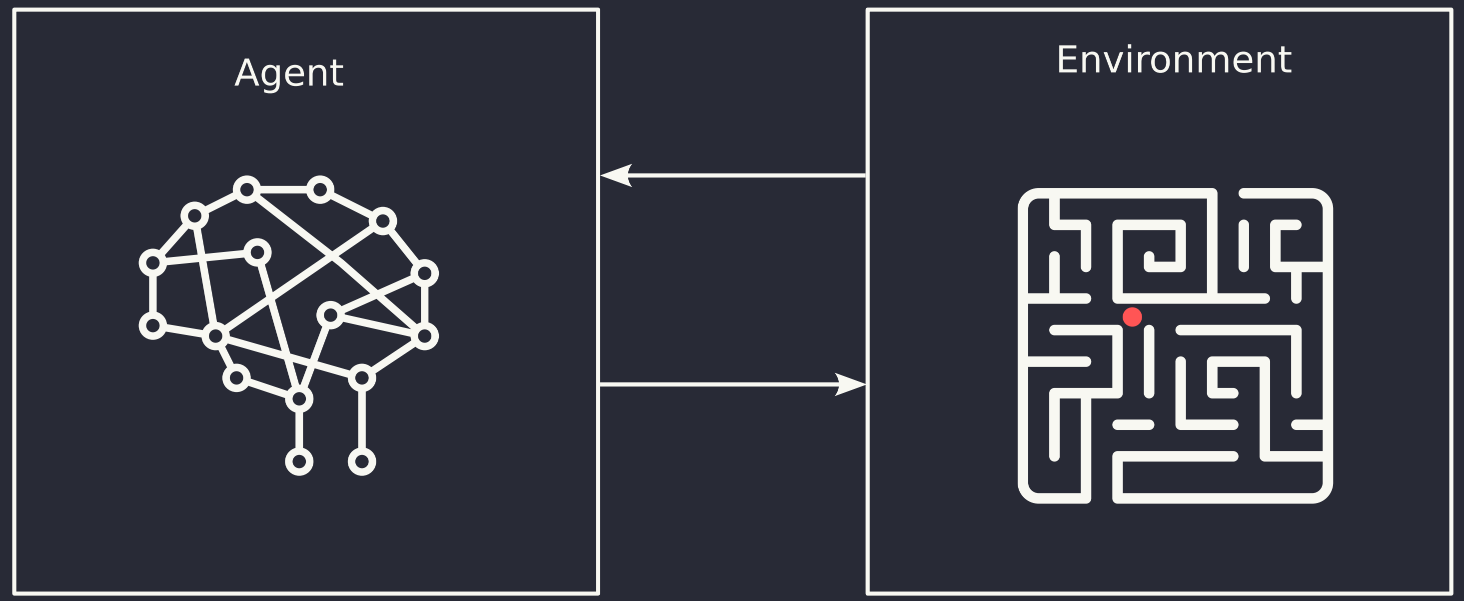
From Classical to Quantum Cryptography



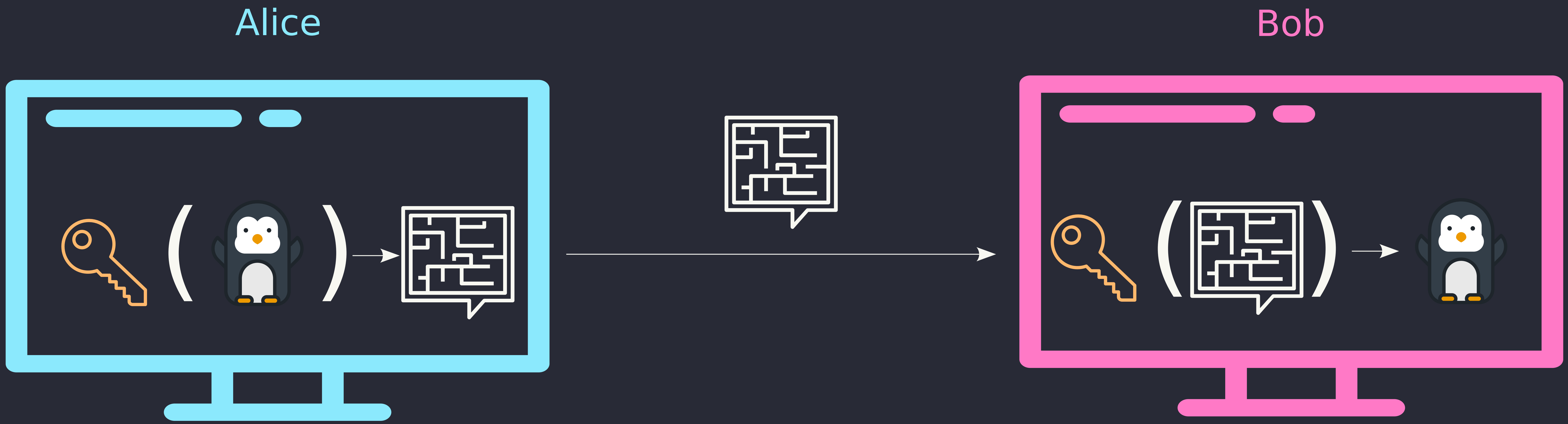
Quantum Optical Circuits



Reinforcement Learning



From Classical cryptography...



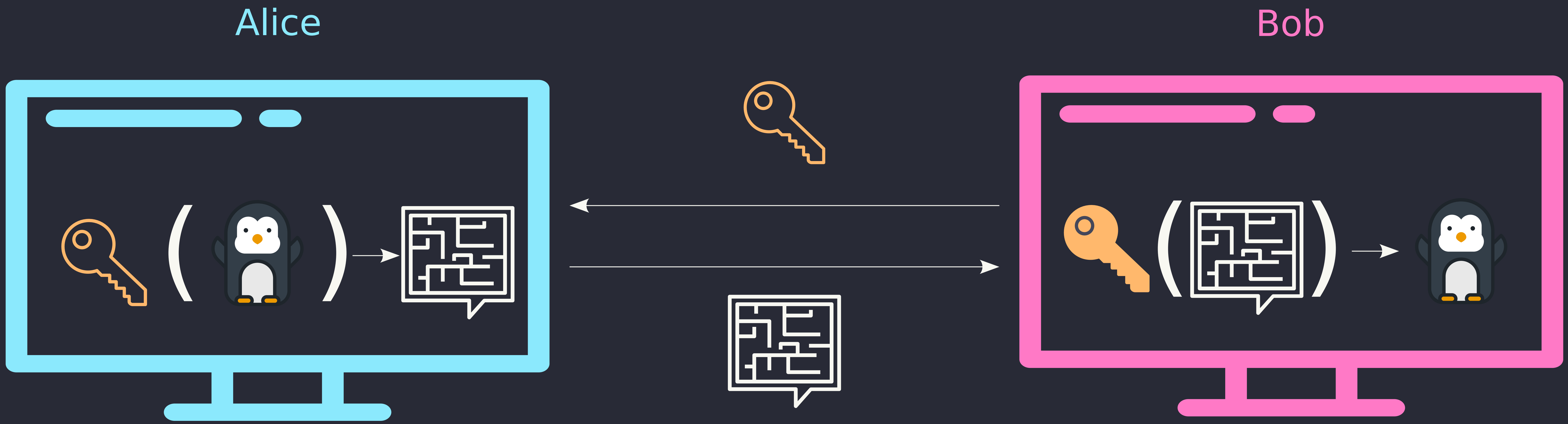
Symmetric cryptography:

Alice and Bob share the same key used to en/de-crypt the message

✔ Information-theorietically secure

✘ Impractical: size( ) == size( ), key has to be preshared

From Classical cryptography...



Asymmetric cryptography:

Bob has a private key and shares a public key

✓ Practical, no need for a pre-shared keys of size ( )

✗ Cryptography proof relying on computational assumption
Can be hacked using a quantum computer [Gouzien et. al., PRL 127 (14)]

... to Quantum Cryptography

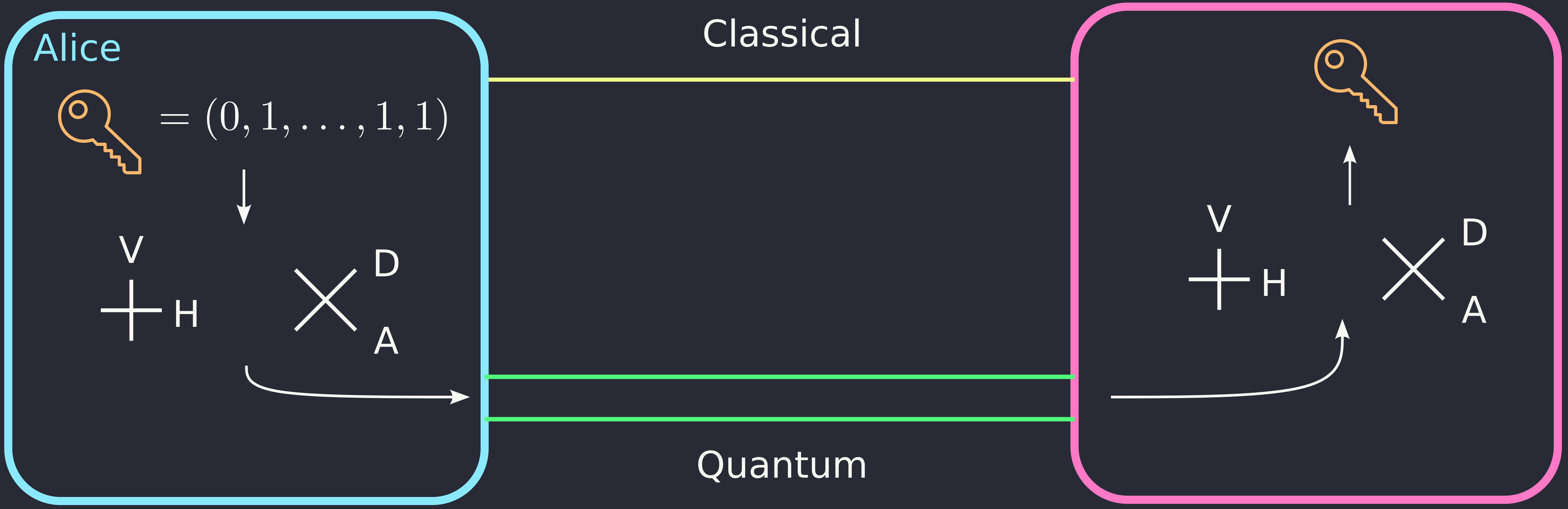
Quantum key distribution:

Use quantum ressources to generate and distribute a symmetric key

Key is provably secure (unkown to a third party, Eve)

BB84:

Key encoded in the polarization of photons



QKD relies on a small set of assumptions:

- ✓ The devices used to generate the key behave according to quantum theory
- ✓ Alice and Bob have access to random numbers
- ✓ Alice and Bob labs are isolated (no information leakage)
- ✓ Classical information is performed on trusted computers
- ✗ Their quantum devices are trusted and perfectly calibrated

→ Can be hacked (side channel attack) [F. Xu et al., Rev. Mod. Phys. 92]

Device-independent quantum key distribution

Device-independent:

No assumptions made on the quantum devices

DIQKD, principles:

Entanglement-based

Maximally entangled state

Measurement outcomes are unpredictible to any third party

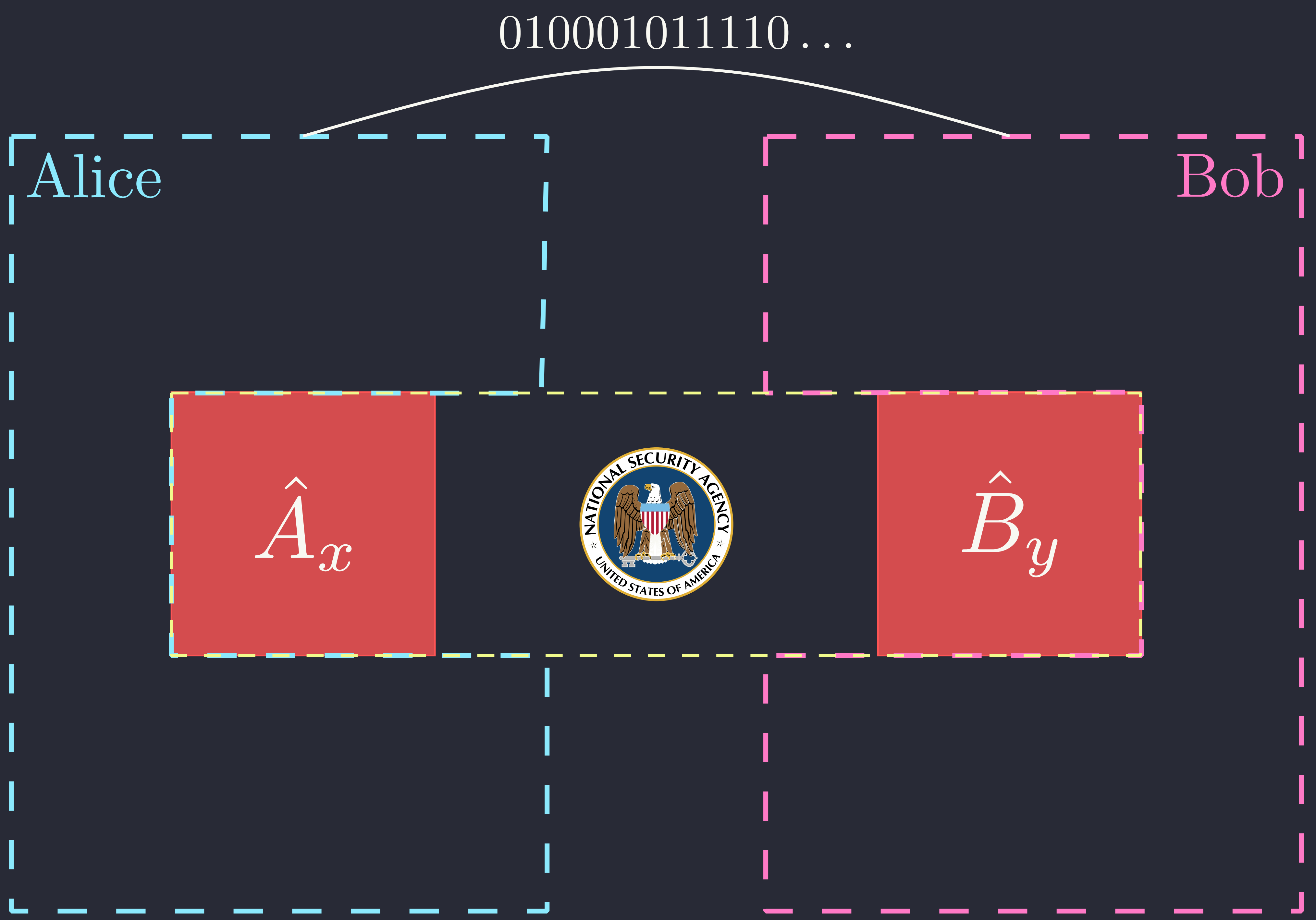
H(🔑 |)=1

Measurement outcomes are strongly correlated

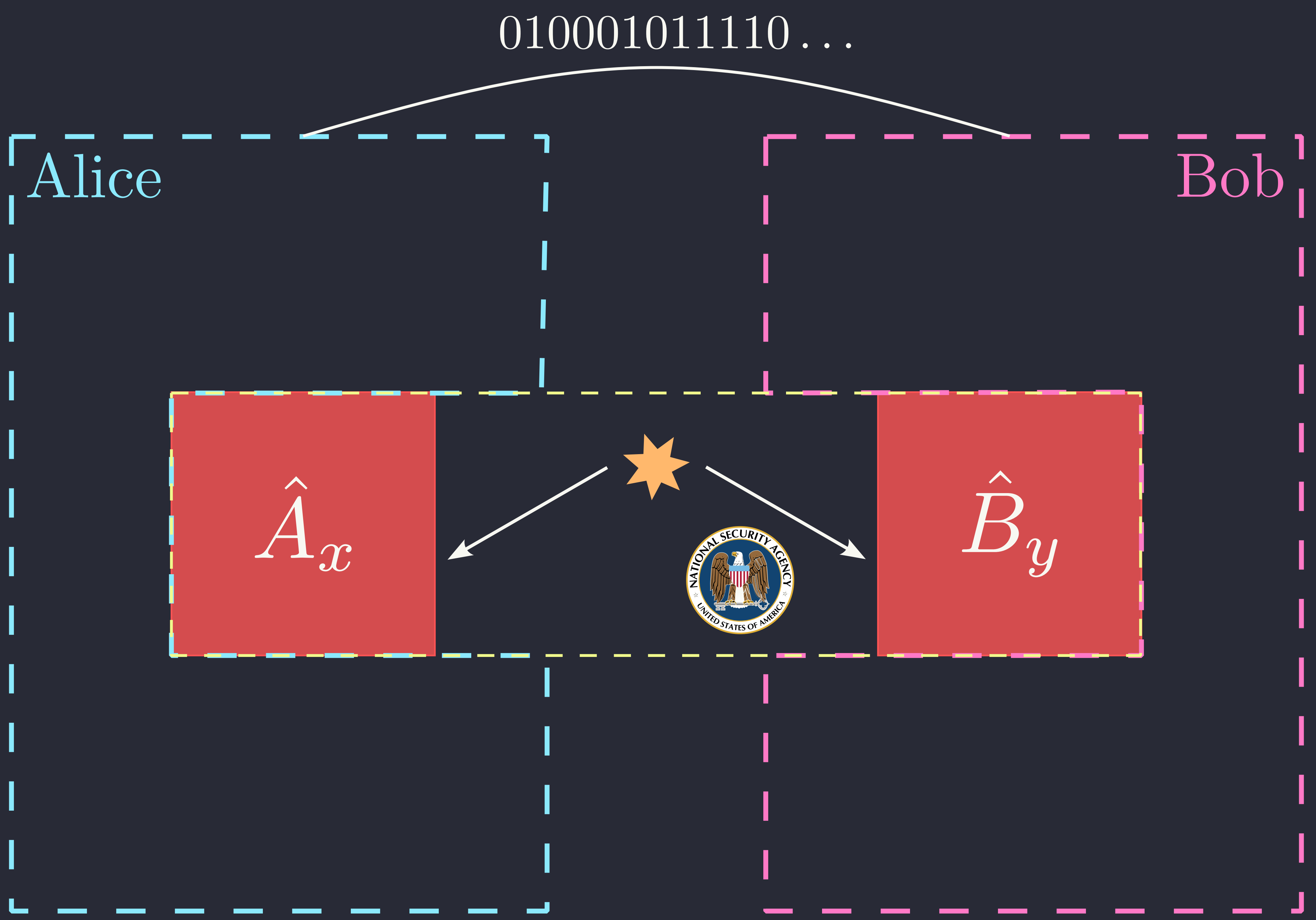
H(🔑 |B)=0

Bell tests are used as a security statement

DIQKD protocol

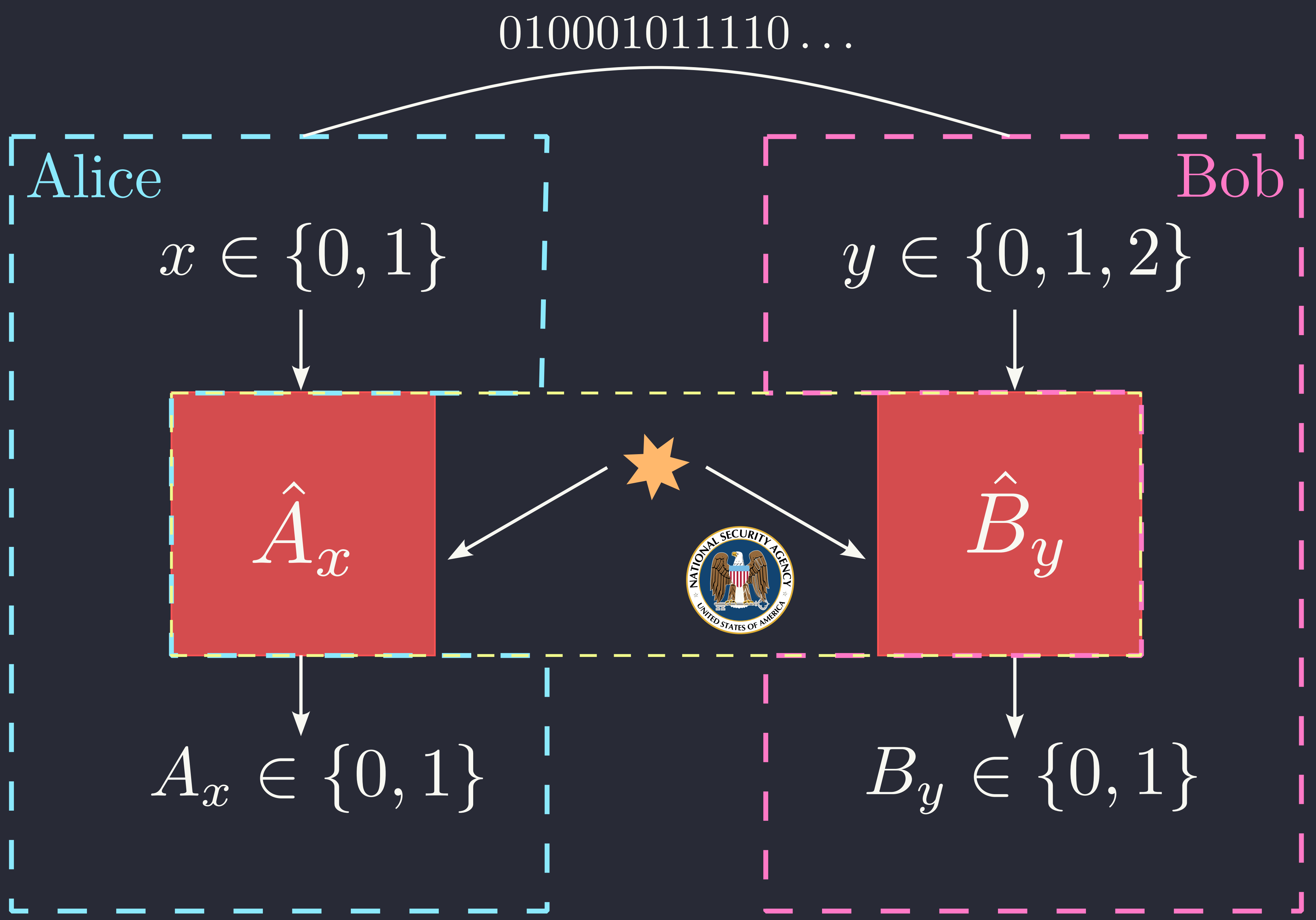


DIQKD protocol



At each round an entangled state is distributed to Alice and Bob

DIQKD protocol



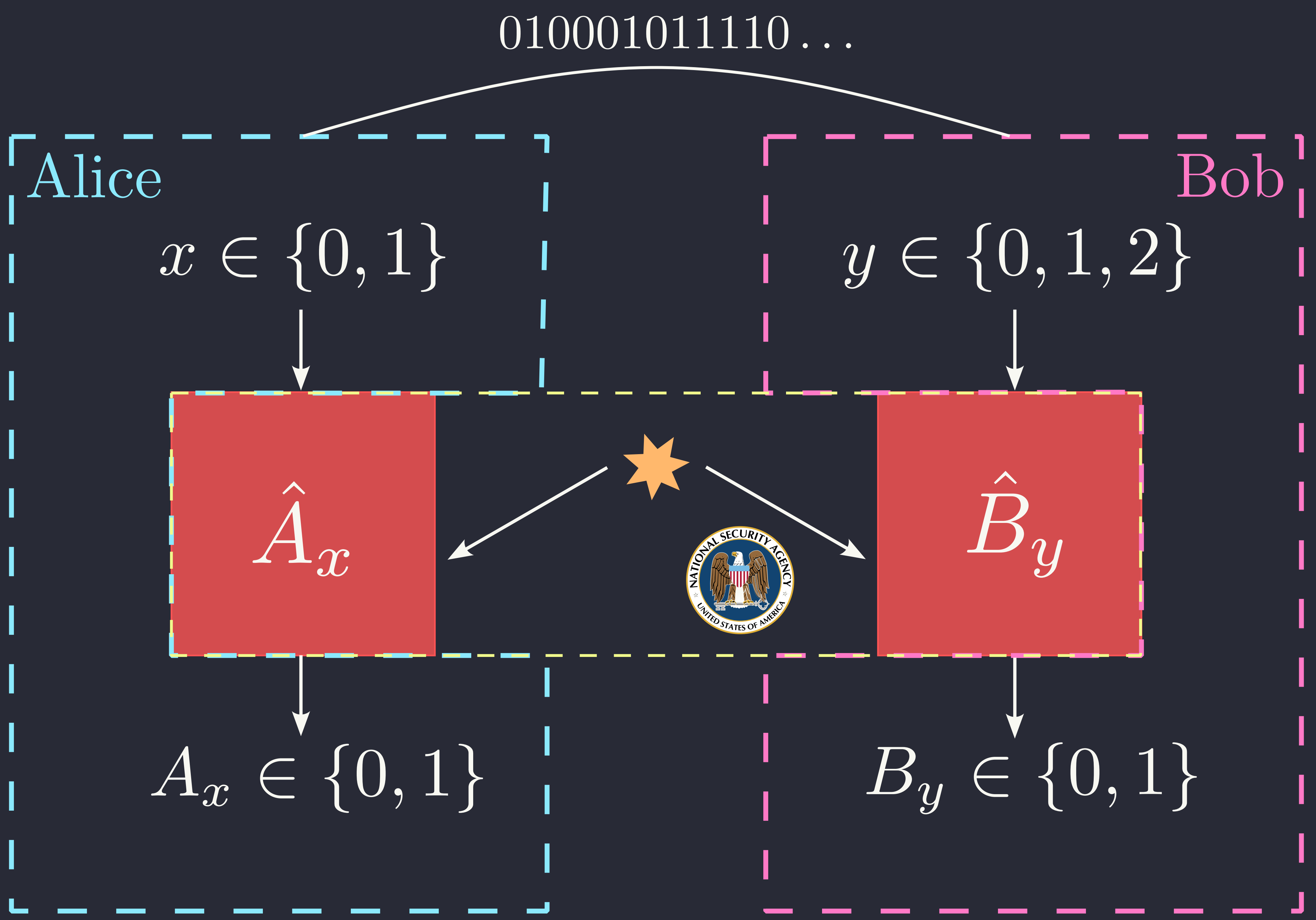
At each round an entangled state ✸ is distributed to Alice and Bob

Alice and Bob randomly chose a measurement setting x, y

They measure ✸ using measurements $\hat{A}_x, \hat{B}_y$

Outcomes A_x, B_y are recorded

DIQKD protocol



Two types of rounds:

Test round ⟶ Bell test

$\hat{A}_0, \hat{A}_1, \hat{B}_0, \hat{B}_2$ are used to compute the CHSH score

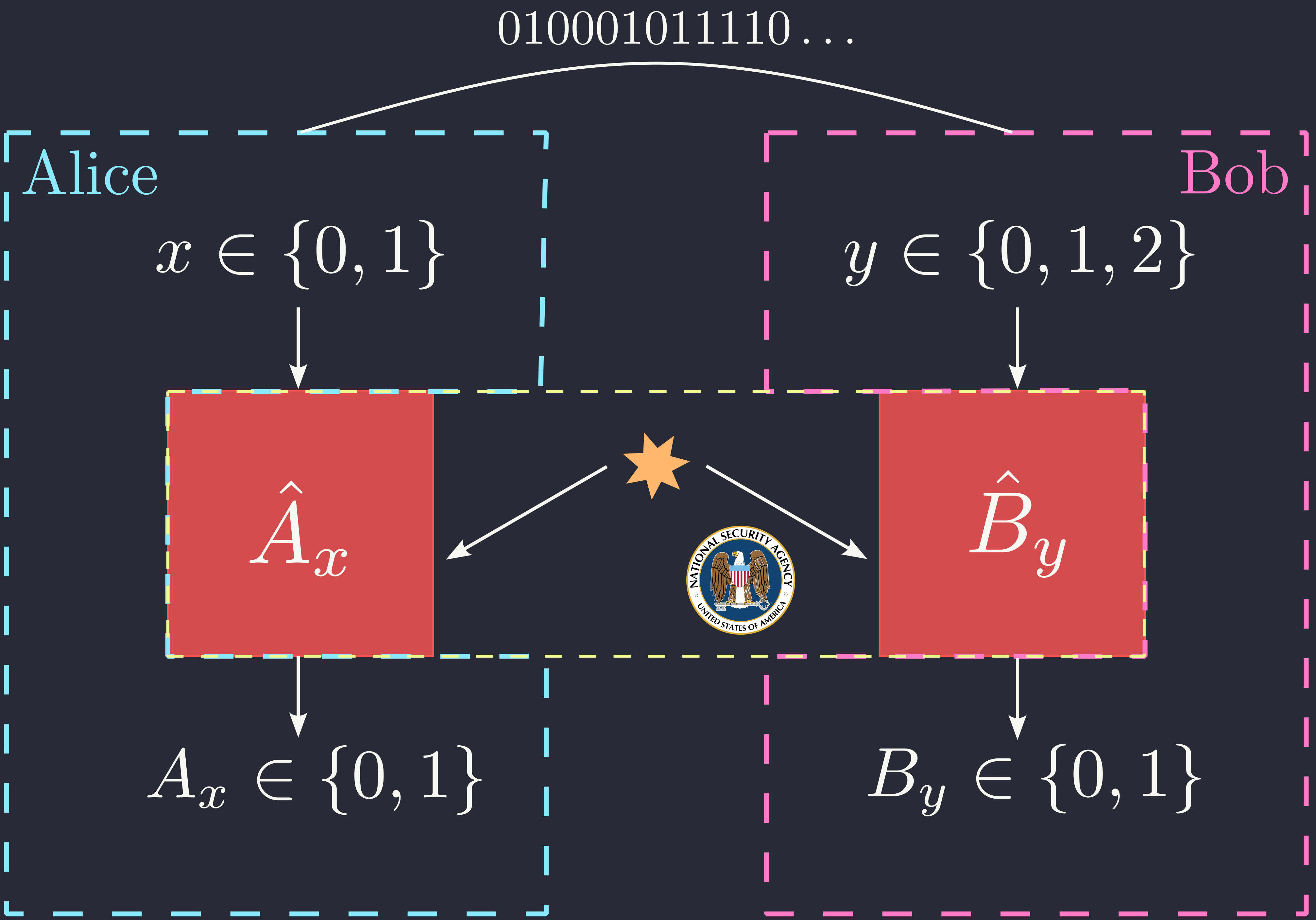
$$S = \langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_0 \hat{B}_1 \rangle + \langle \hat{A}_1 \hat{B}_0 \rangle - \langle \hat{A}_1 \hat{B}_1 \rangle$$

Key generation round ⟶ key

key generated from A_0

Bob tries to guess key using B_2

DIQKD protocol



Key rate: number of secure key bit that can be extracted per round

In the assymptotic limit of a large number of round

can be bounded using the CHSH score

$$\leq 1 - f(S)$$

DIQKD Implementation

What's needed:

- Generation of entangled states to obtain high CHSH score and correlated keys
- High frequency of state generation to obtain a sufficient number of round in a limited time

Proof-of-concept

Trapped ion

- first DIQKD experiment
- [D. Nadlinger et al., Nature 607, 682]

Single atom

- extend DIQKD over ~100m
- [W. Zhang et al., Nature 607, 687]

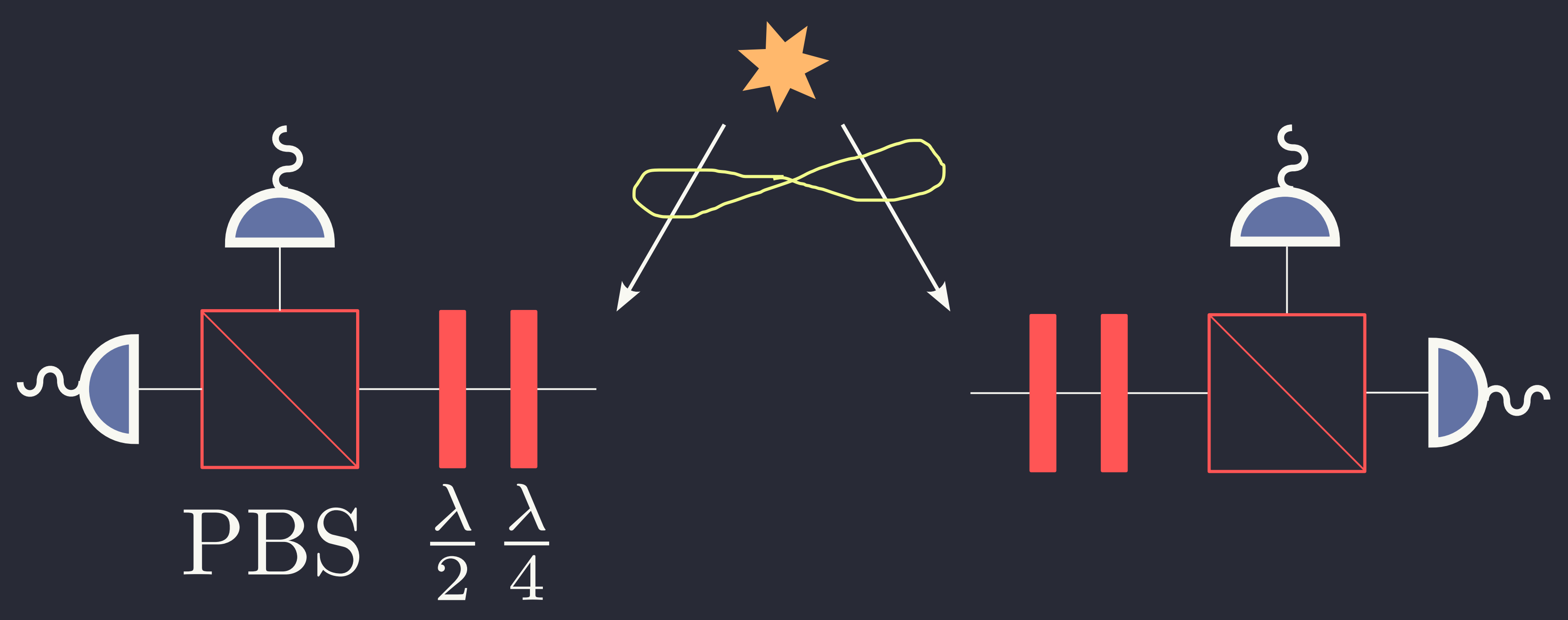
Practical / Commercial

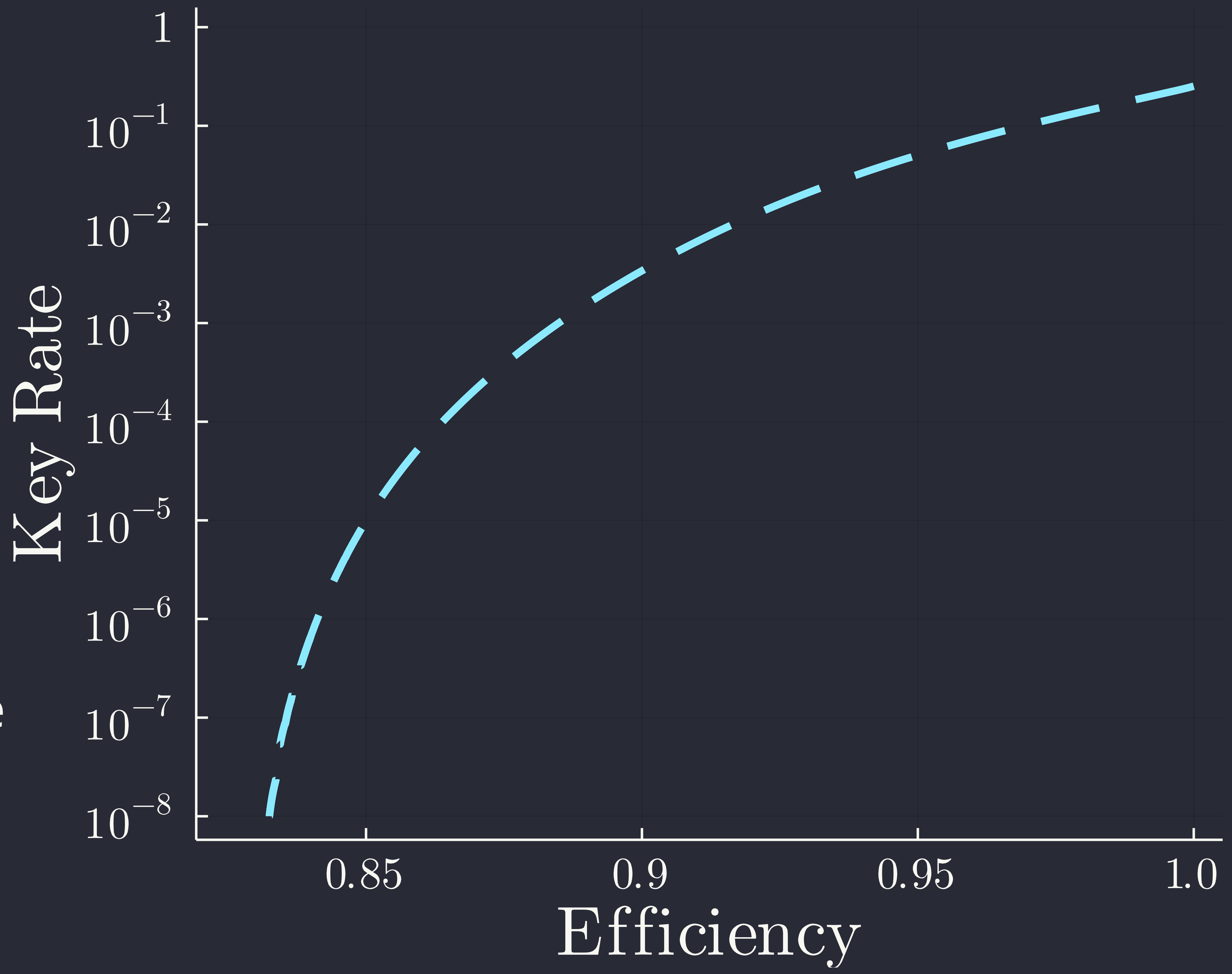
Photonic plateform seems promising

- ✓ Bell-CHSH game already implemented
- ✓ High state-generation rate
- ✓ Capacity to implement complex circuit
- ✗ Low CHSH score
- ✗ Susceptible to losses

A DIQKD Implementation: SPDC source

"Standard" implementation to realize Bell tests is using a SPDC source generating photons entangled in polarization



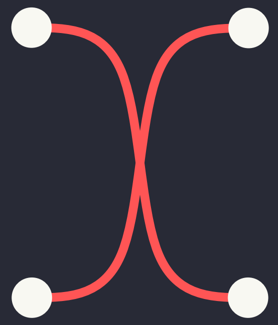


Yield a key rate of ~0.2522 in the ideal case

Positive key rate for min ~82.6% efficiency

Quantum Optics: operations

Two-mode Squeezer



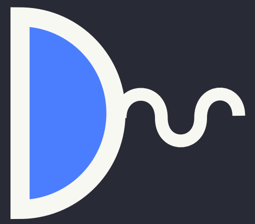
Beam-splitter

Single-mode squeezer

Phase-shifter

Displacement (in p)

Displacement (in x)



Heralding

Photo-detection (NPNR)

Quantum Optics: simulation

Bosonic mode are characterized by ladder operators $a_i, a_i^\dagger$

or, alternatively, with $\hat{x}_i = \frac{a_i^\dagger + a_i}{2}$ and $\hat{p}_i = i\frac{a_i^\dagger - a_i}{2}$

For a n-mode system, we have $\mathbf{q} = (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_n, \hat{p}_n)$

Gaussian state can be represented using $2n^2+3$ real parameters:

2n displacement vector

$$\mu$$

$$\mu_i = \langle q_i \rangle$$

2nx2n covariance matrix

$$\Sigma$$

$$\Sigma_{ij} = \frac{1}{2}\langle q_i q_j + q_j q_i \rangle$$

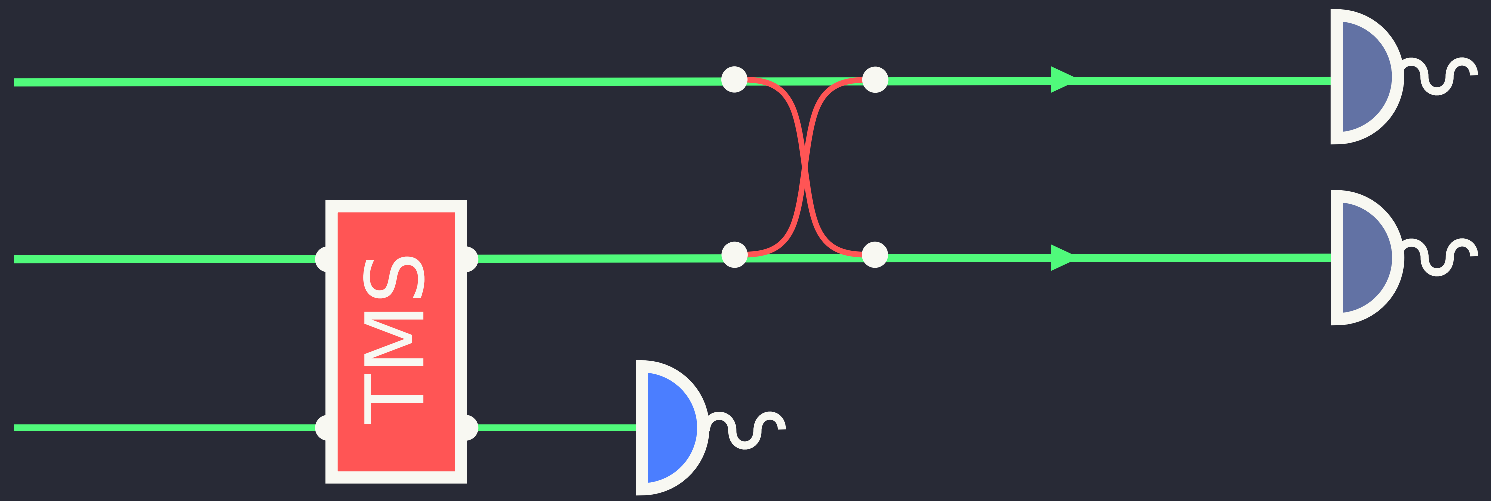
Gaussian operations acts following $T : (\mu, \Sigma) \to (M\mu + \vec{d}, M\Sigma M^T)$

Heralding operation are non-Gaussian but the resulting (conditionned) state is a sum of Gaussian state

QuantumOpticalCircuits.jl

Julia pkg to simulate Gaussian optics , heradling , and photondetection

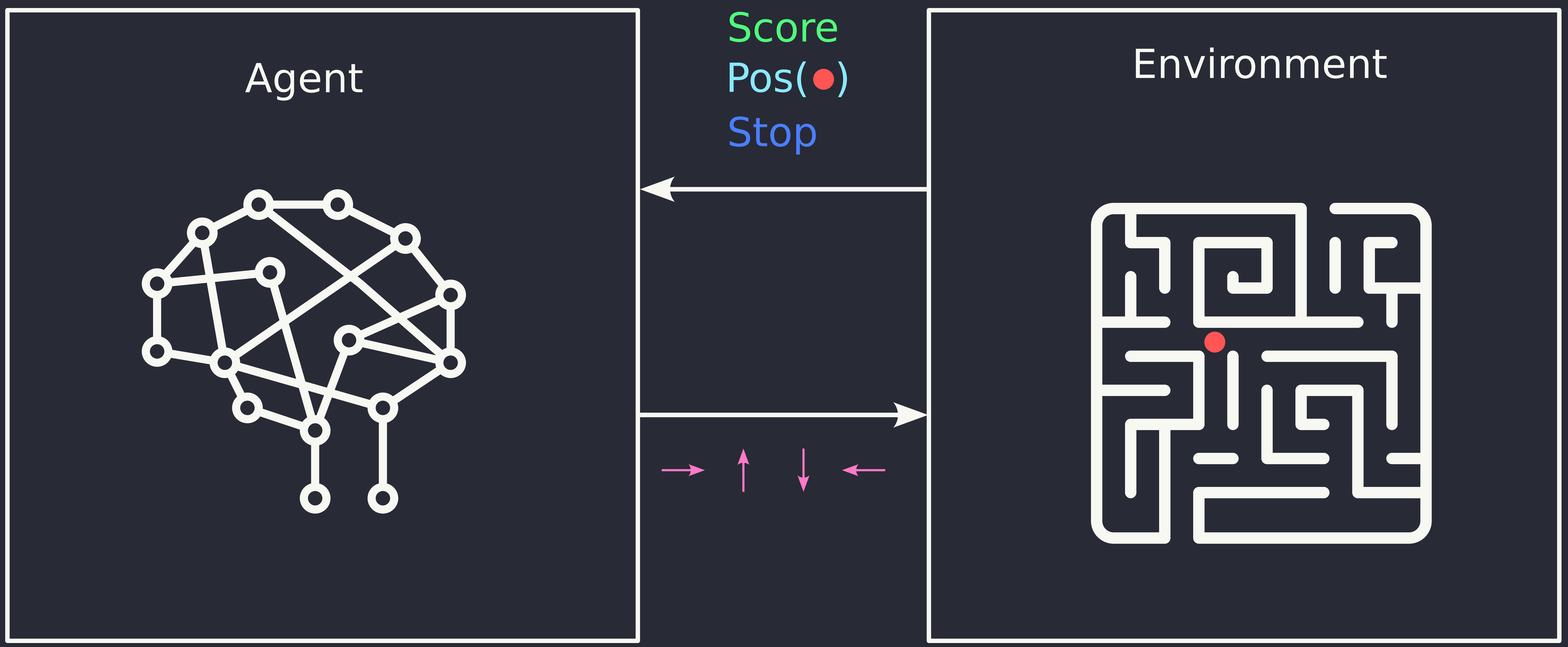
Available on github.com/xvalcarce/QuantumOpticalCircuits.jl




```
julia> using QuantumOpticalCircuits

julia> state = PseudoGaussianState(3);

julia> state = state |> TMS(0.01)(2,3) |> Heralding(3) |> BS(π/4)(1,2);

julia> p_click_1 = state |> PhotonDetector(1,η=0.8)
0.4000239998415148

julia> p_click_2 = state |> PhotonDetector(2,η=0.8)
0.4000239998415148
```

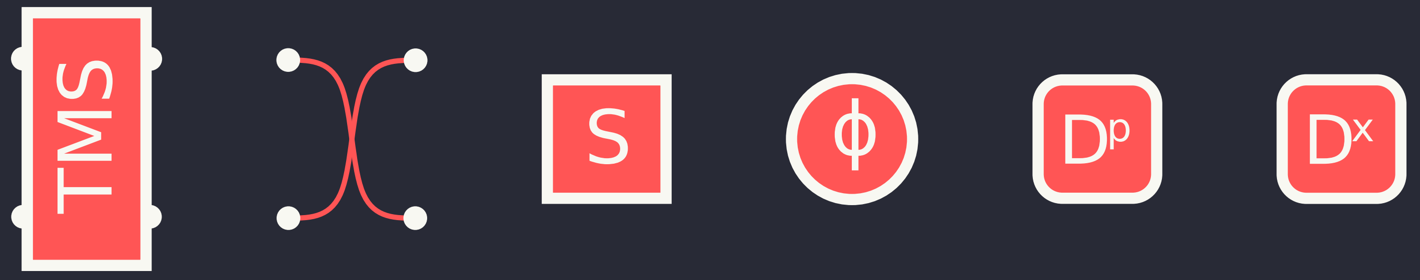
Reinforcement Learning

Reinforcement Learning aims at learning a task (game) by trial-and-erros



Reinforcement Learning for photonic DIQKD

Environment: n-mode Optical Circuits

Actions: 

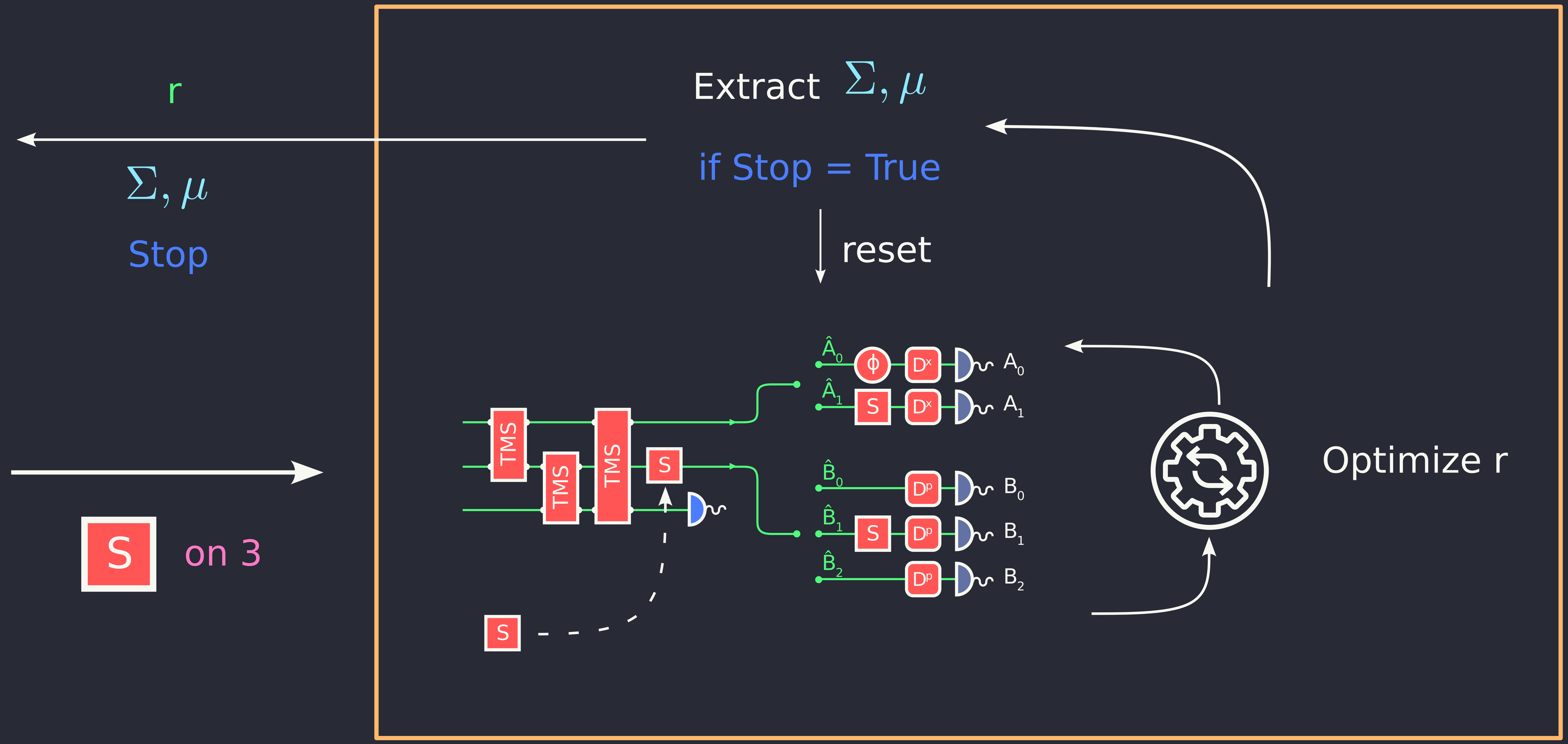
acting on mode i (or i,j)

Score: $r = H($$|$ NATIONAL SECURITY AGENCY, UNITED STATES OF AMERICA $) - H($$|B)$

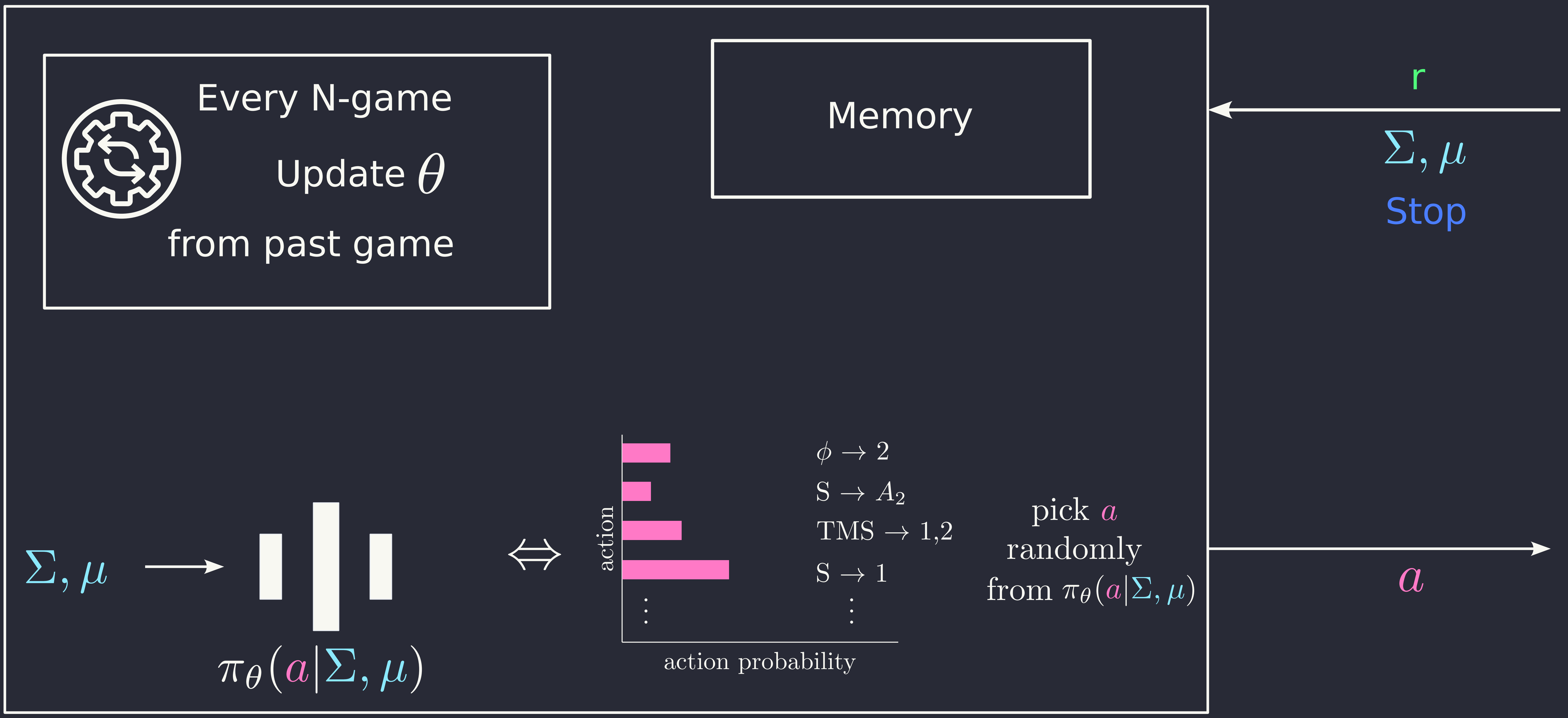
Stop: Maximum # gate reached || r = 1

State: Gaussian state, i.e. Σ, μ

Reinforcement Learning for photonic DIQKD

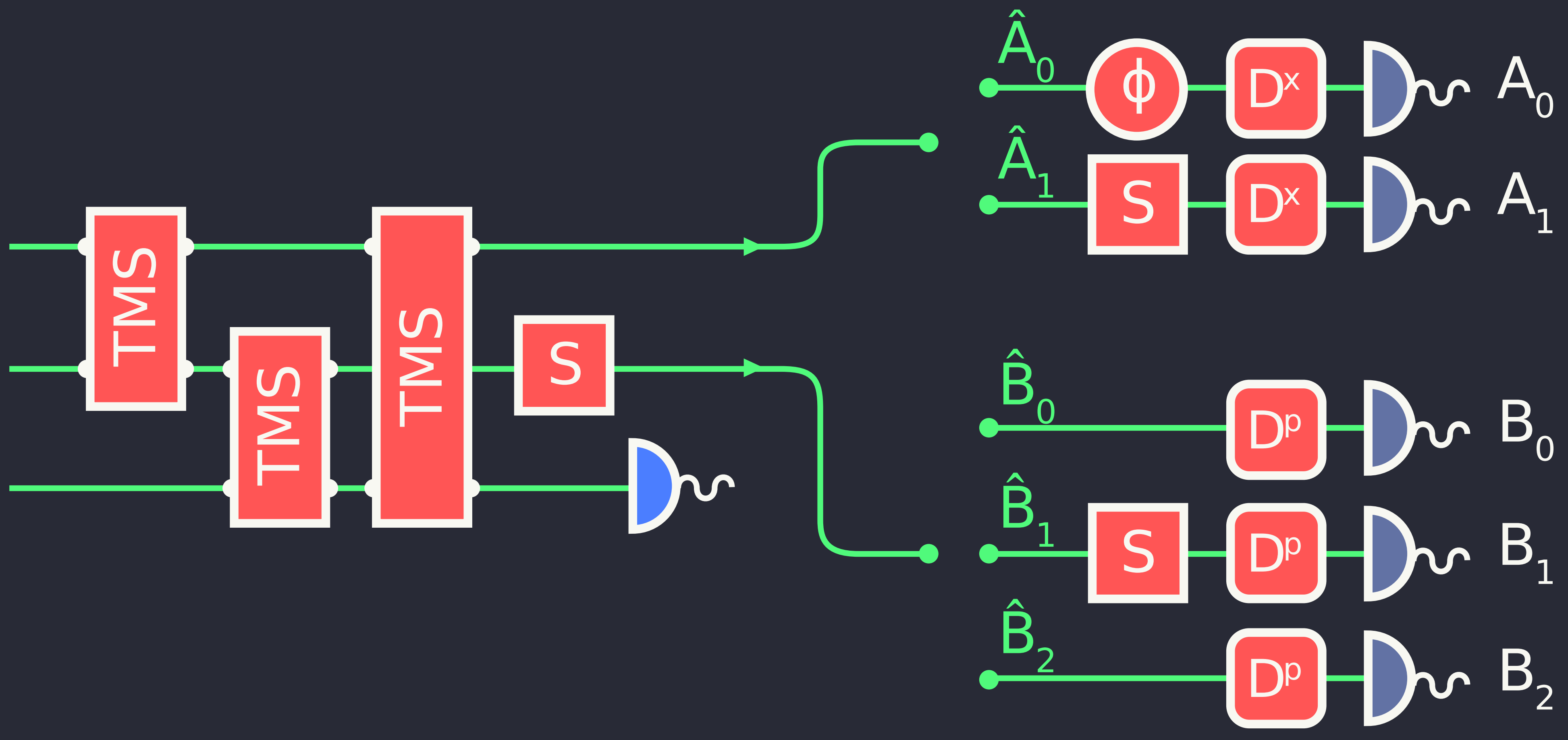


Reinforcement Learning for photonic DIQKD

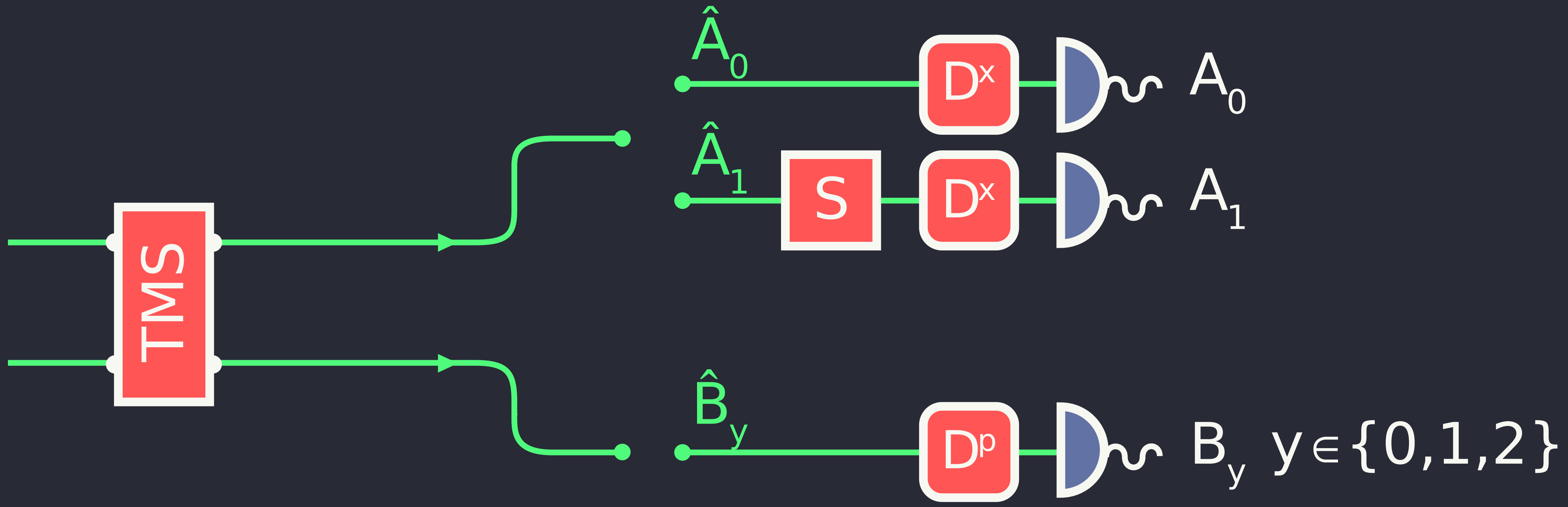


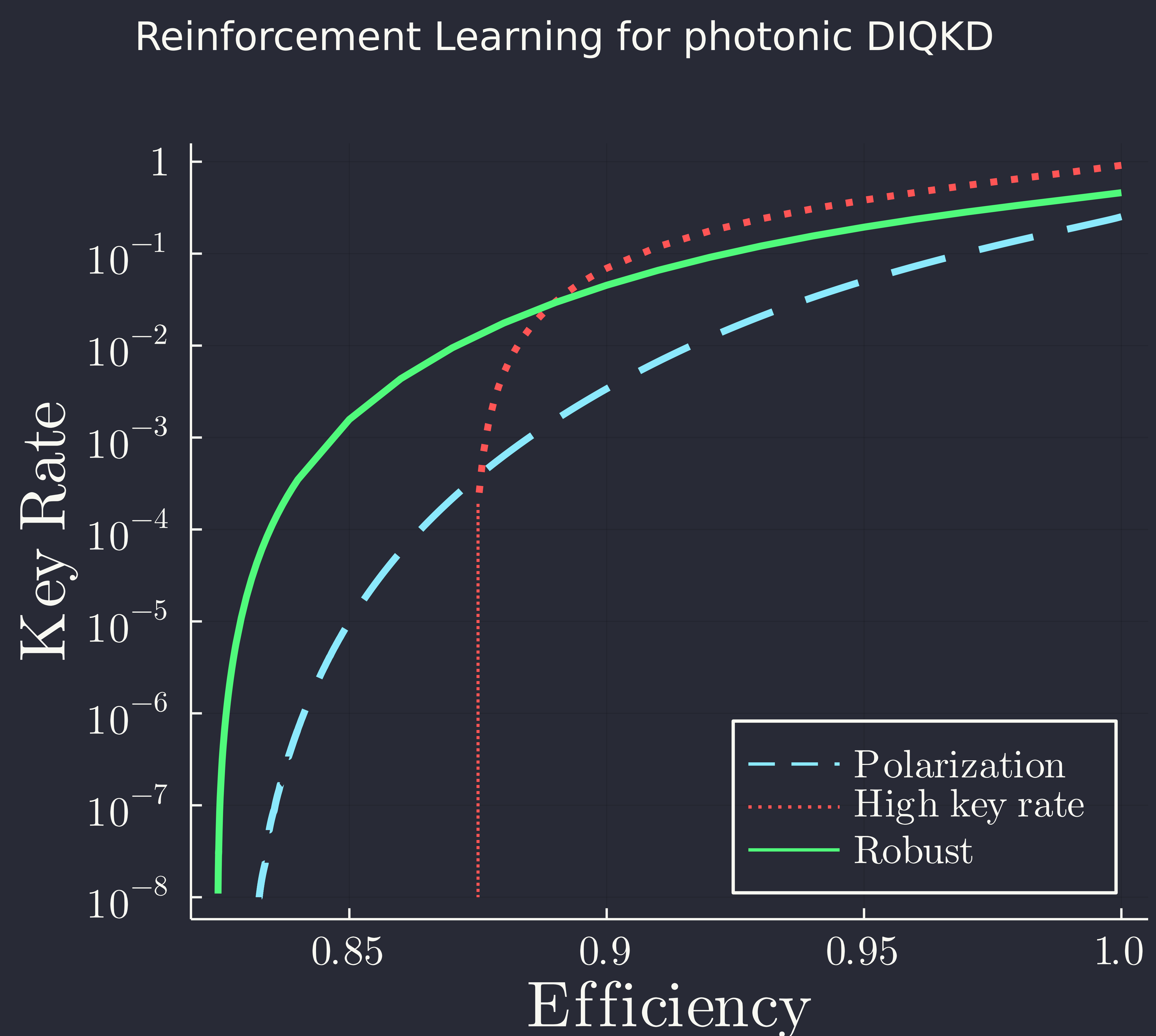
RL for photonic DIQKD, found circuits

Maximize r in a ideal scenario



Maximize loss such that $r > 10^{-4}$




Reinforcement Learning for photonic DIQKD
Key Rate
1
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
0.85
0.9
0.95
1.0
Efficiency
Polarization
High key rate
Robust

Takeaways

Device-independent Quantum Key Distribution allow to share a key between two parties without assumption on the quantum devices used

+

Quantum optics limited to Gaussian operation and heralding can be simulated efficiently (QuantumOpticalCircuits.jl)

+

Reinforcement learning aims at learning a task by interacting with an environment

=

We used Reinforcement Learning to design quantum optical circuit allowing to implement device-independent quantum key distribution

Thanks for your attention