QAMP 2025

Exploring Quantum Key Distribution Protocols #17

Speaker name: **Ariadna Prat Bosch**
Team members: Fernando Bitti Loureiro
Mentor: Sanya Nanda

Project #17
Exploring Quantum Key Distribution Protocols

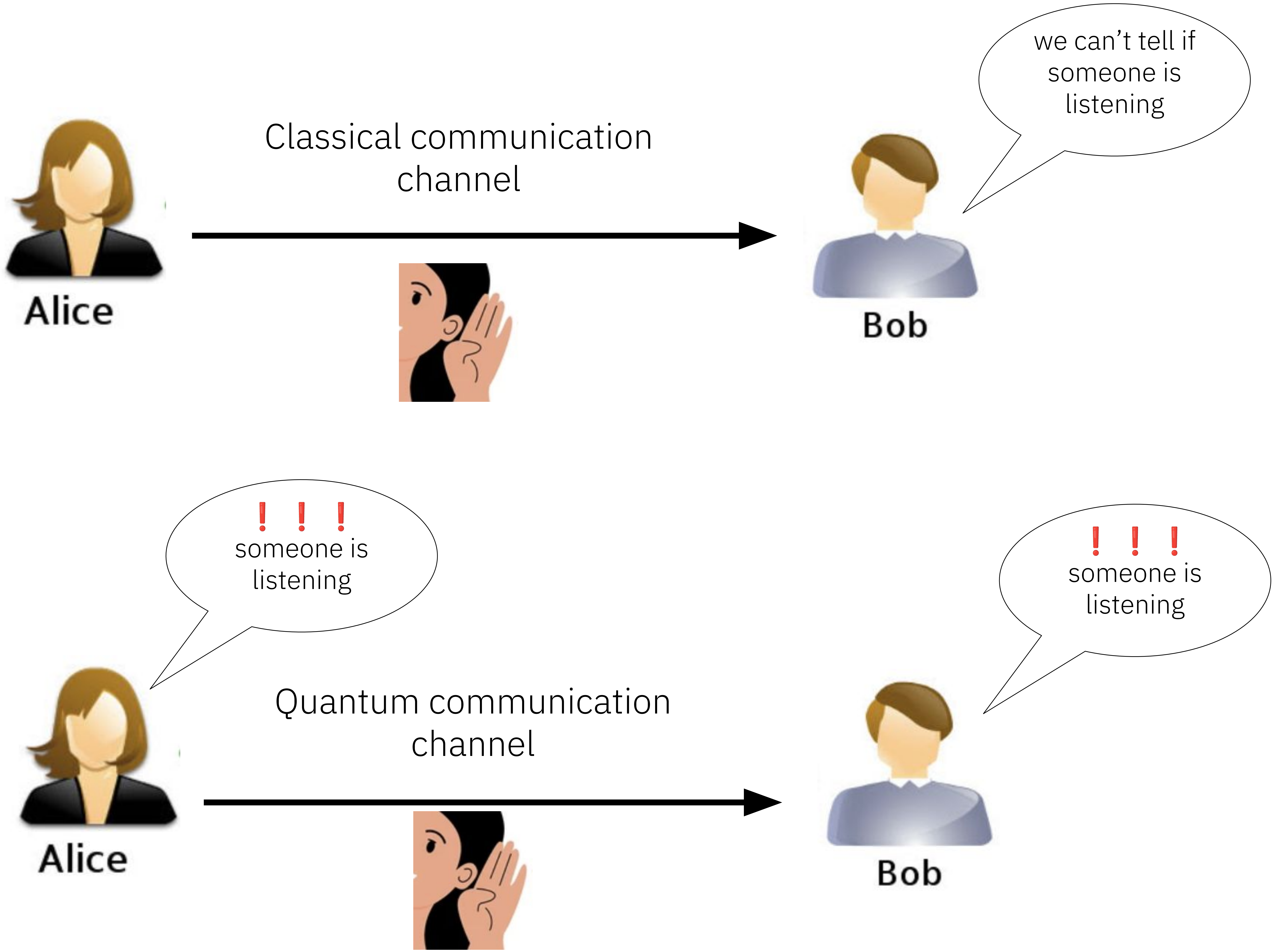
Team introduction

- **Ariadna Prat Bosch:** Student in Computer Science and solid foundations in cryptography
- **Fernando Loureiro:** Sales Engineer in web acceleration and security solutions

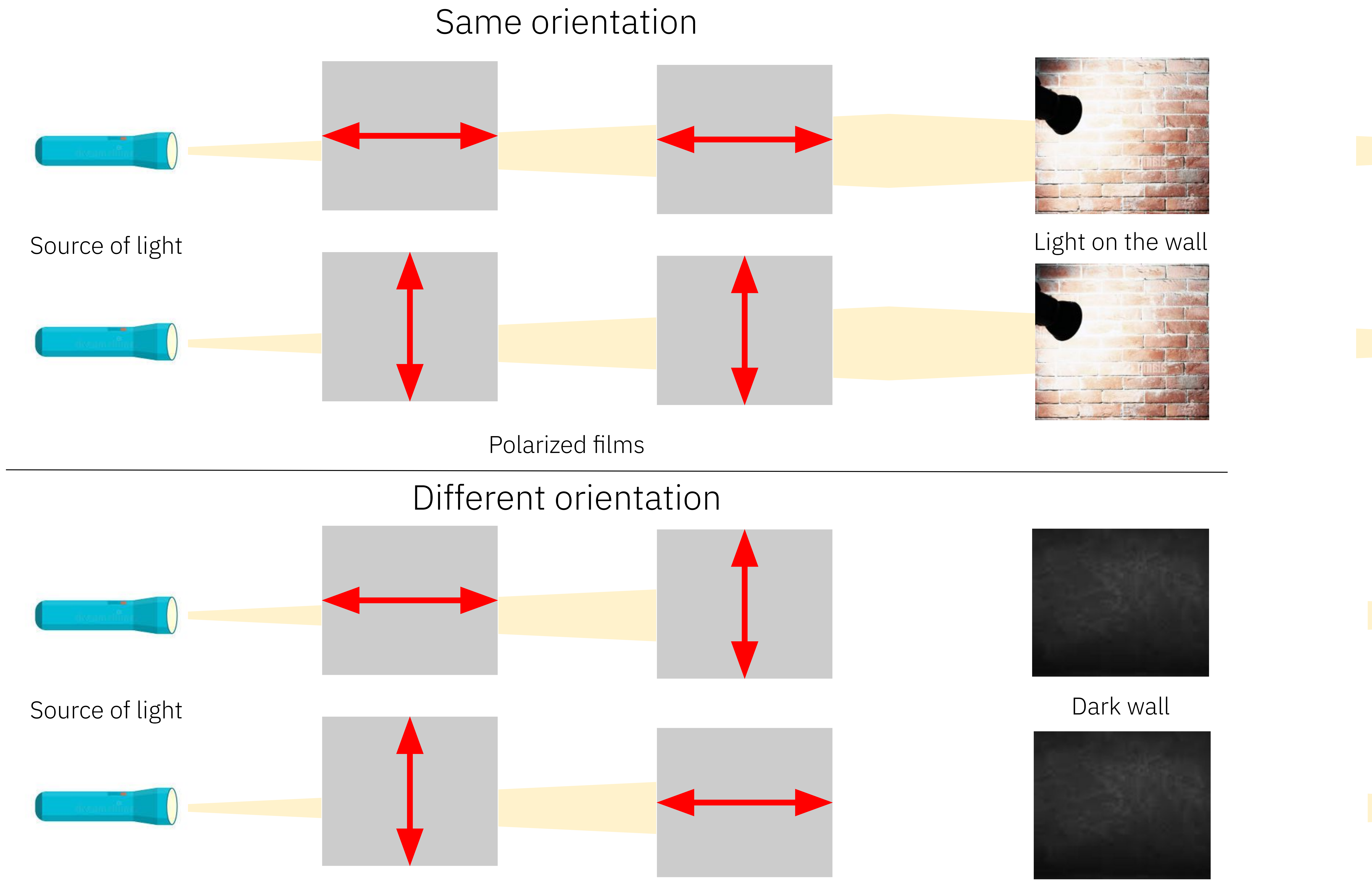
Project overview

Exploring Quantum Key Distribution Protocols: using Quantum properties to detect if someone is spying and your communication channel is not safe anymore.

Project #17
Main idea behind Quantum Key Distribution

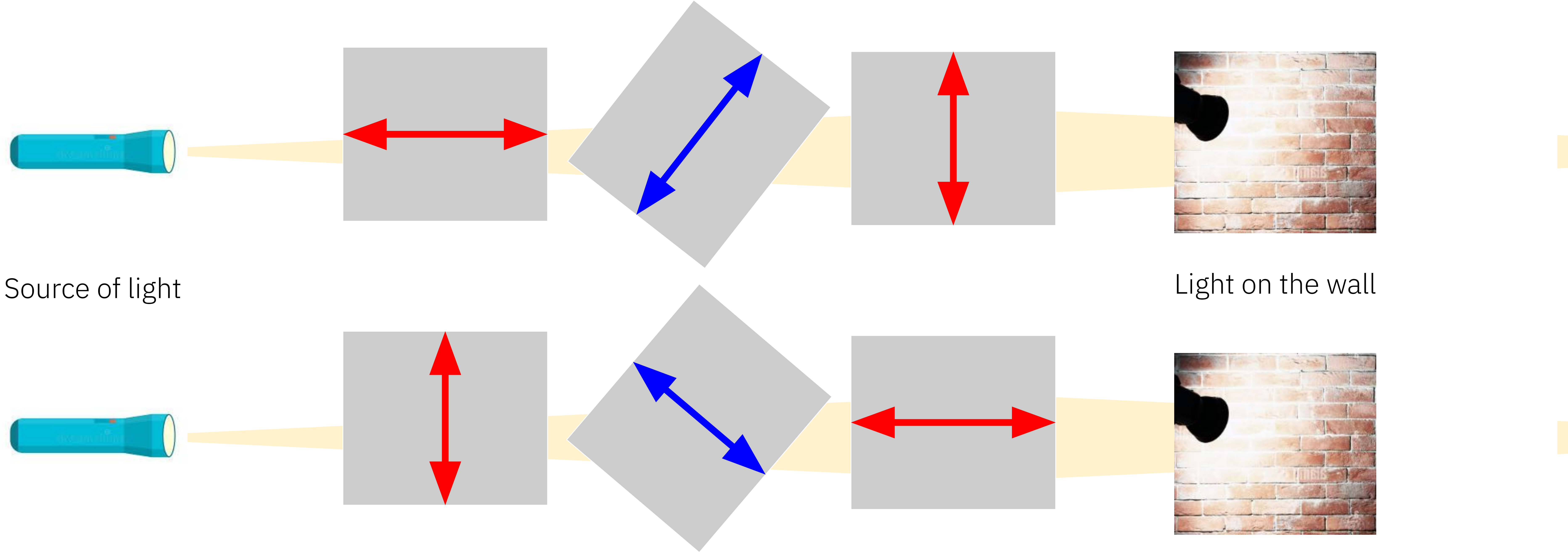


Project #17
Visible quantum properties



Project #17
Visible quantum properties

Different orientation,
insert an extra polarized film tilted in diagonal and you see light on the wall



Because the expected result changed, we are able to use this property to detect if someone is watching the communication channel

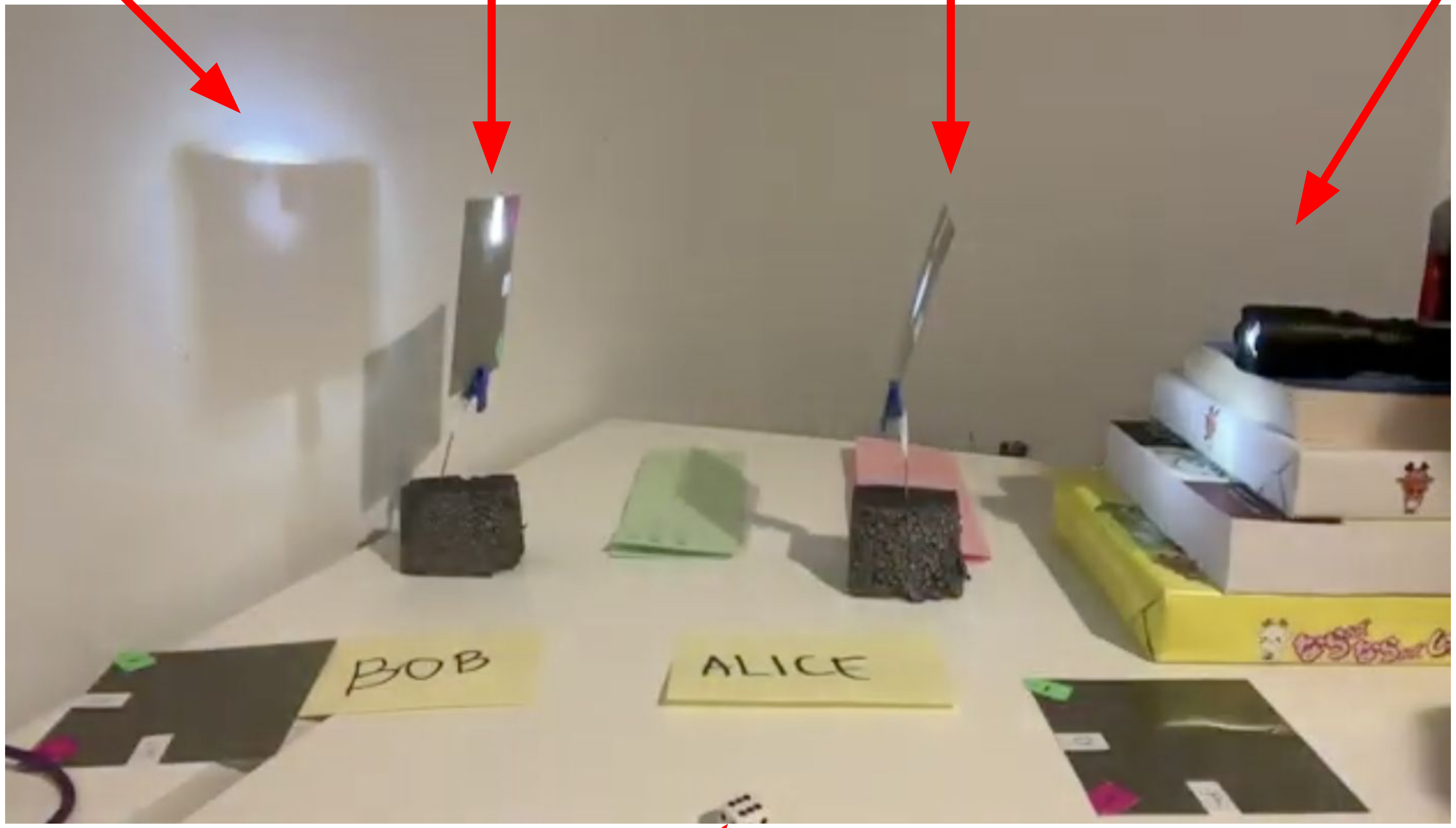
#17
A homemade simulation of BB84 (a real implementation would use a single photon, not a flashlight)

state |1> measured

Bob measures state

Alice sets state

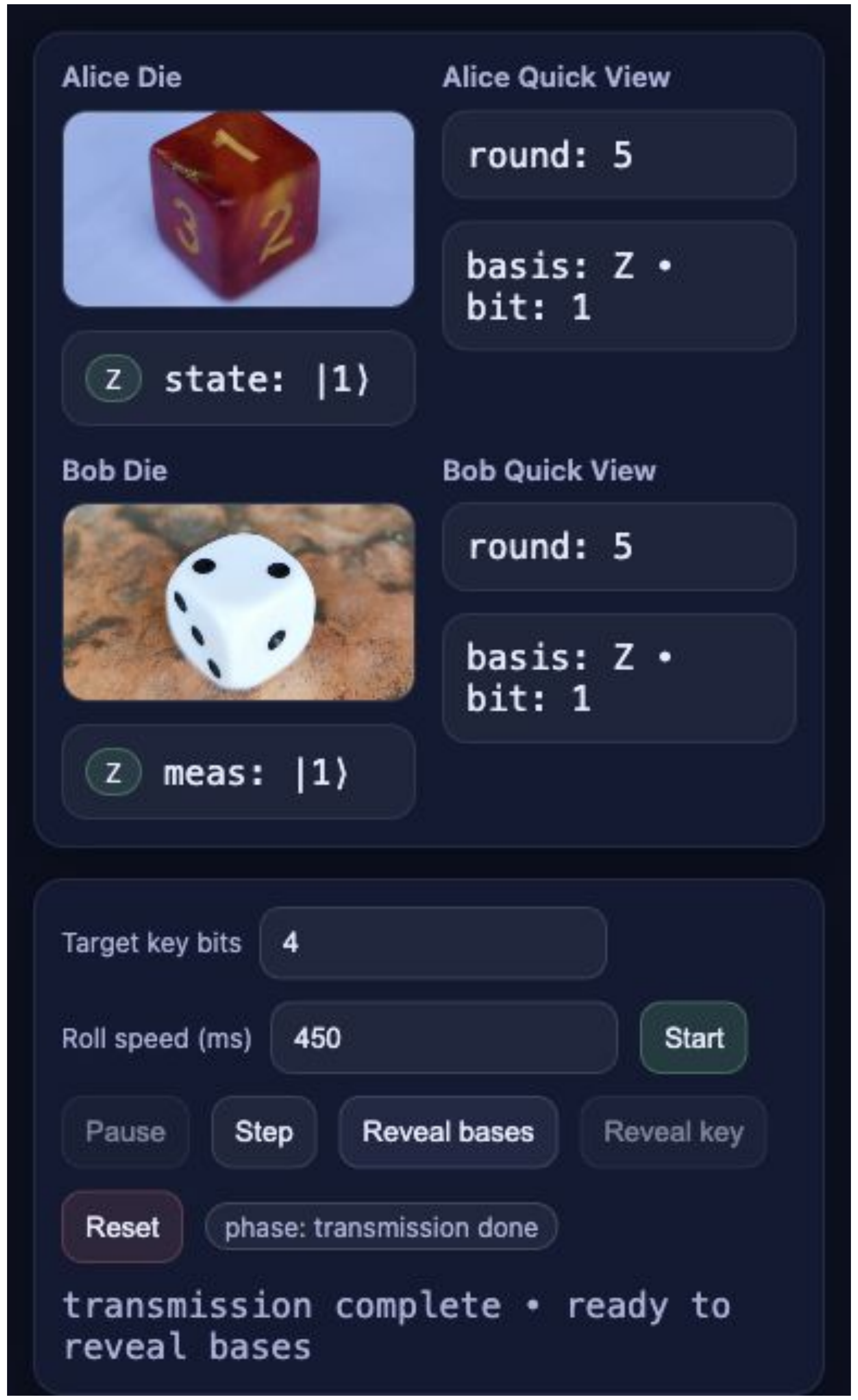
Photons generator



Random choices generator

Project #17
Test our simulation tool online

https://bb84-simulator.edgecompute.app/



#17
E91 Tutorial Notebook

Tutorial E91 protocol

Prerequisites

- Basic knowledge of Dirac notation and Pauli operations.
- Basic knowledge of Python (Qiskit).

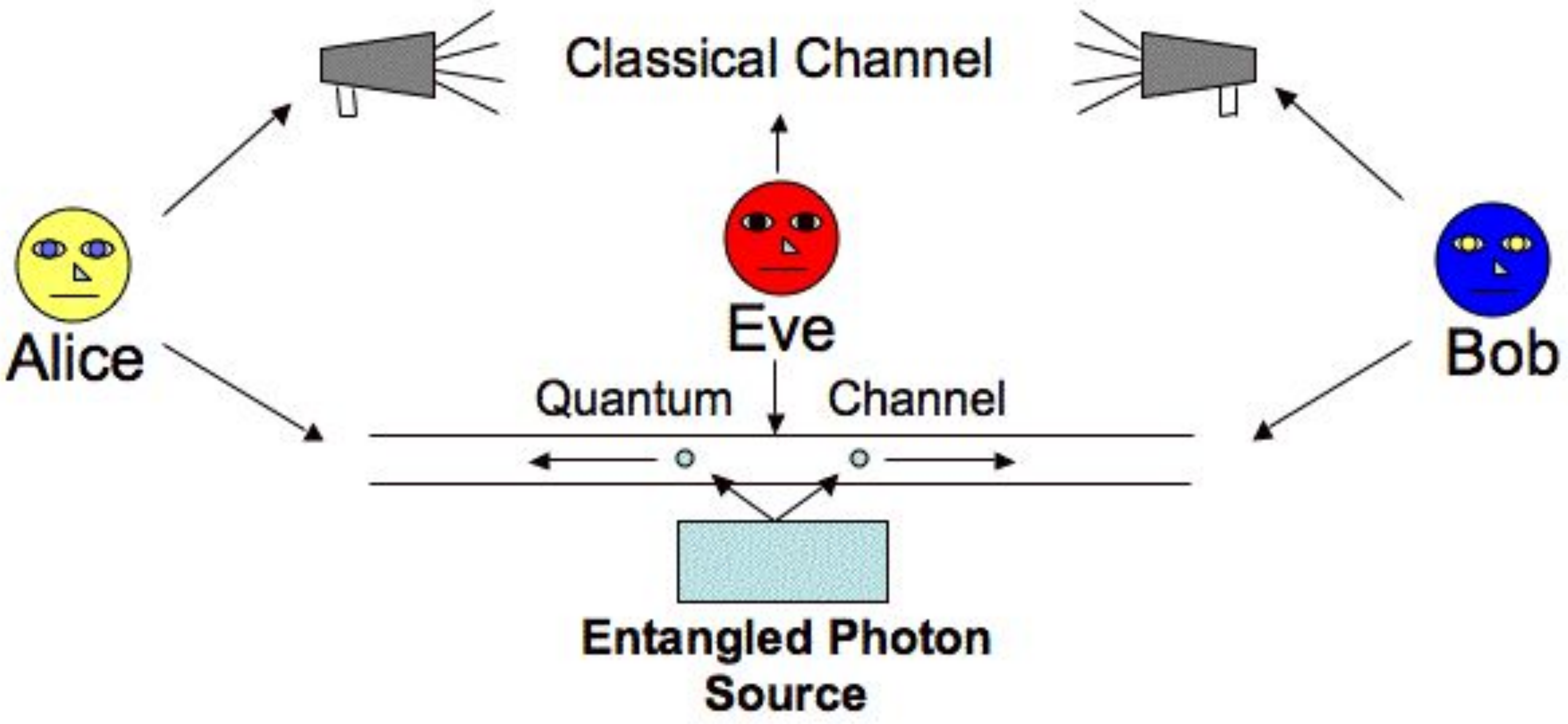
https://colab.research.google.com/drive/1X9zZ8umSXaidn19-R7DBH4OiD84ztw11#scrollTo=cO9zvHCYfj9o

#17
Main idea of E91 protocol

- To send pairs of entangled photons to Alice and Bob in order to generate a secret shared key and detect Eve's presence.
- The photons will be measured with angles, that are shared on classical channel.

Split in two parts:

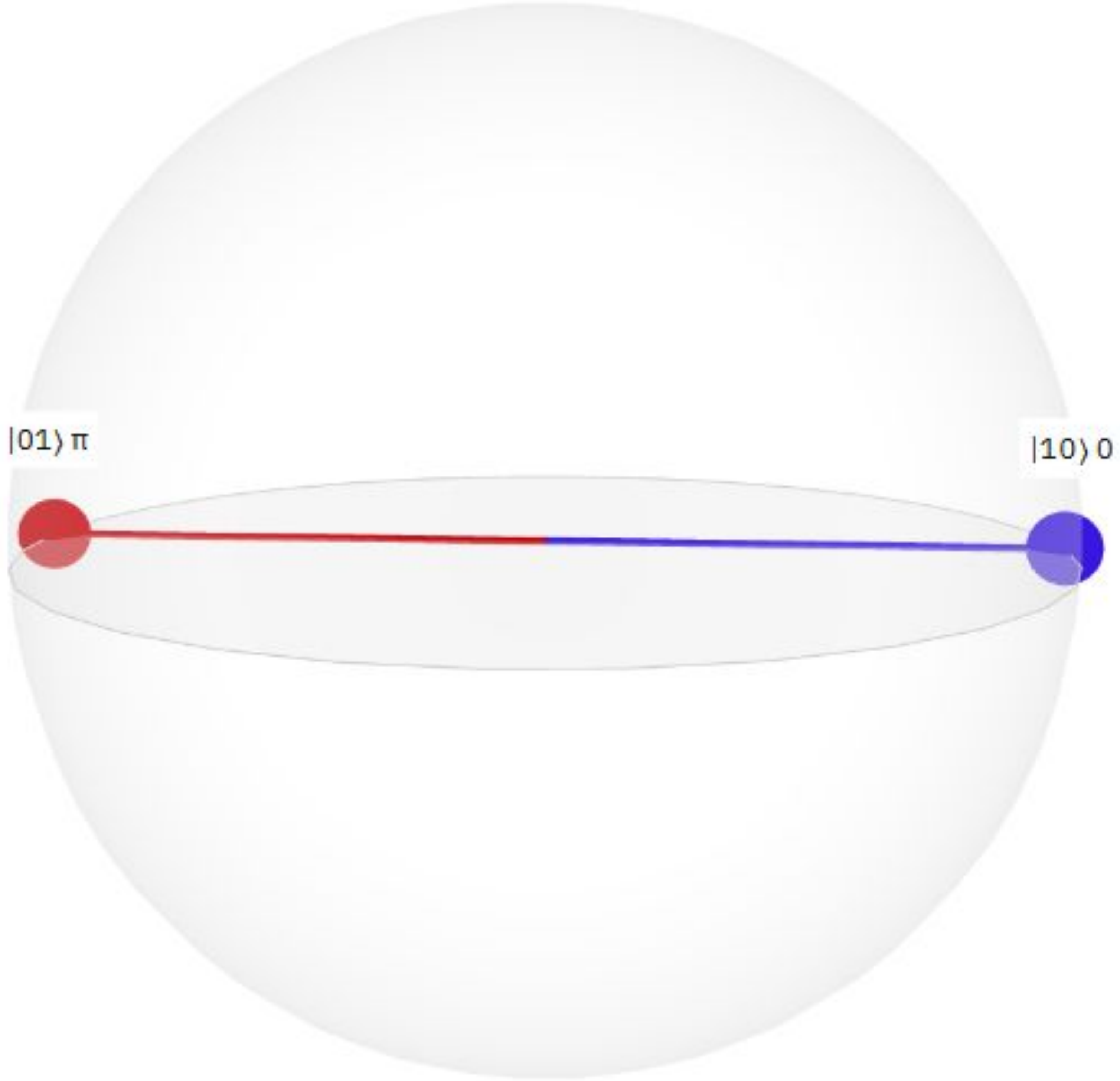
- A small subset of the measured bits is used to create the shared secret key.
- A larger subset is used to evaluate Bell's inequalities.

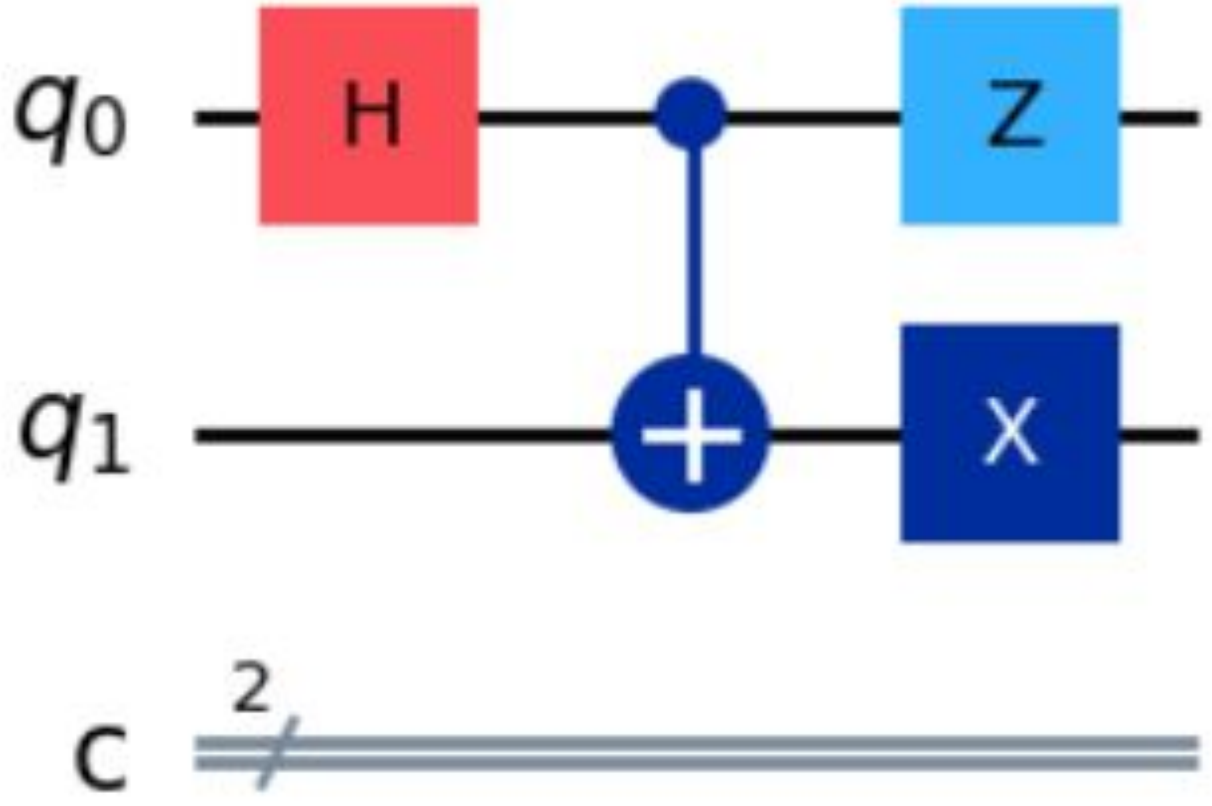


#17
E91 tutorial: Security behind Quantum Entanglement

- Quantum entanglement between two qubits.
- Two entangled qubits are sent to two parties located at large distances.
- The measurement of one qubit immediately breaks the entanglement.

$$|\psi_s^{(-)}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

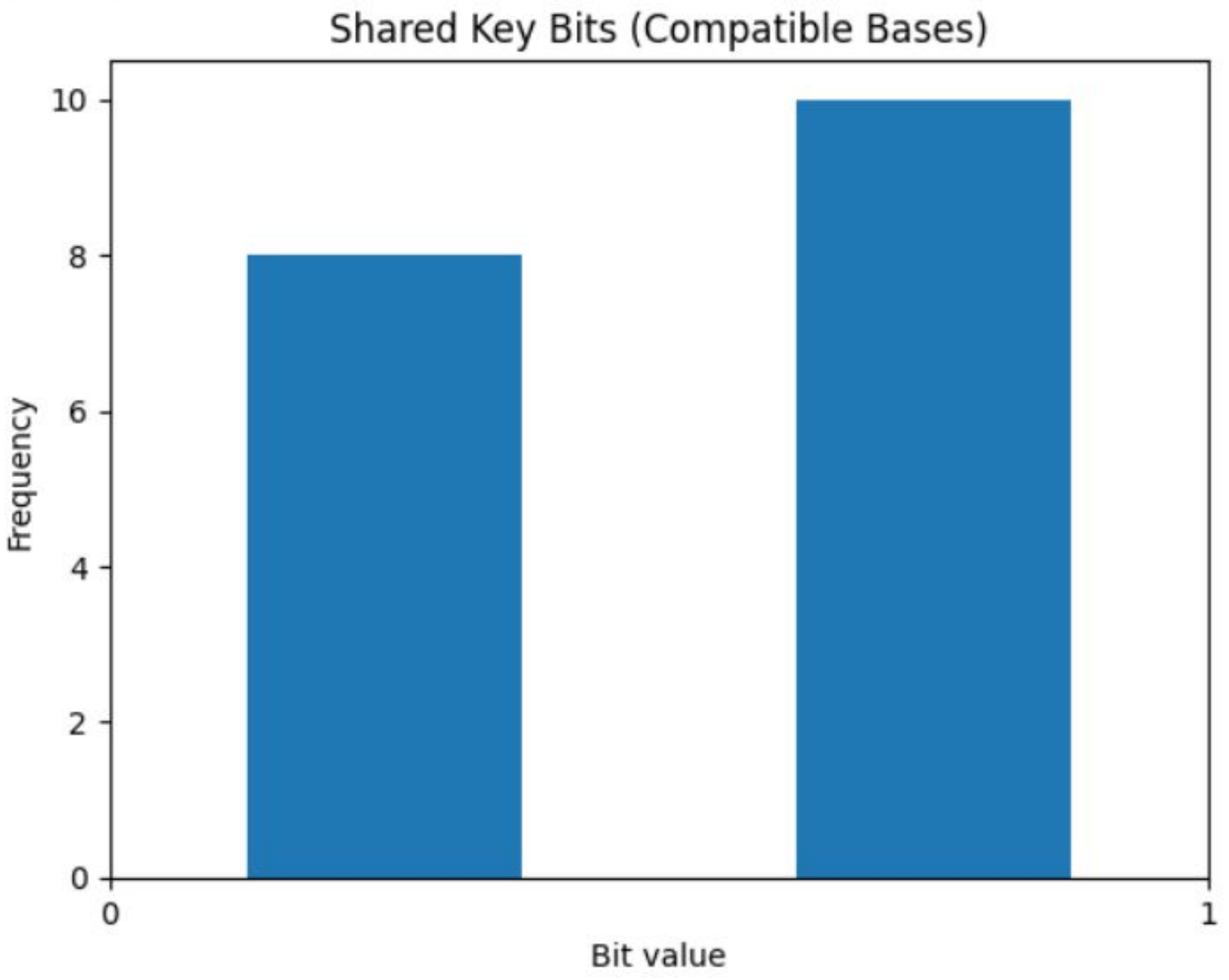




#17
E91 tutorial: Create the shared key

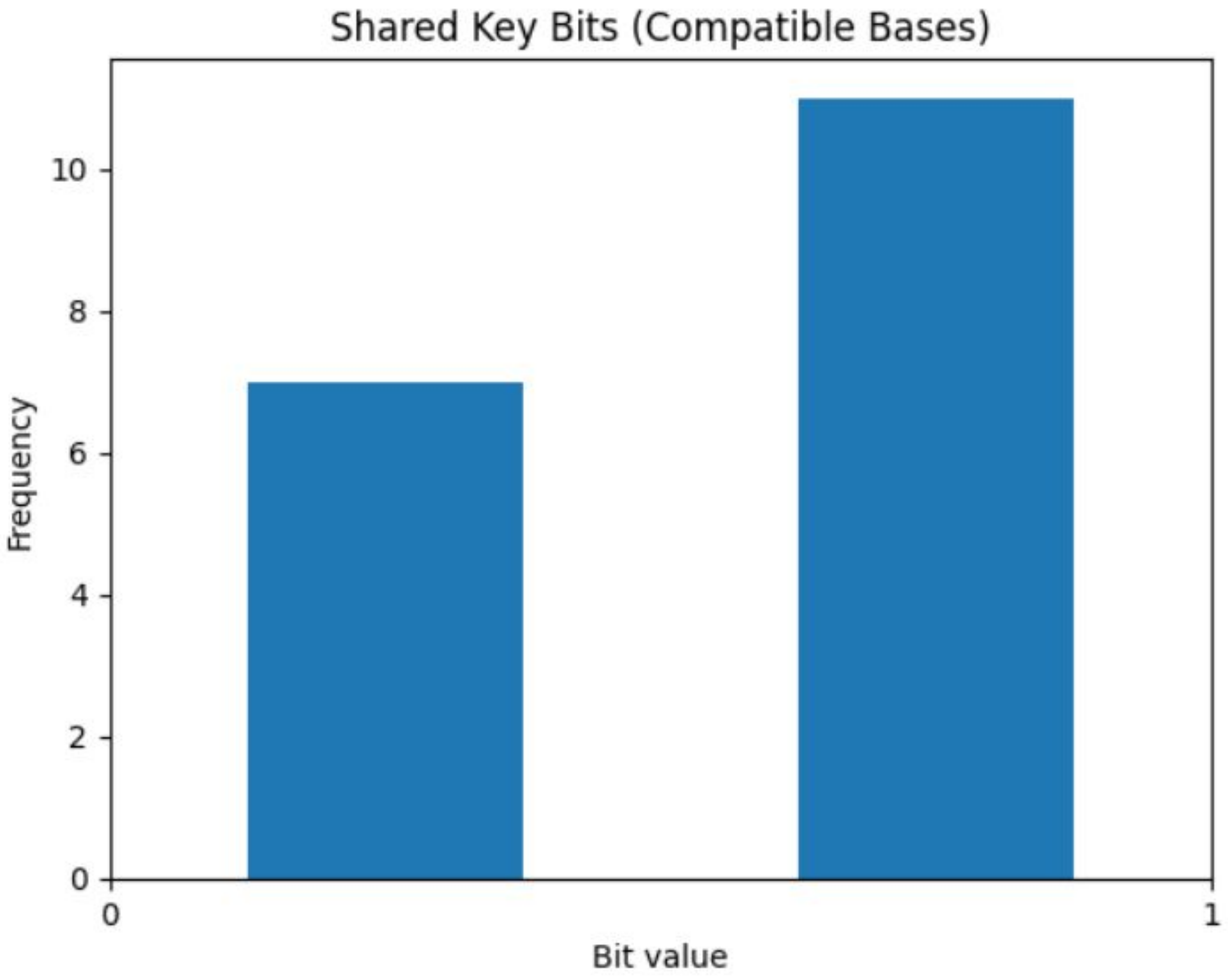
Eavesdropping is deactivated.

```
Alice results: [(0.7853981633974483, 0), (1.5707963267948966, 1), (0, 0), (
Bob results: [(0.7853981633974483, 1), (0.7853981633974483, 0), (-0.7853981
Shared key: [0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0]
Number of key bits: 18
```



Eavesdropping is activated.

```
Alice results: [(1.5707963267948966, 0), (0, 0), (0, 1), (1.57079632679489
Bob results: [(-0.7853981633974483, 0), (0.7853981633974483, 0), (-0.78539
Shared key: [1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0]
Number of key bits: 18
```



#17
E91 tutorial: Bell's Inequalities

What is the relation between Bell's inequalities and eavesdropping?

In E91, we have the following cases:

- If Bell's inequality is violated, there is no eavesdropping.
- If Bell's inequality is not violated, Eve's presence is active.

The bell's inequalities formula is the following:

$$S = E(a,b) + E(a,b') + E(a',b) - E(a',b')$$

where E is an estimation of bit results between Alice's Angles (a, a') and Bob's angles (b, b').

- If $S \leq 2$, then Bell's inequalities are not violated.
- If $2 \leq S \leq 2\sqrt{2}$, the equation is violated.
- Otherwise, is not physically possible.

#17
E91 tutorial: Bell's Inequalities

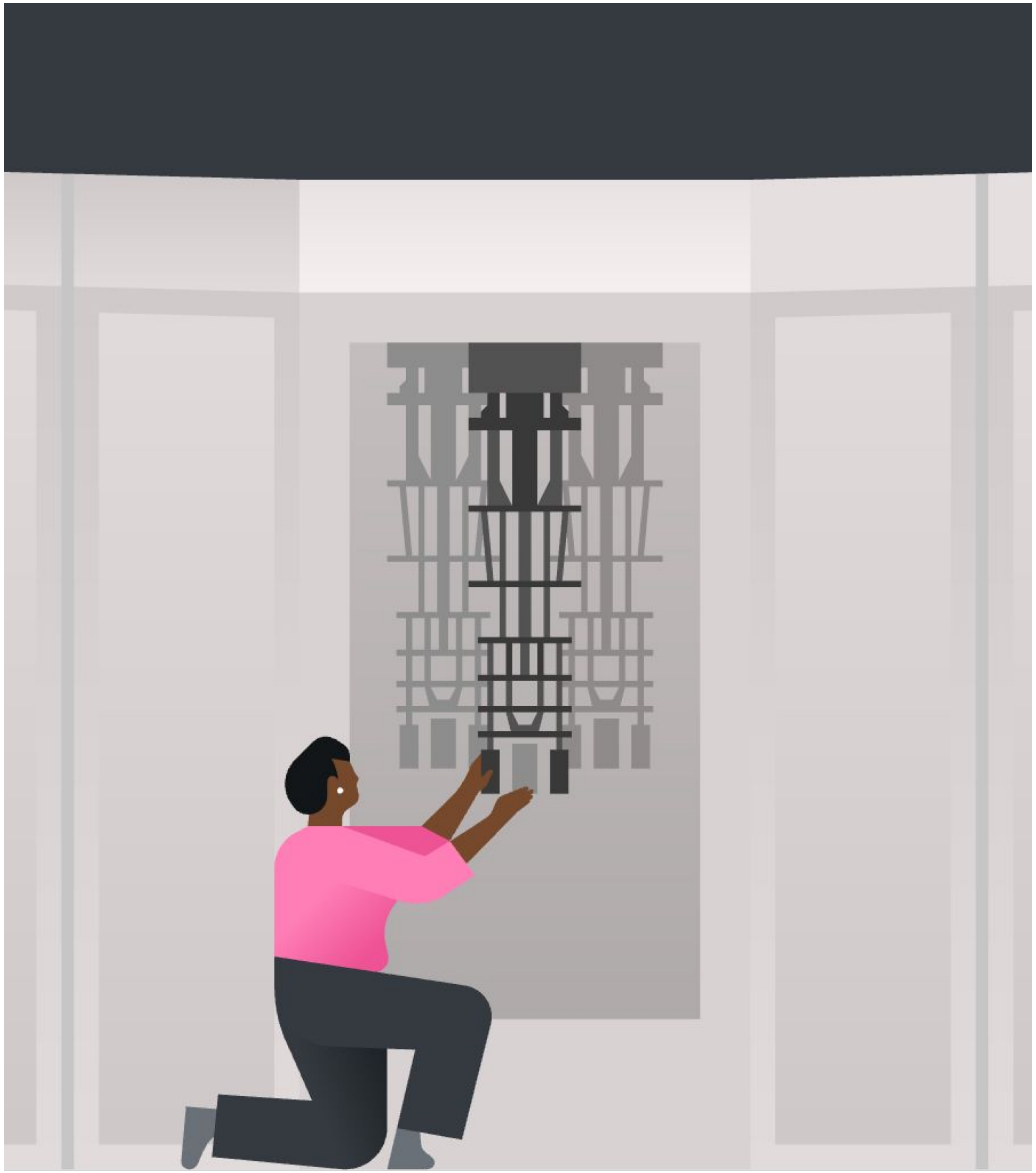
Eavesdropping is deactivated.

```
E(A0,B0) = -1.000
E(A0,B1) = -0.707
E(A0,B2) = -0.704
E(A1,B0) = 0.006
E(A1,B1) = -0.715
E(A1,B2) = 0.728
E(A2,B0) = -0.711
E(A2,B1) = -1.000
E(A2,B2) = -0.015

CHSH:
S = -2.854
|S| = 2.854
```

Eavesdropping is activated.

```
E(A0,B0) = 0.009
E(A0,B1) = 0.015
E(A0,B2) = 0.002
E(A1,B0) = 0.005
E(A1,B1) = 0.004
E(A1,B2) = 0.000
E(A2,B0) = -0.011
E(A2,B1) = -0.002
E(A2,B2) = 0.005

CHSH:
S = 0.020
|S| = 0.020
```

Thank you!



QISKIT ADVOCATE

2025 2025

MENTORSHIP PROGRAM