

Welcome to the Quantum World

A Short Introduction to Quantum Cryptography

Carolin Lunemann

DAIMI, Aarhus University, DK



Welcome to the Quantum World

Quantum Mechanics offers new possibilities...

...Quantum Cryptography

...Quantum Computing

...Quantum Information Processing

Welcome to the Quantum World

Quantum Mechanics offers new possibilities...

...Quantum Cryptography

...Quantum Computing

...Quantum Information Processing

Secret-Key Cryptography

Problem: Secure channel needed for key distribution;
only OTP is unconditionally secure.

Welcome to the Quantum World

Quantum Mechanics offers new possibilities...

...Quantum Cryptography

...Quantum Computing

...Quantum Information Processing

Secret-Key Cryptography

Problem: Secure channel needed for key distribution;
only OTP is unconditionally secure.

Public-Key Cryptography

Problem: Security based on non-proven assumptions;
may be broken by quantum computers.

Welcome to the Quantum World

Quantum Mechanics offers new possibilities...

...Quantum Cryptography

...Quantum Computing

...Quantum Information Processing

Secret-Key Cryptography

Problem: Secure channel needed for key distribution;
only OTP is unconditionally secure.

Public-Key Cryptography

Problem: Security based on non-proven assumptions;
may be broken by quantum computers.

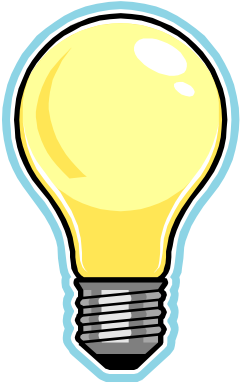
Quantum Key Distribution (QKD)

Security of OTP without secure channel.

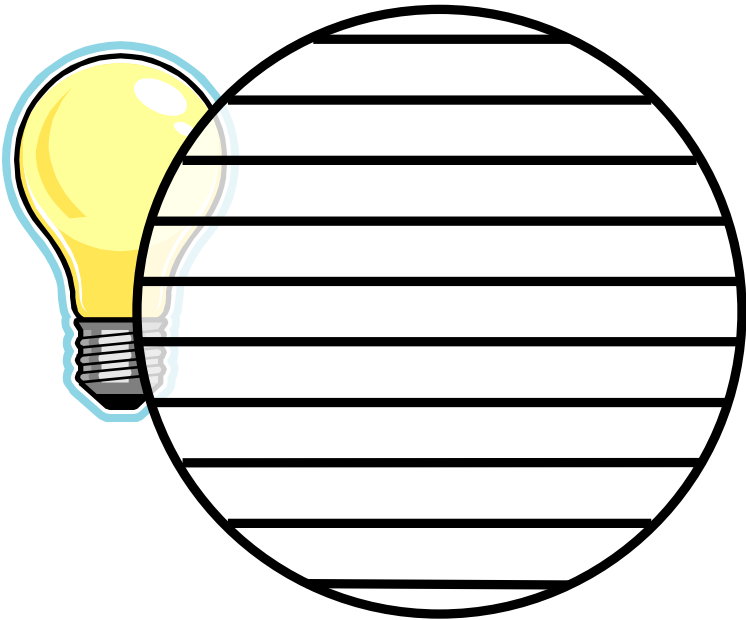
Security based on physical laws that also hold against quantum computers.

Qubits

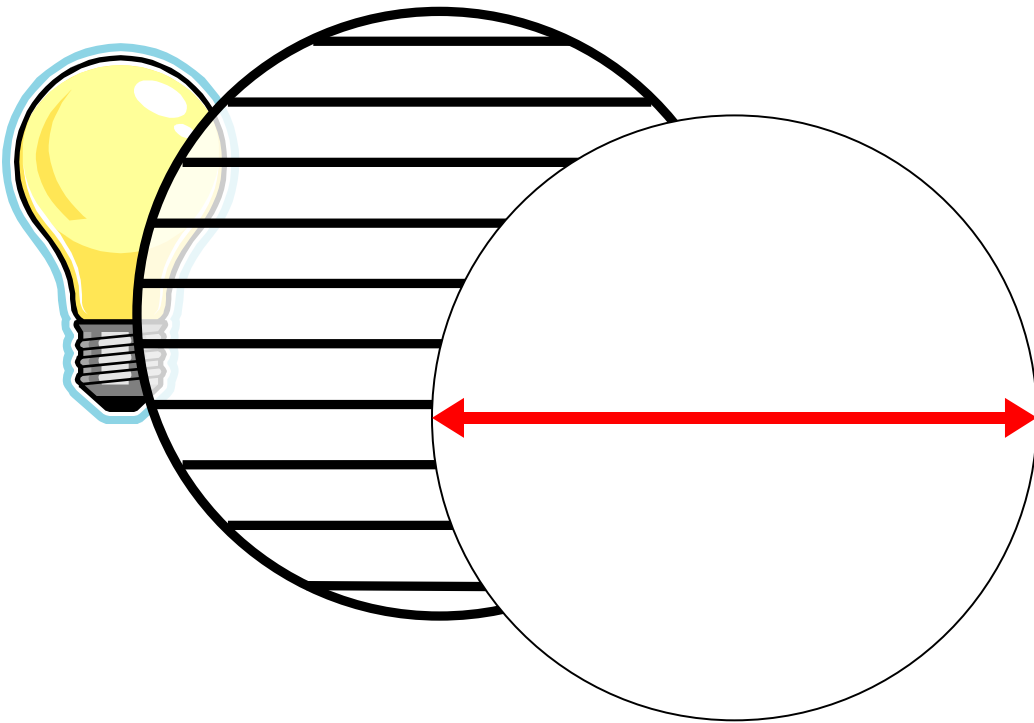
Qubits



Qubits

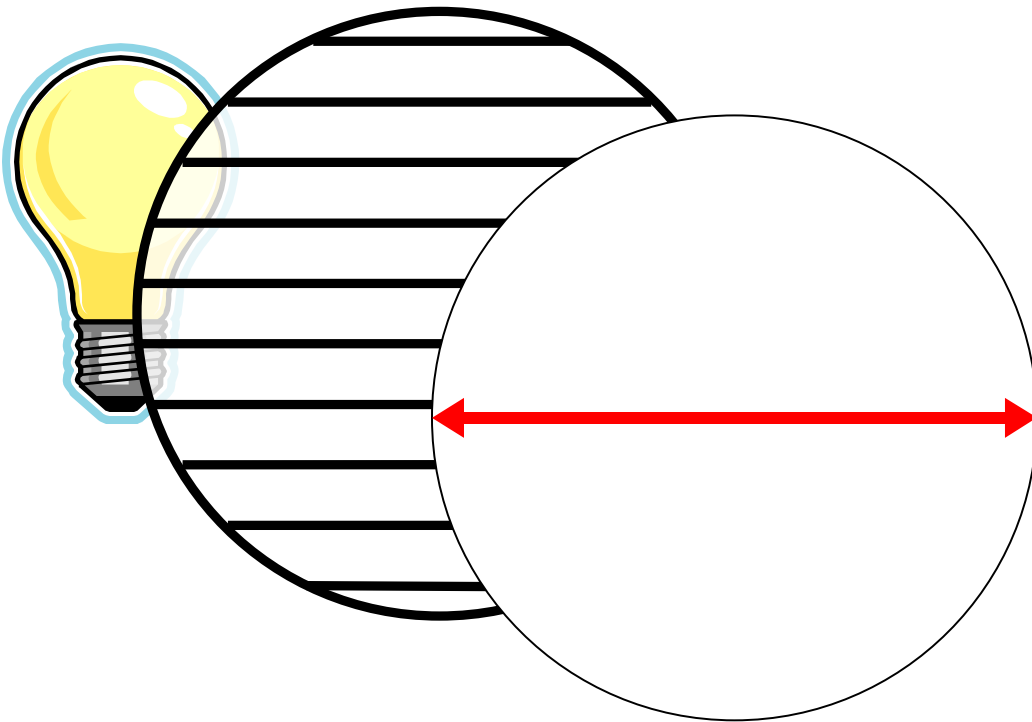


Qubits

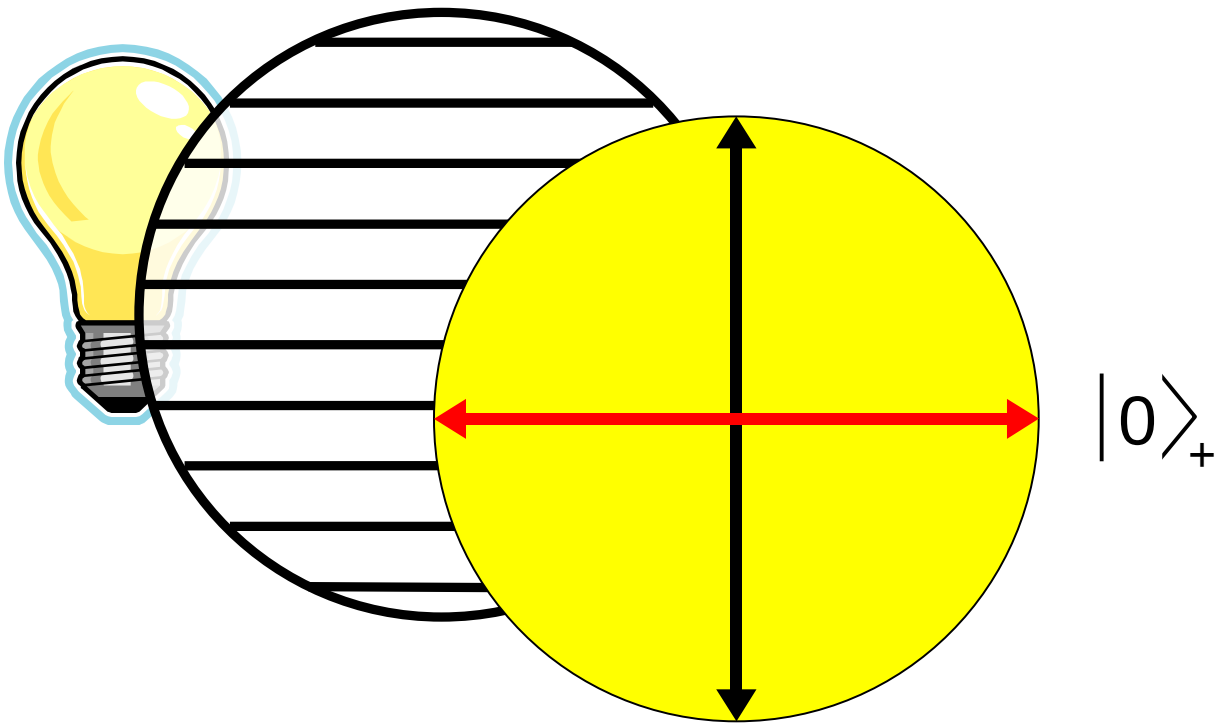


Qubits

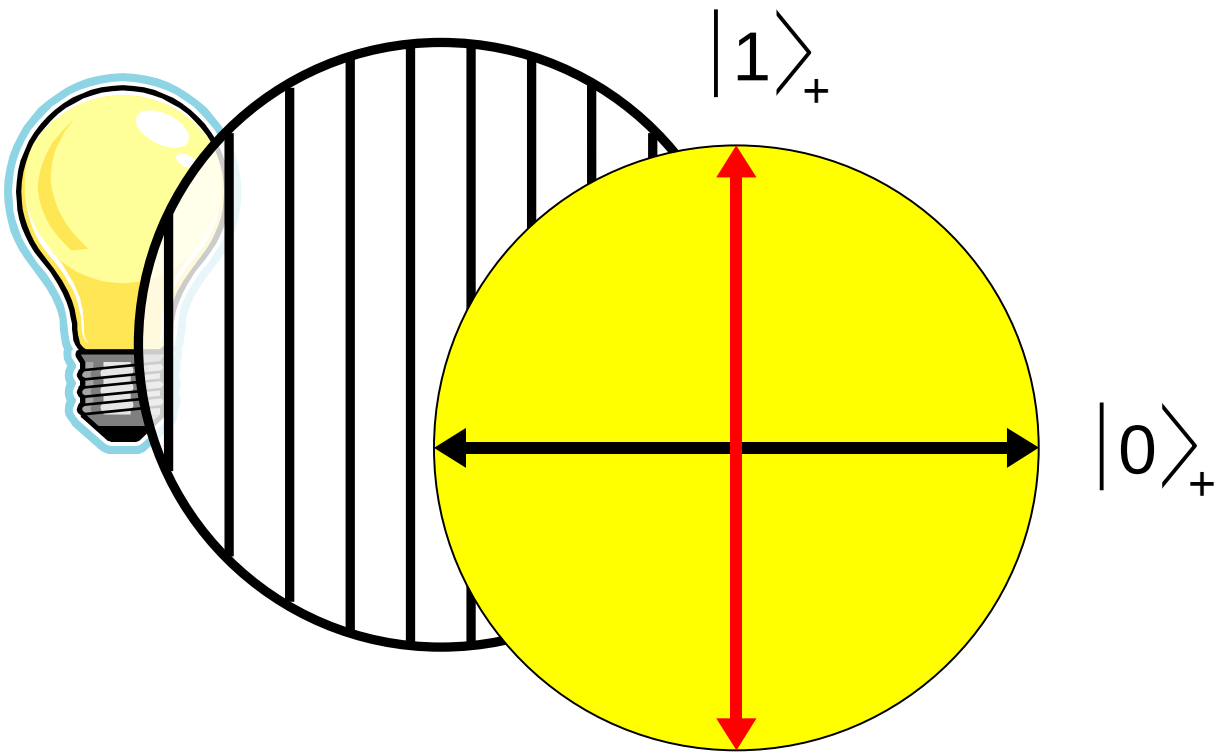
Qubits: Photons ("light quantum") are encoded by polarization.



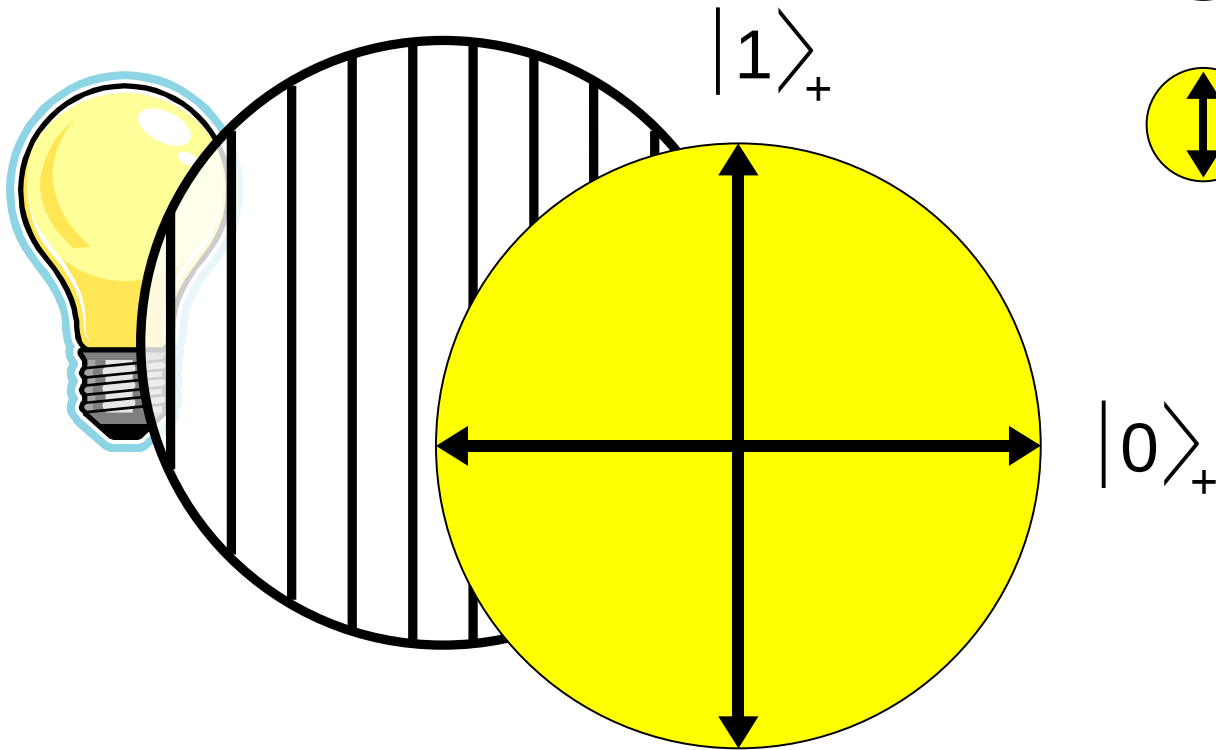
 **Basis**

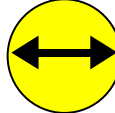


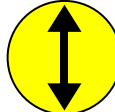
 **Basis**



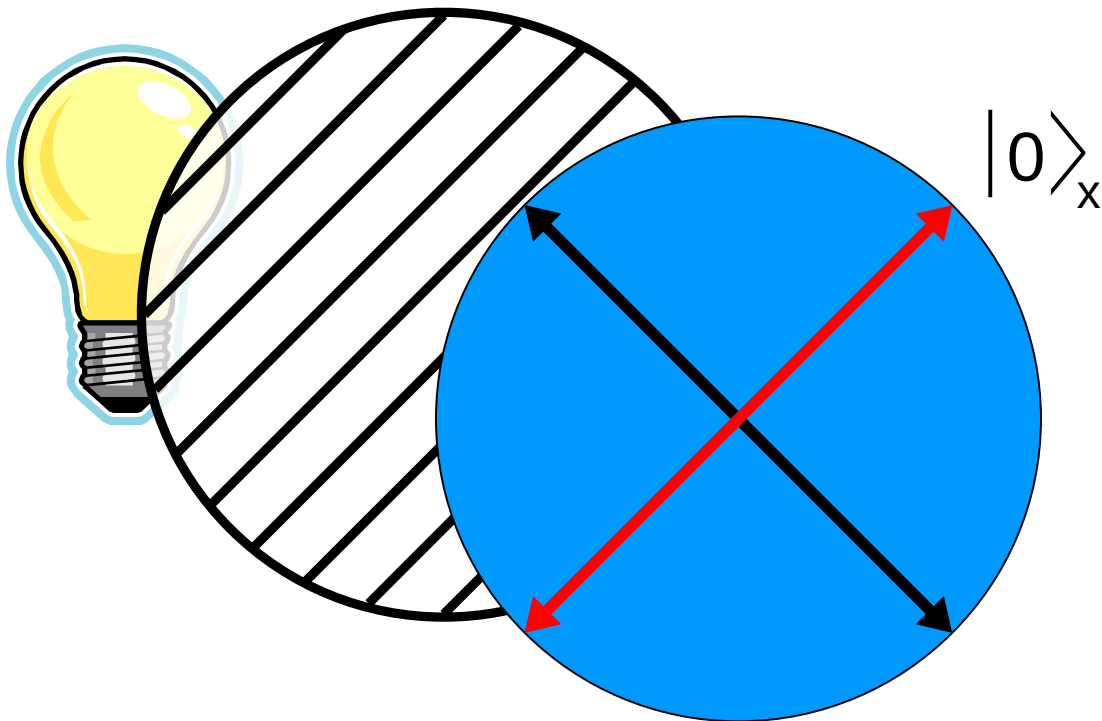
 **Basis**



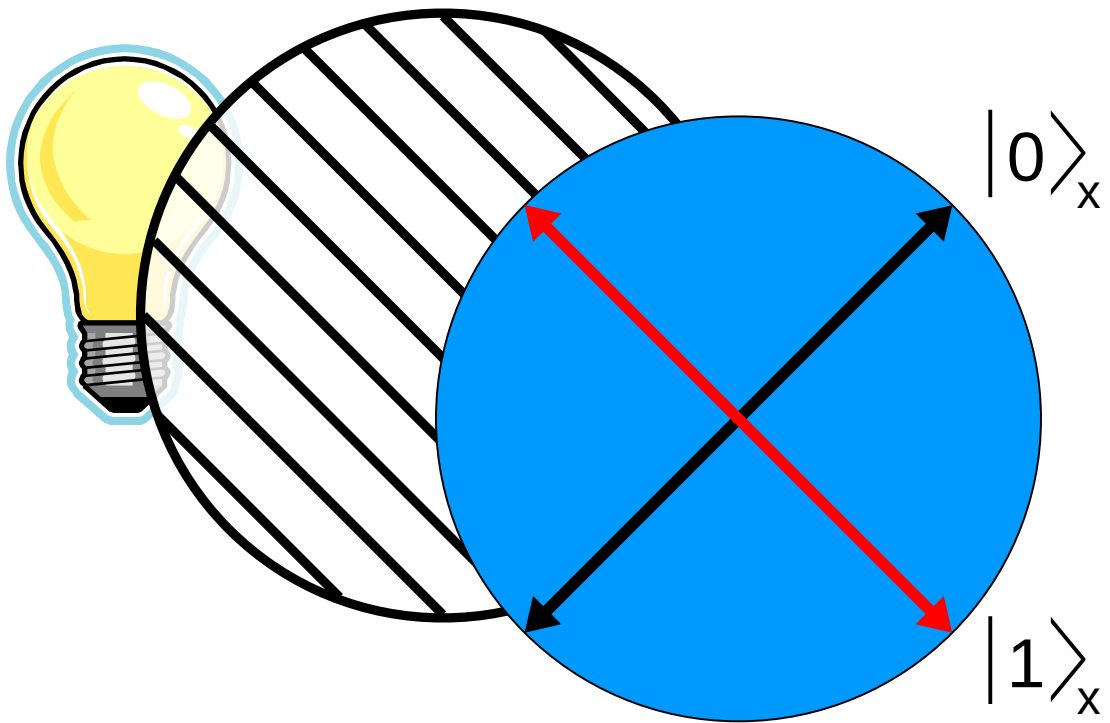
 $|0\rangle_+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

 $|1\rangle_+ = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

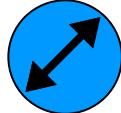
 **Basis**




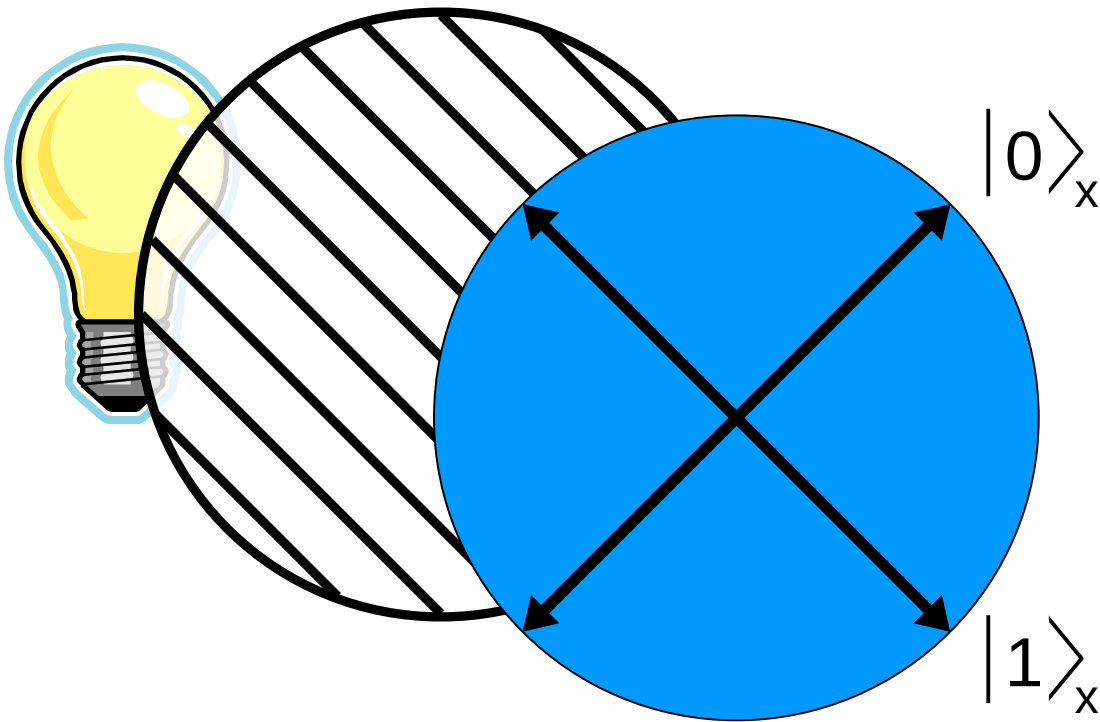
 **Basis**



 **Basis**

 $|0\rangle_x$

 $|1\rangle_x$



Measurement

$$\text{⦿} = \frac{1}{\sqrt{2}} \text{⦿} + \frac{1}{\sqrt{2}} \text{⦿}$$

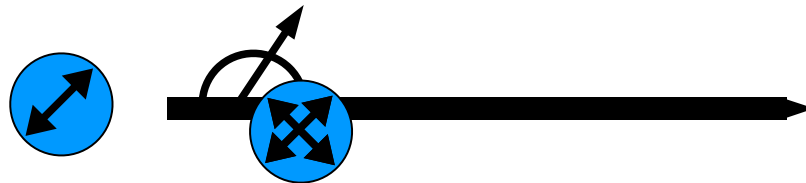
Measurement

$$\text{⊗} = \frac{1}{\sqrt{2}} \text{⊕} + \frac{1}{\sqrt{2}} \text{⊞}$$



Measurement

$$\text{Blue Circle} = \frac{1}{\sqrt{2}} \text{Yellow Circle} + \frac{1}{\sqrt{2}} \text{Yellow Circle}$$



Measurement

$$\text{Blue Circle} = \frac{1}{\sqrt{2}} \text{Yellow Circle} + \frac{1}{\sqrt{2}} \text{Yellow Circle}$$



Measurement

$$\text{Blue Circle} = \frac{1}{\sqrt{2}} \text{Yellow Circle} + \frac{1}{\sqrt{2}} \text{Yellow Circle}$$



Coding in a basis and measurement in **same** basis:
--> correct state with same polarization

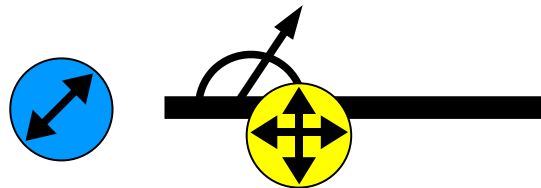
Measurement

$$\text{⦿} = \frac{1}{\sqrt{2}} \text{⦿} + \frac{1}{\sqrt{2}} \text{⦿}$$



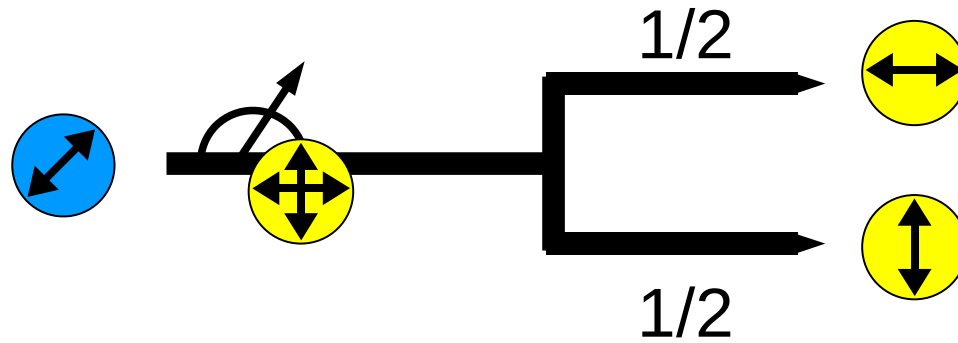
Measurement

$$\text{Blue Circle} = \frac{1}{\sqrt{2}} \text{Yellow Circle (H)} + \frac{1}{\sqrt{2}} \text{Yellow Circle (V)}$$



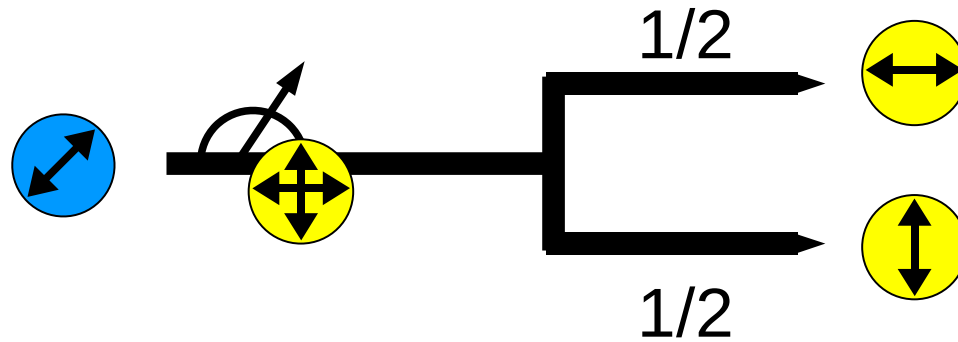
Measurement

$$\text{Blue Circle} = \frac{1}{\sqrt{2}} \text{Yellow Circle (H)} + \frac{1}{\sqrt{2}} \text{Yellow Circle (V)}$$



Measurement

$$\text{Blue Circle} = \frac{1}{\sqrt{2}} \text{Yellow Circle (H)} + \frac{1}{\sqrt{2}} \text{Yellow Circle (V)}$$

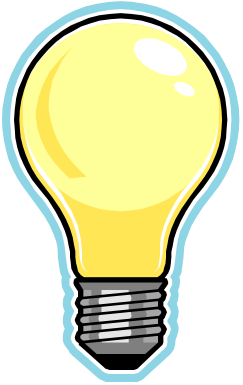


Coding in a basis and measurement in **different** basis:

- > random state
- > polarization according new basis
- > original information completely lost

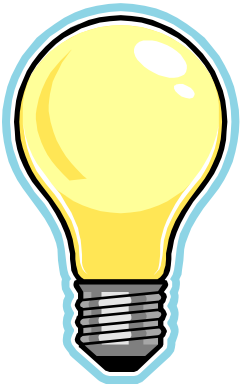
How does it work?

How does it work?



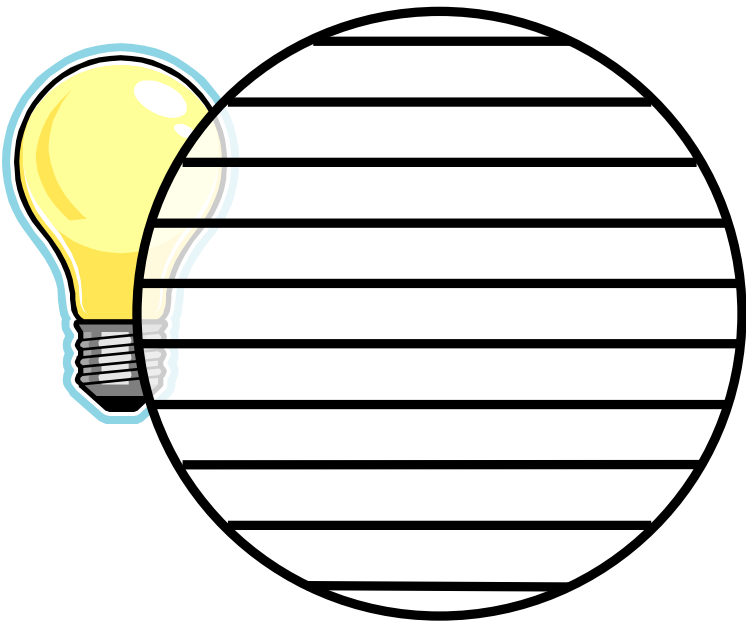
How does it work?

Alice $|0\rangle_+$



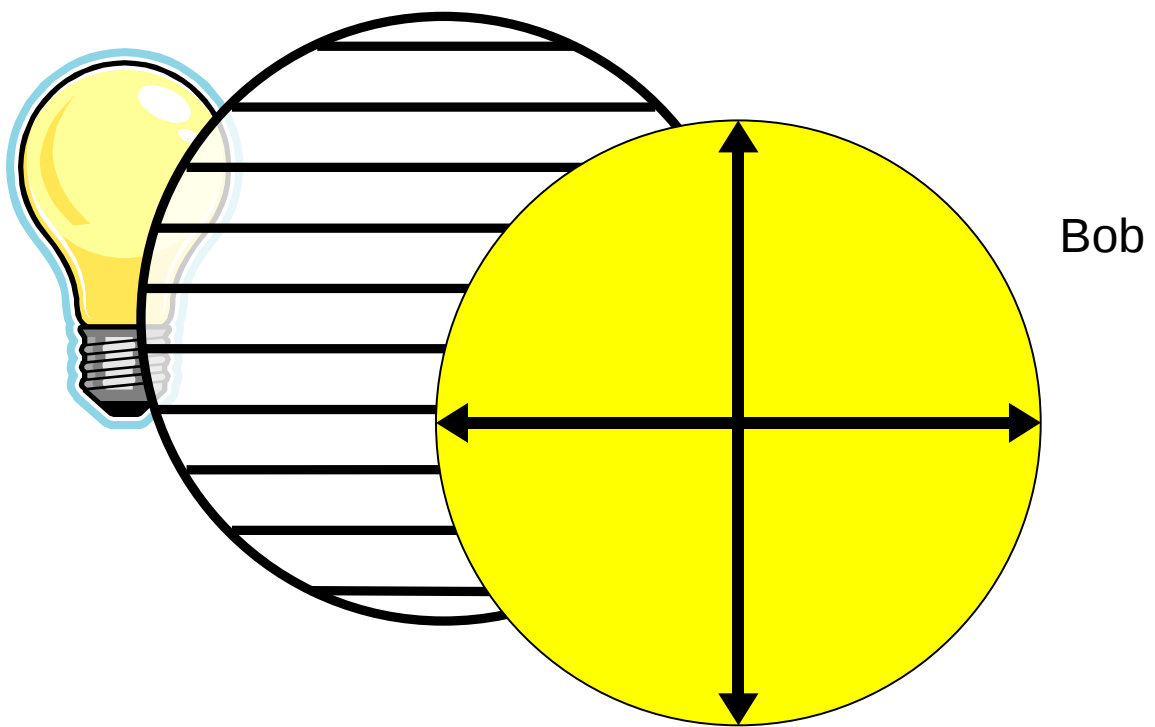
How does it work?

Alice $|0\rangle_+$

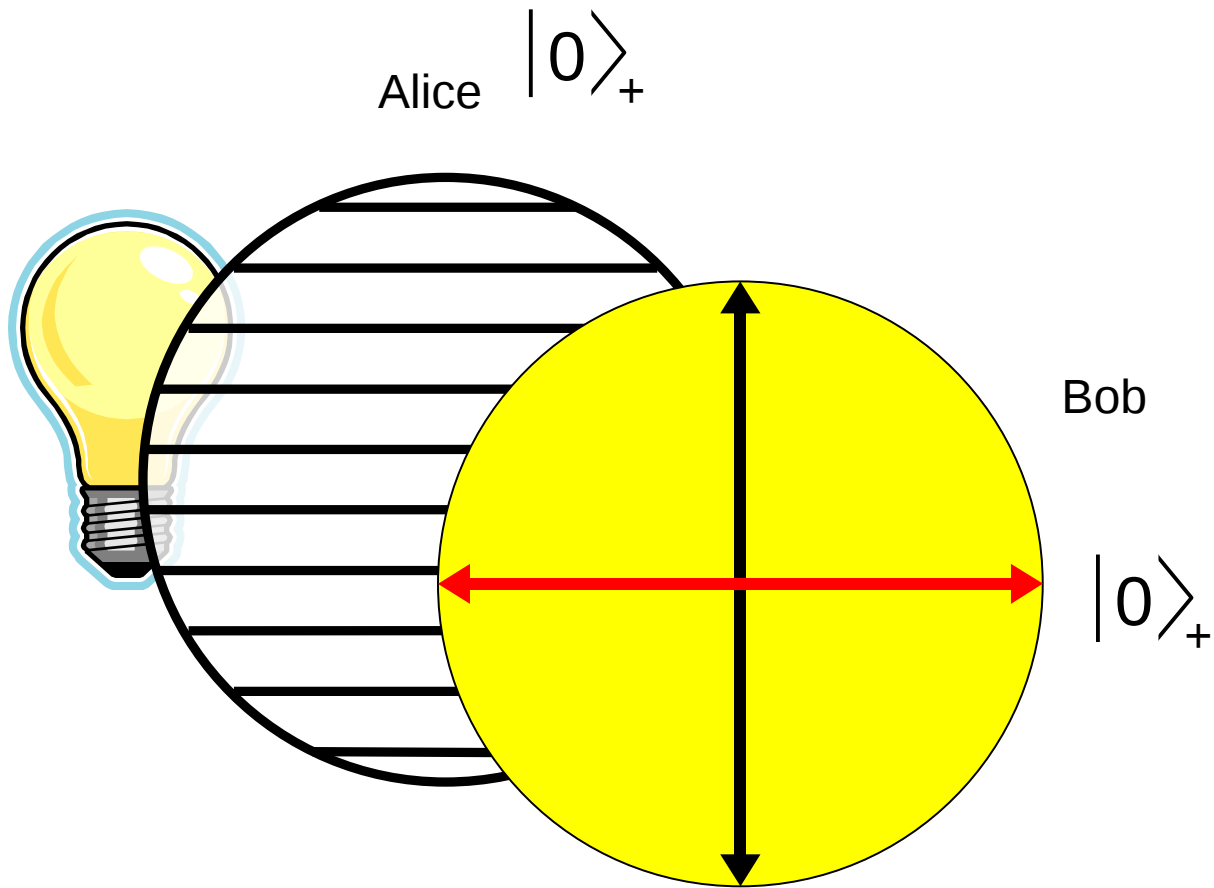


How does it work?

Alice $|0\rangle_+$

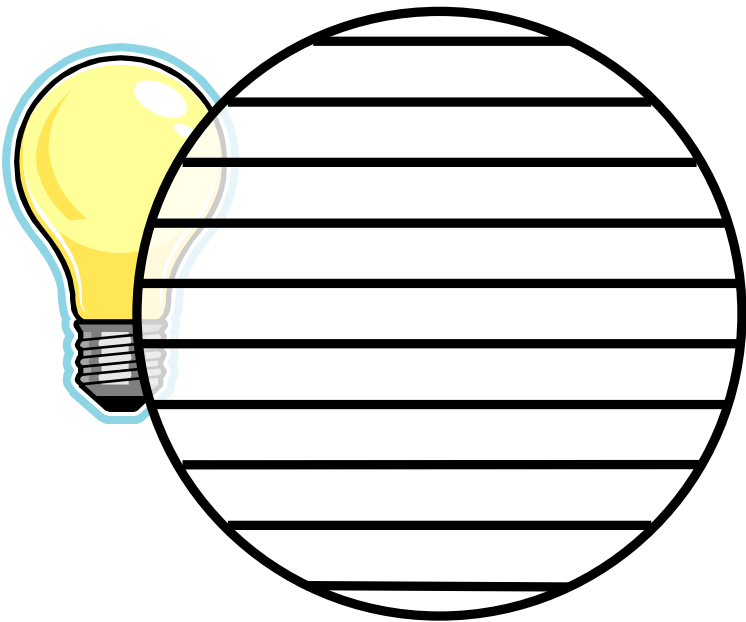


How does it work?

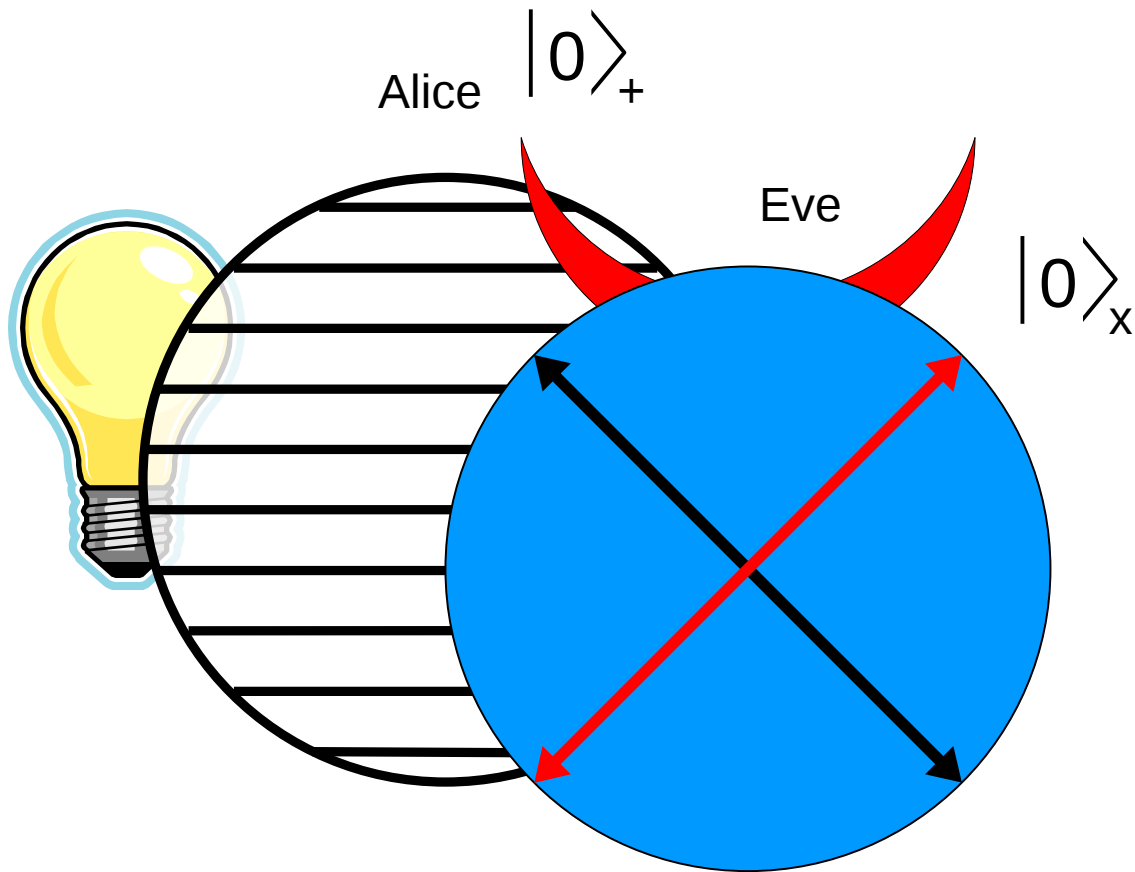


How does it work?

Alice $|0\rangle_+$

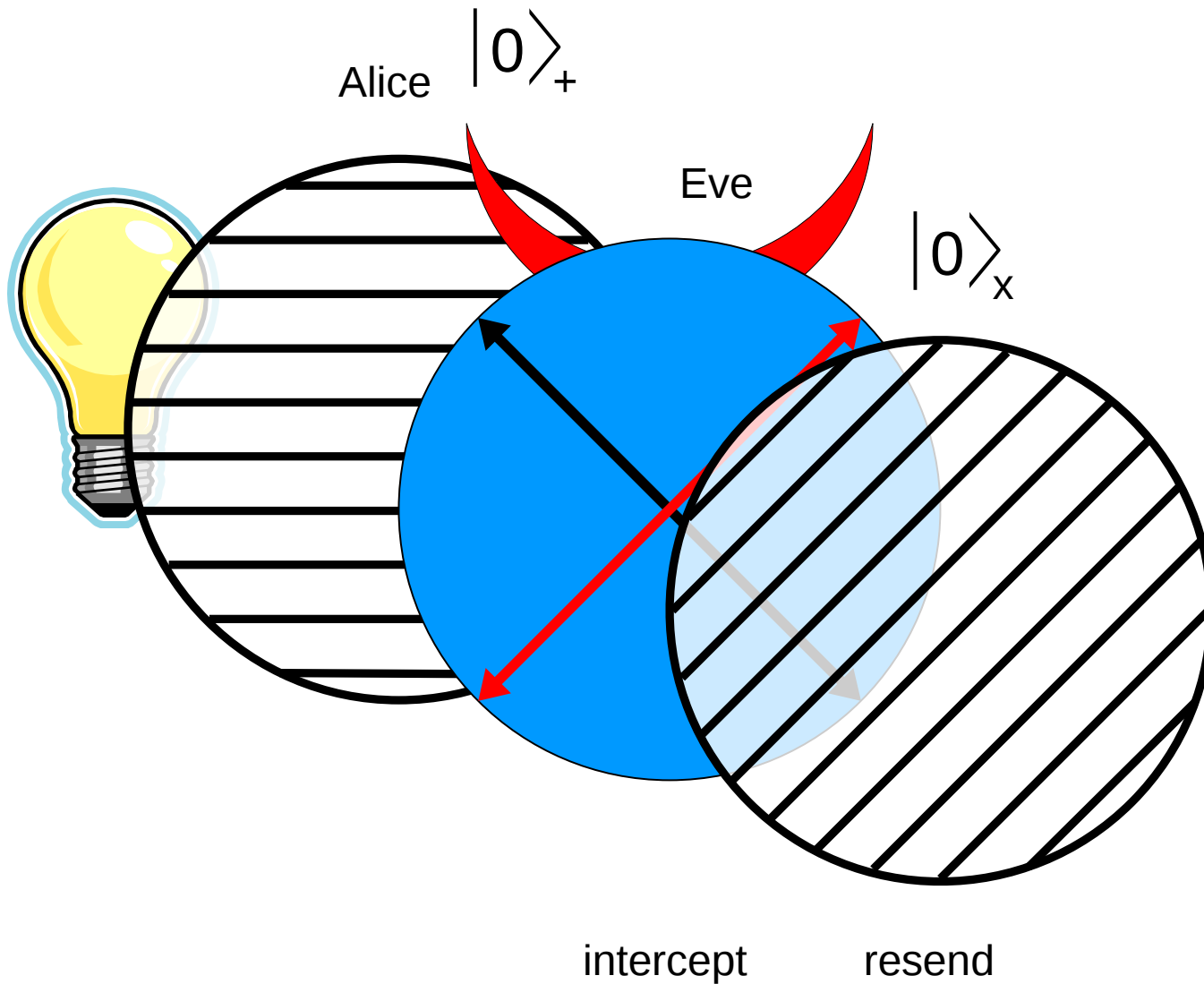


How does it work?

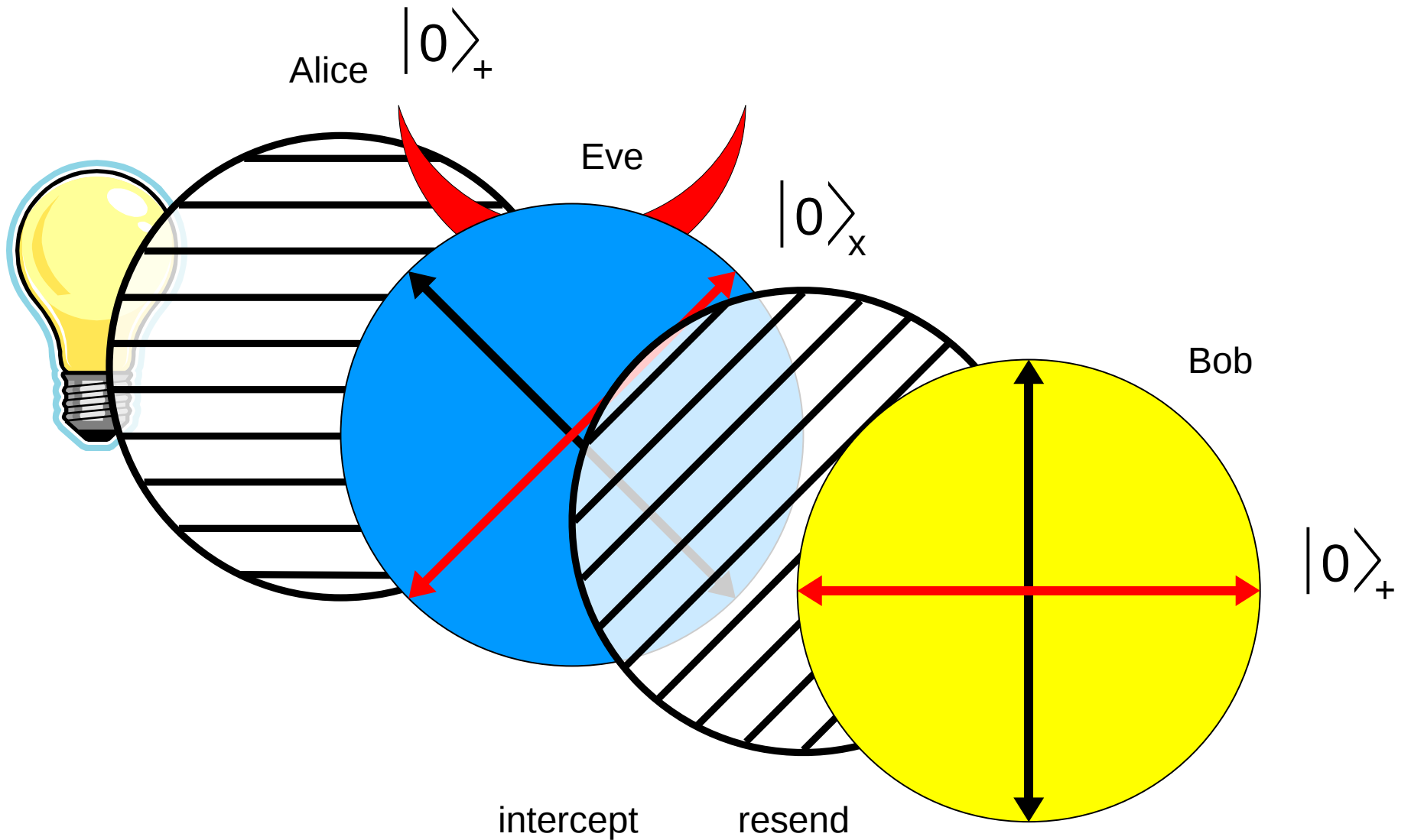


intercept

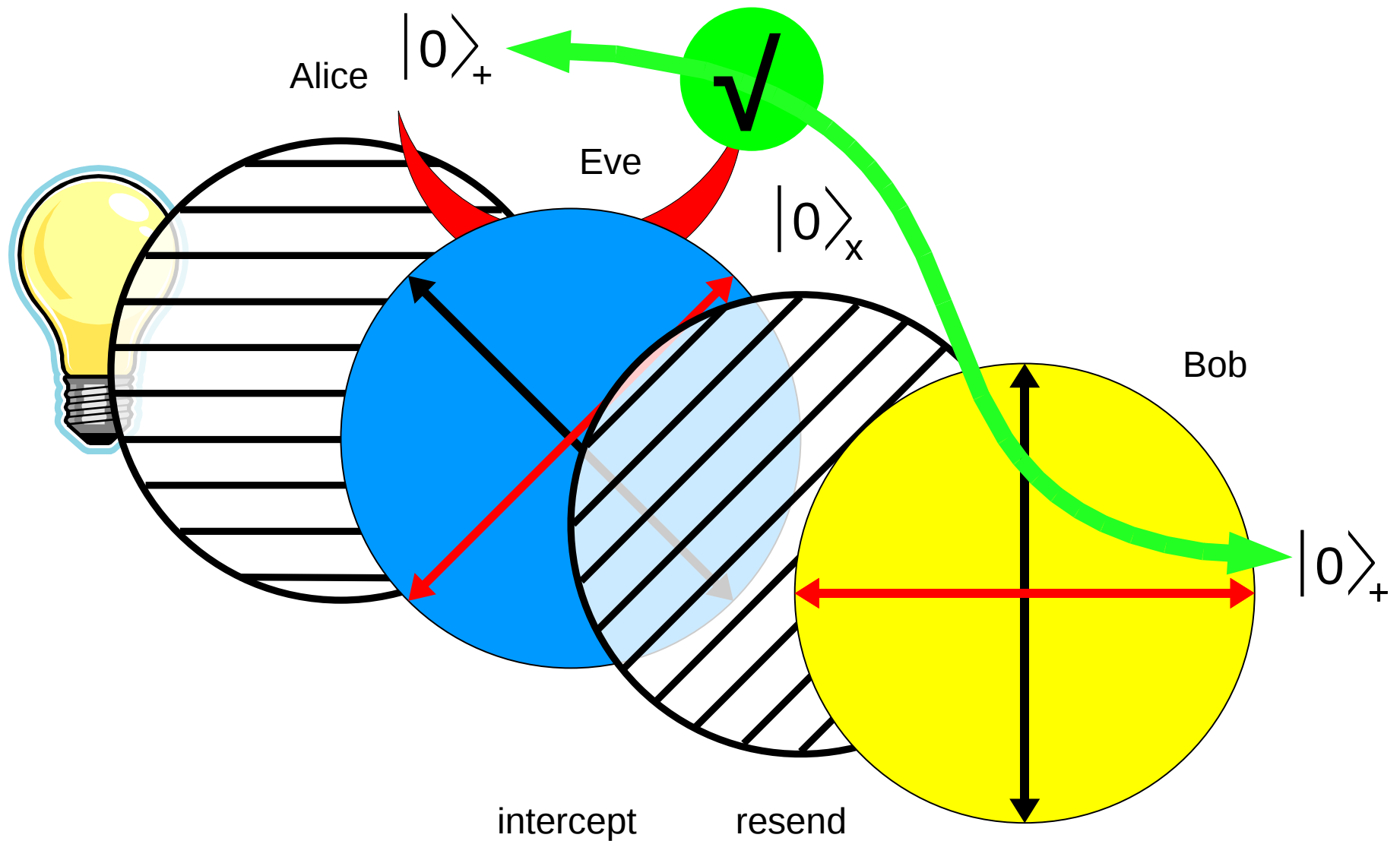
How does it work?



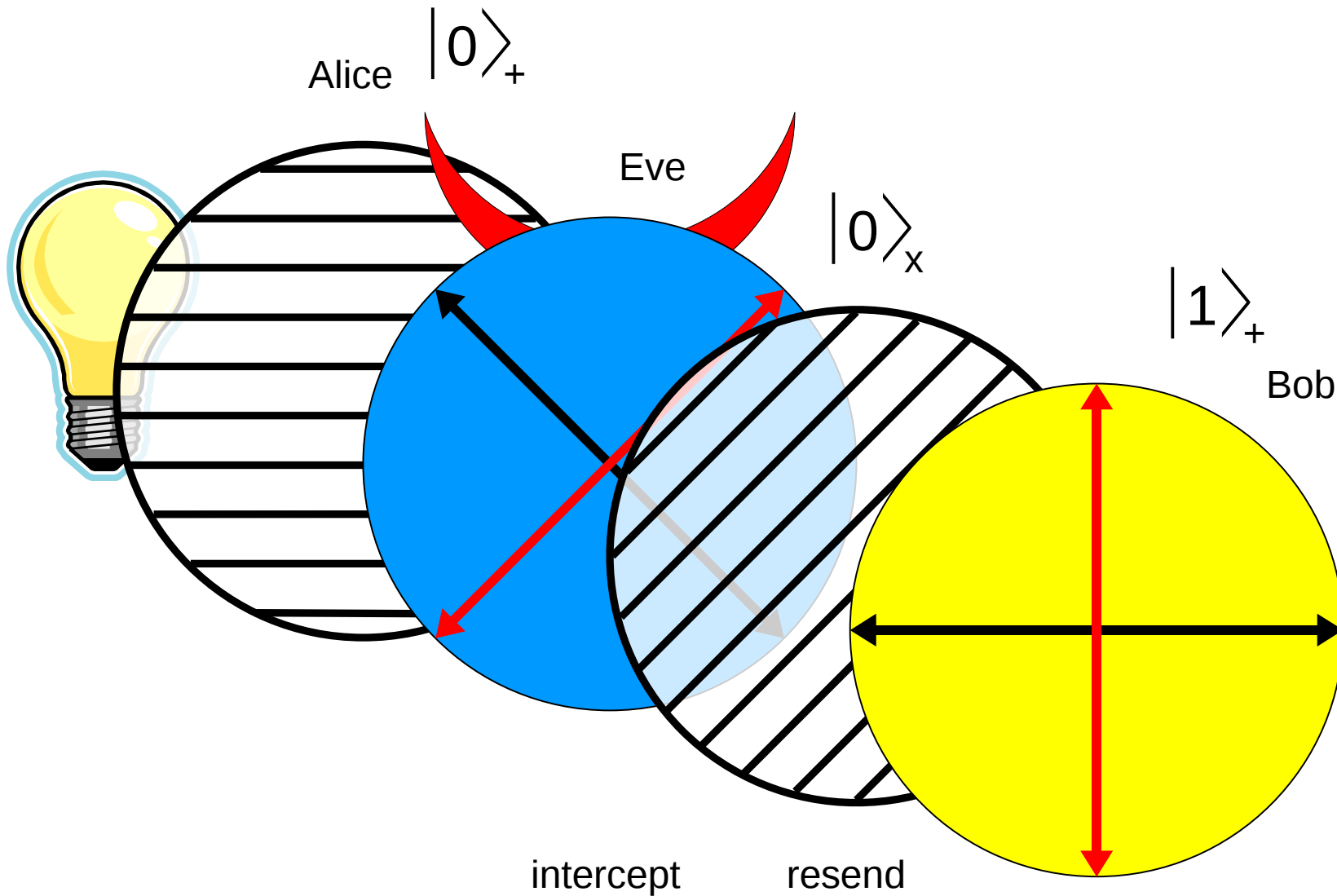
How does it work?



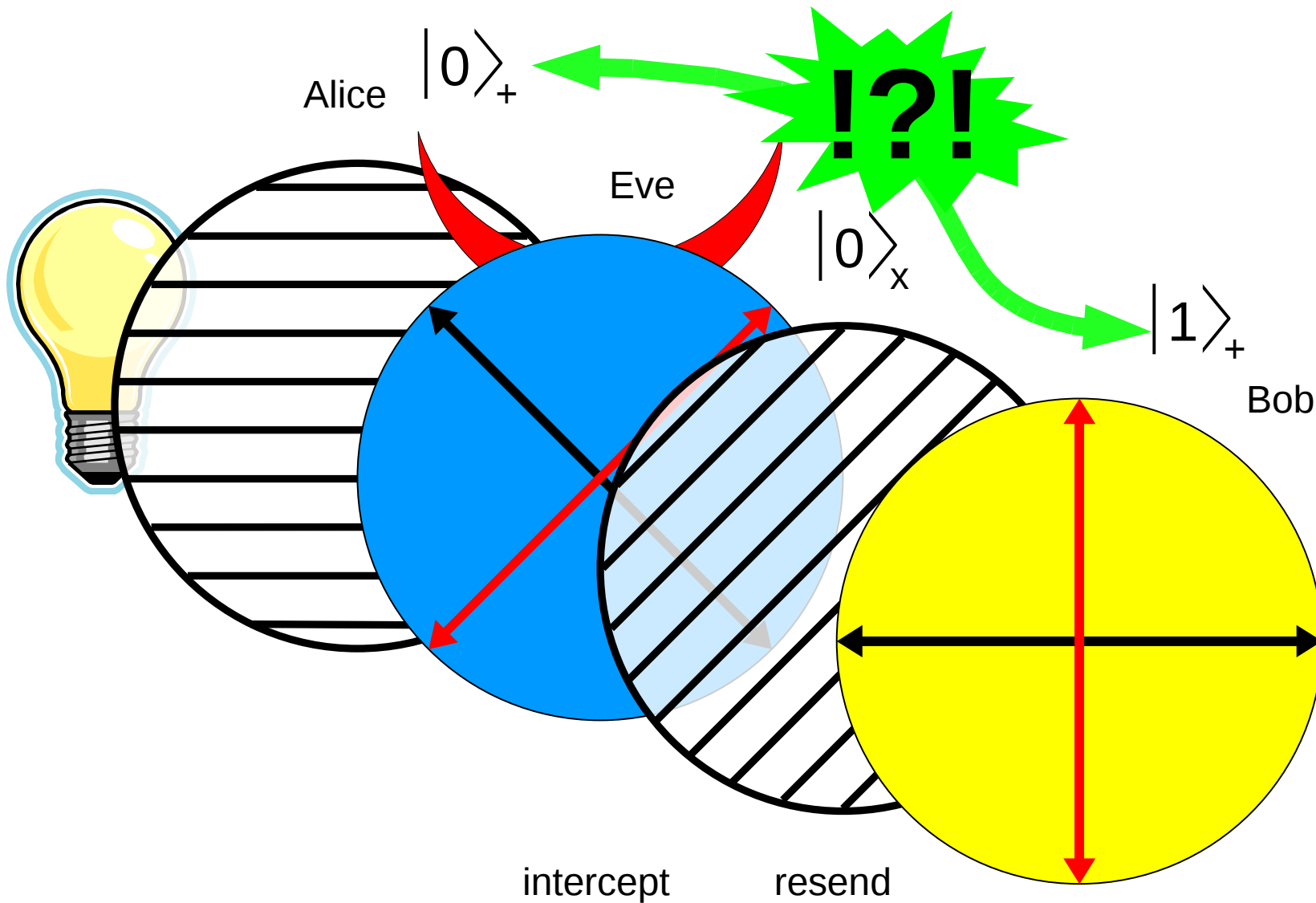
How does it work?



How does it work?



How does it work?



BB84

BB84

ALICE

BOB

BB84

ALICE

0 1 1 0

BOB

BB84

ALICE

BOB

0

1

1

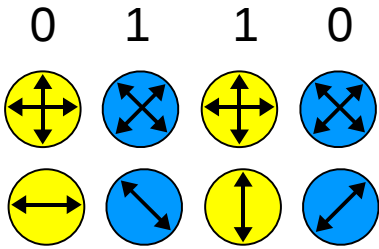
0



BB84

ALICE

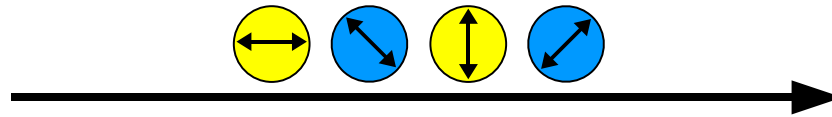
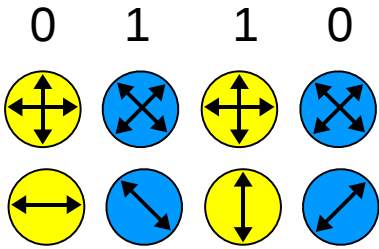
BOB



BB84

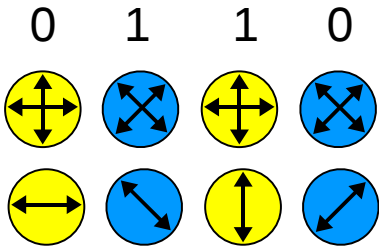
ALICE

BOB

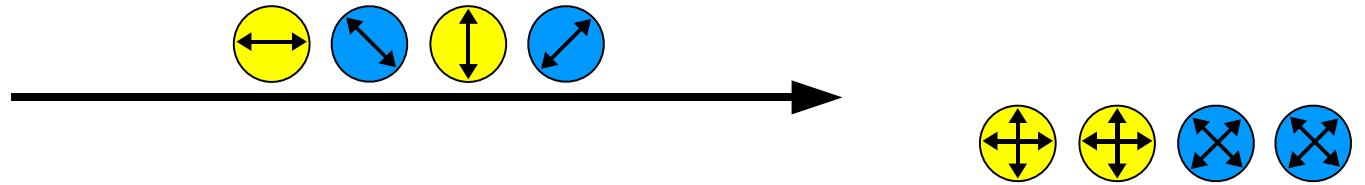


BB84

ALICE

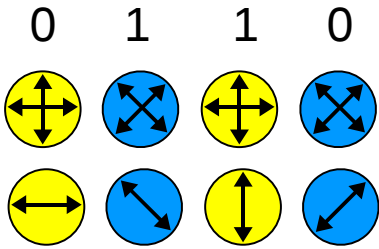


BOB

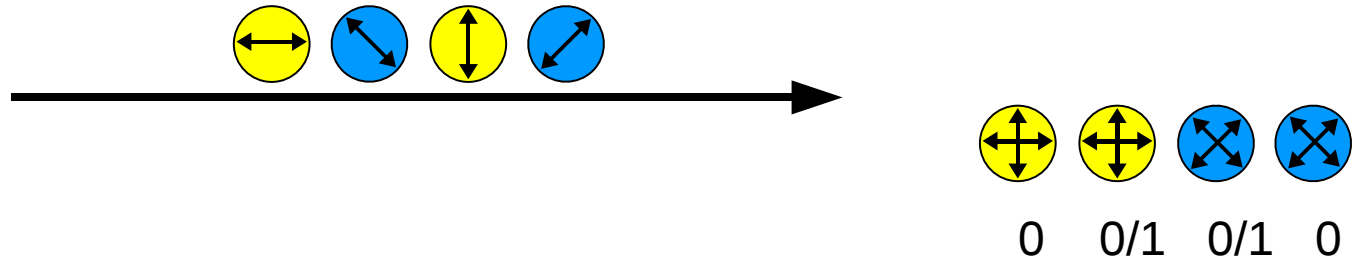


BB84

ALICE



BOB

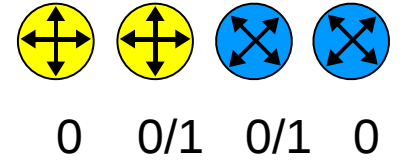
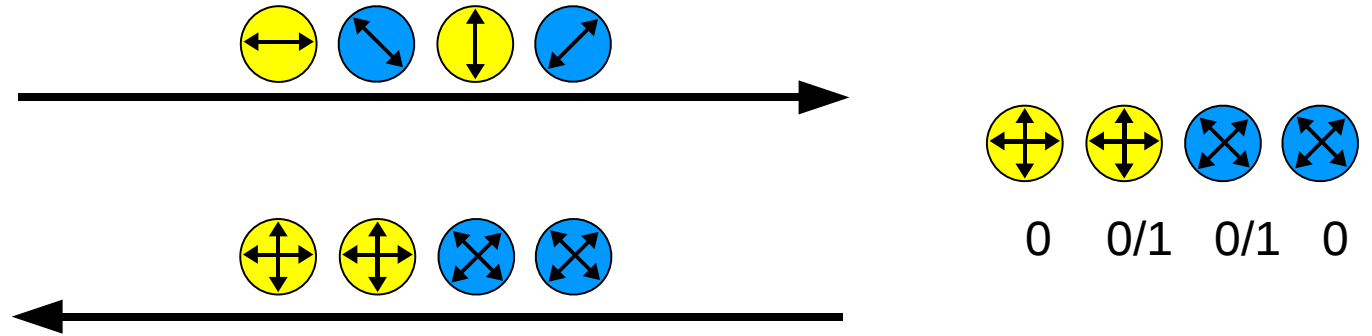


BB84

ALICE



BOB

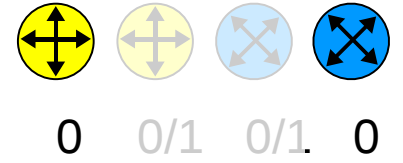
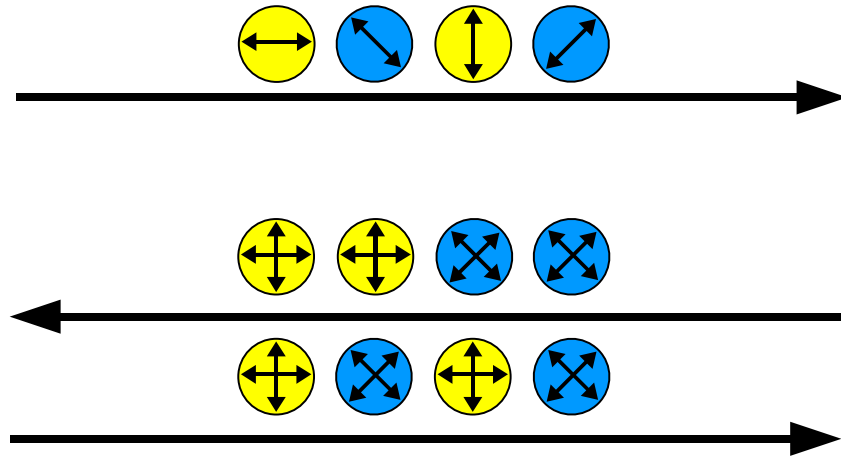


BB84

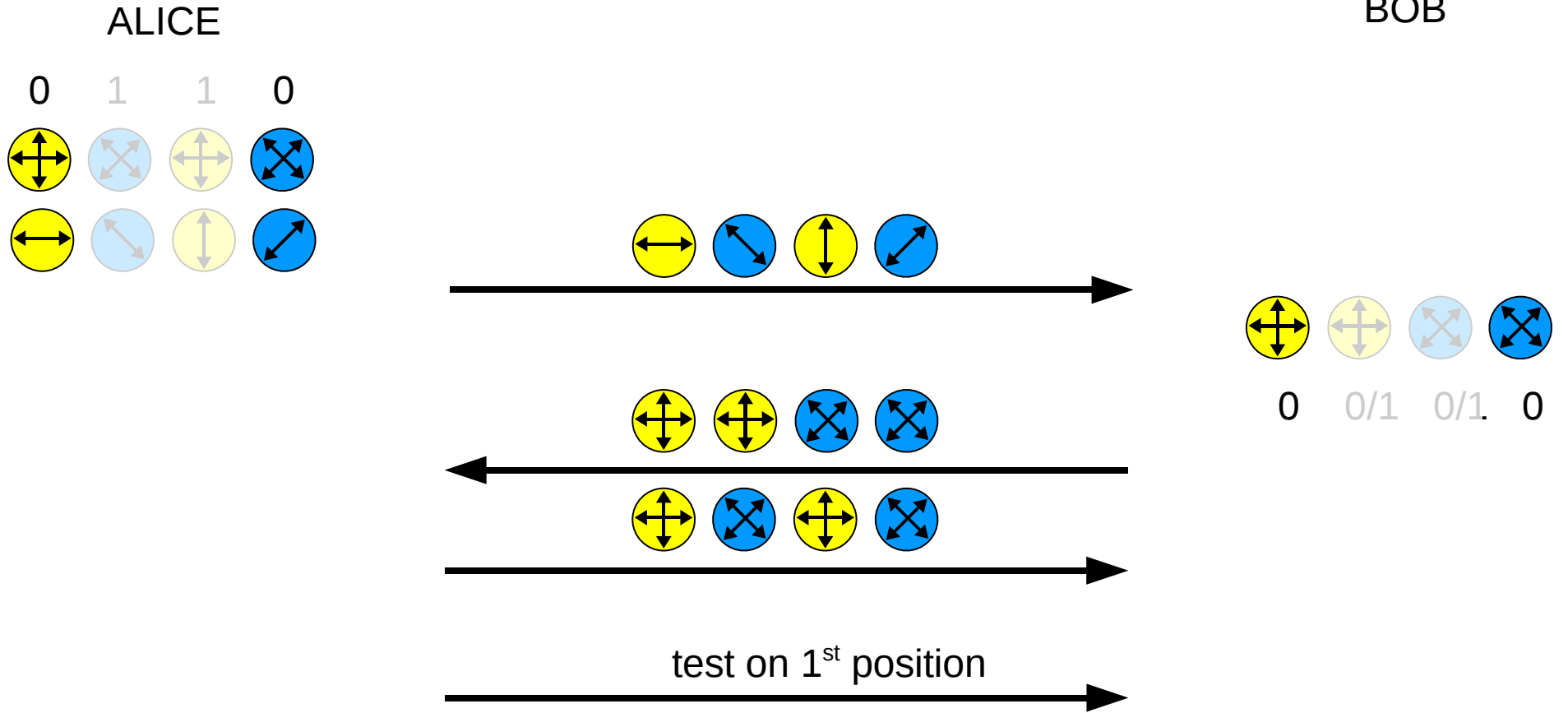
ALICE



BOB



BB84

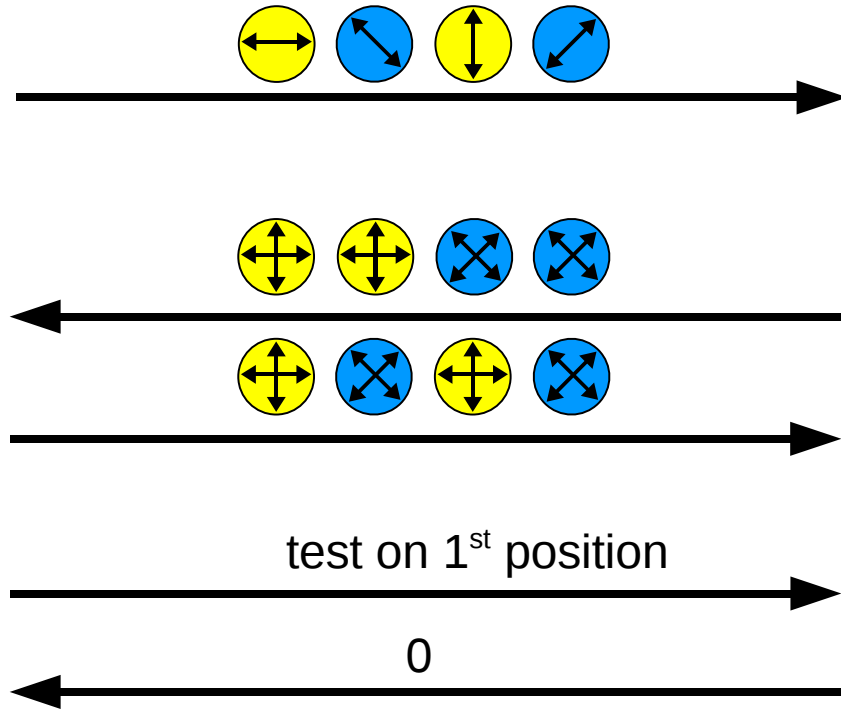


BB84

ALICE



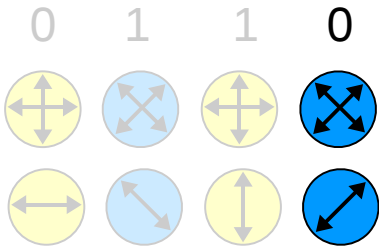
BOB



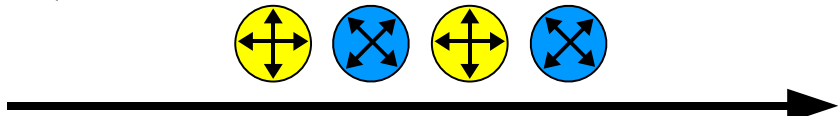
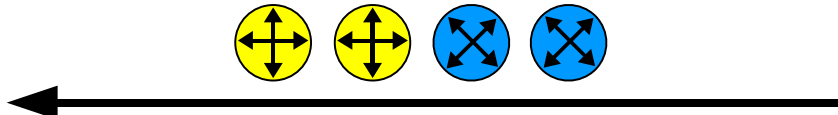
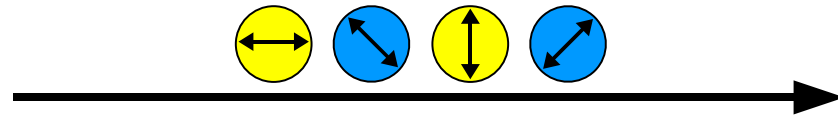
$$0 = 0 \checkmark$$

BB84

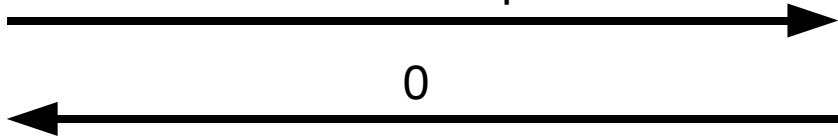
ALICE



BOB



test on 1st position



0 = 0 ✓

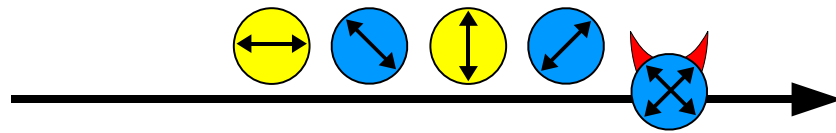
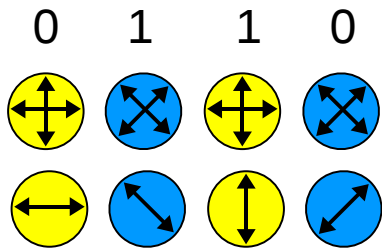
okay



BB84

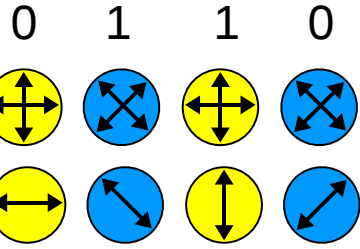
ALICE

BOB

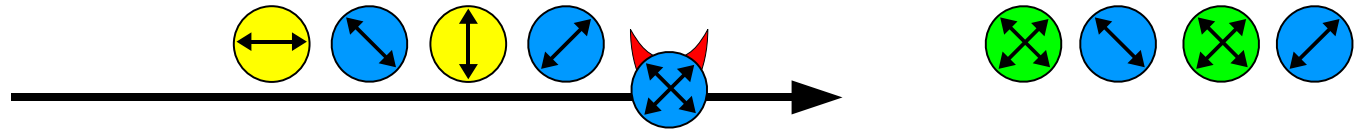


BB84

ALICE

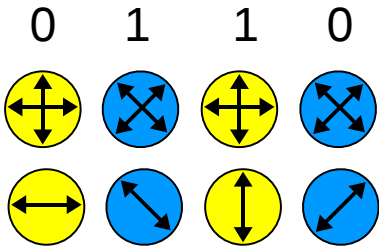


BOB

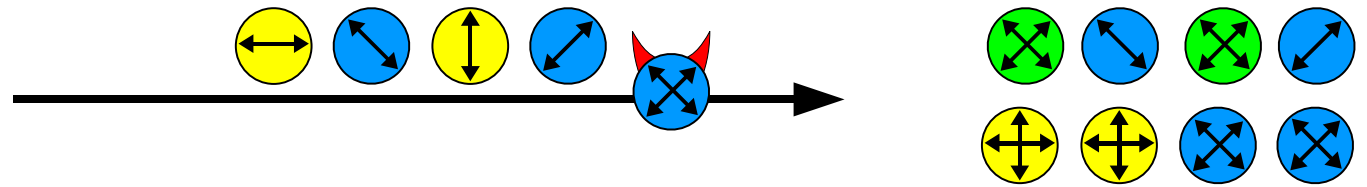


BB84

ALICE

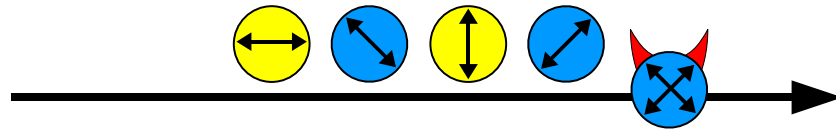
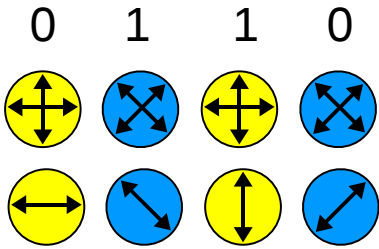


BOB

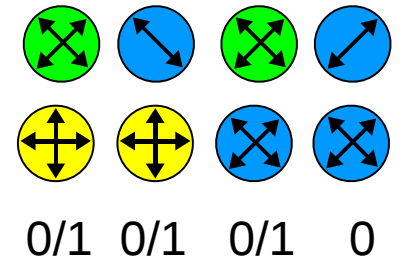


BB84

ALICE



BOB

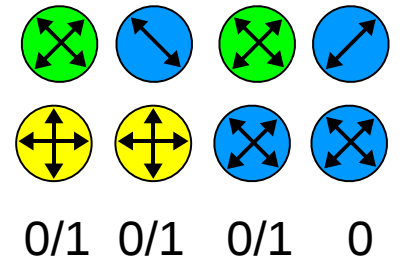
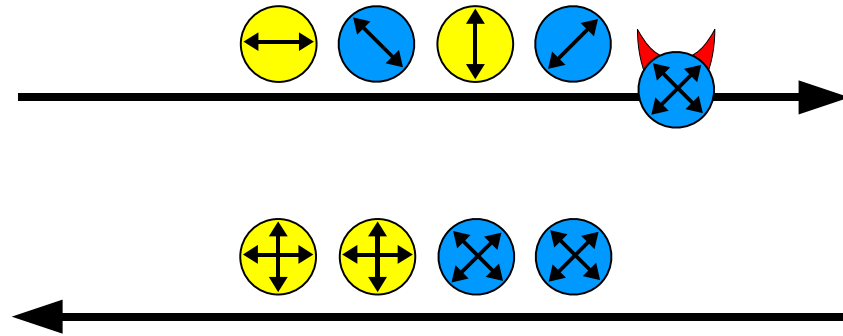


BB84

ALICE

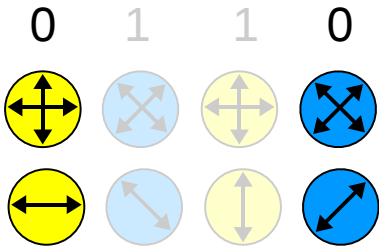


BOB

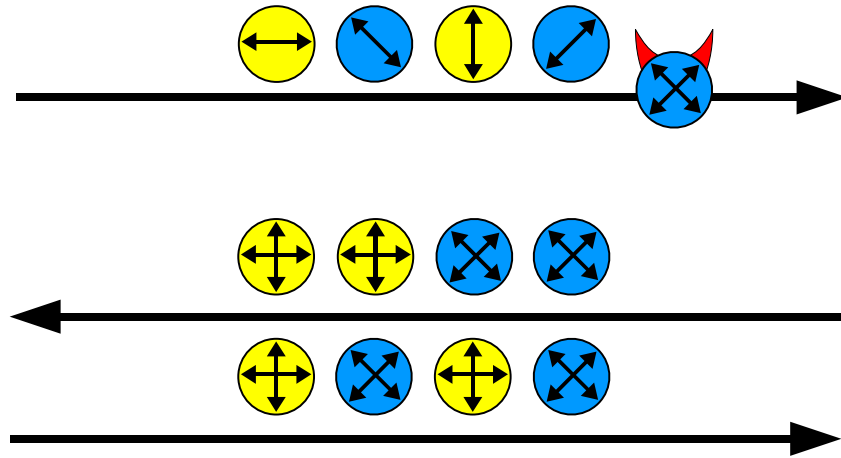


BB84

ALICE



BOB

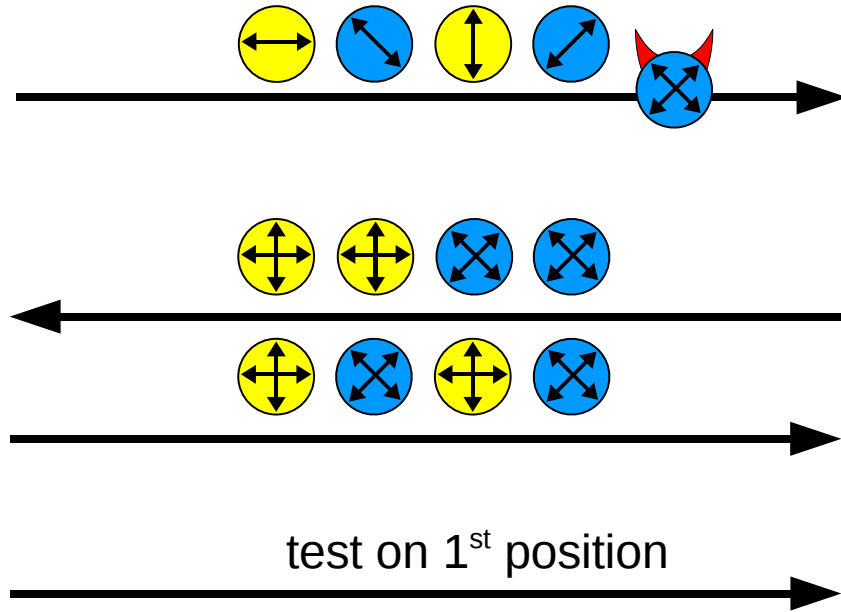


BB84

ALICE



BOB

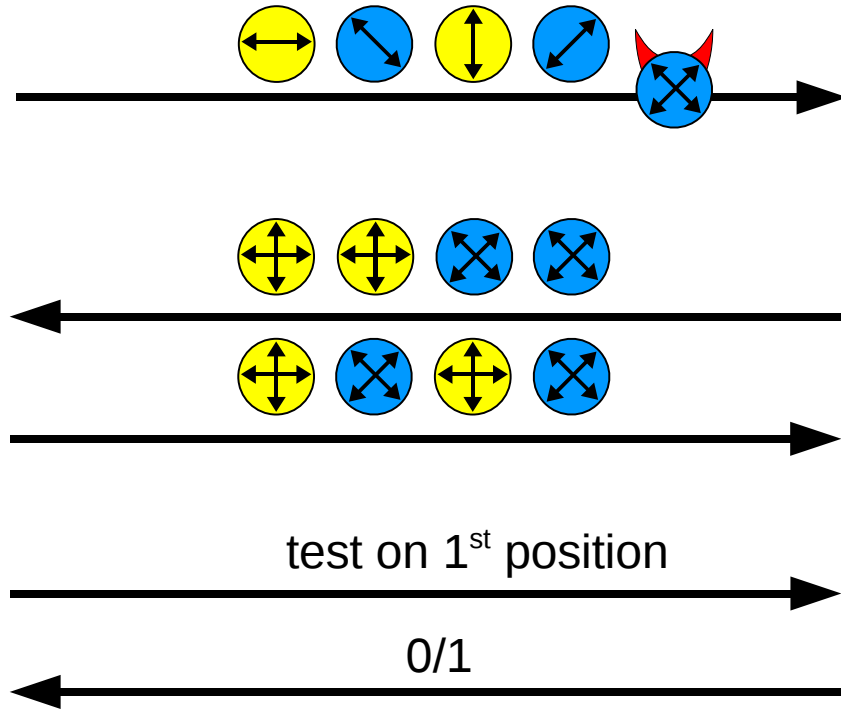


BB84

ALICE



BOB



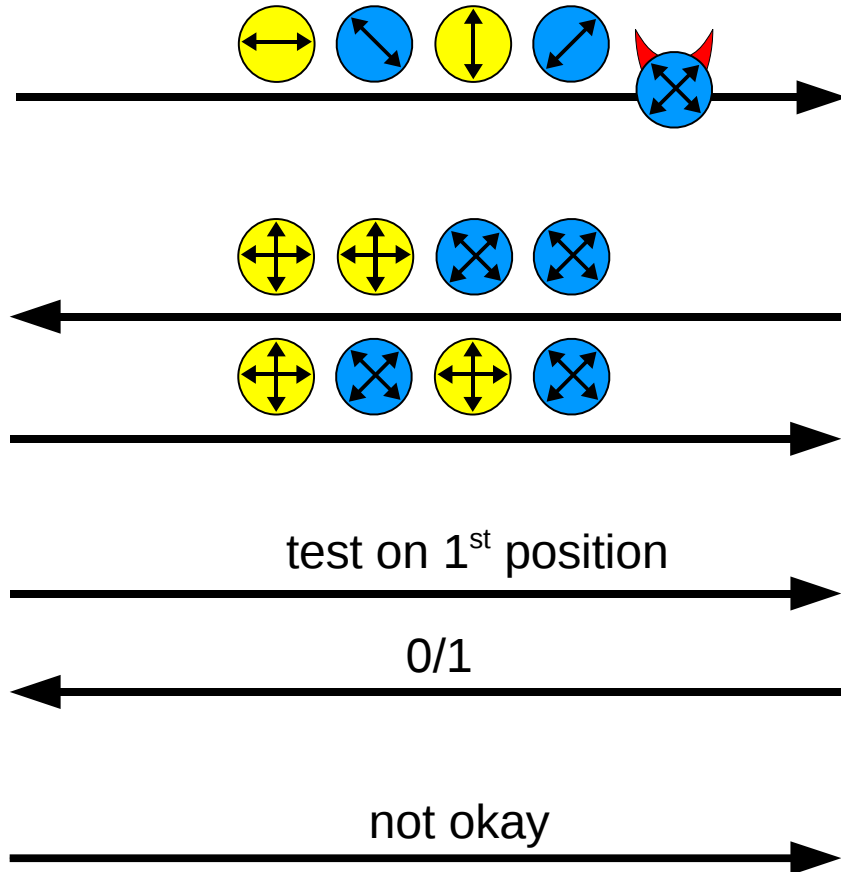
!?!

BB84

ALICE



BOB



!?!

not okay

Quantum Facts

- (1) QKD results in common, secret, random bitstring.**
 - > Key for OTP

Quantum Facts

(1) QKD results in common, secret, random bitstring.

--> Key for OTP

(2) Any measurement (= observation) disturbs the system.

--> Eavesdropping disturbs the system.

--> Eavesdropping can be detected.

--> Information gain vs disturbance.

Quantum Facts

(1) QKD results in common, secret, random bitstring.

--> Key for OTP

(2) Any measurement (= observation) disturbs the system.

--> Eavesdropping disturbs the system.

--> Eavesdropping can be detected.

--> Information gain vs disturbance.

(3) No-Cloning Theorem.

--> An unknown quantum state cannot be copied.

Quantum Facts

(1) QKD results in common, secret, random bitstring.

--> Key for OTP

(2) Any measurement (= observation) disturbs the system.

--> Eavesdropping disturbs the system.

--> Eavesdropping can be detected.

--> Information gain vs disturbance.

(3) No-Cloning Theorem.

--> An unknown quantum state cannot be copied.

(4) Provable security based on physical laws.