UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

THE TWO GOLDEN RULES OF QUANTUM MECHANICS

SESSION #1

Learning Objectives

- The role of probabilities in quantum mechanics
  - Outcomes are not *necessarily* definite
- The nature of quantum superposition
  - Superposition as a *relative* concept
- Measurement disturbance
  - We can't make two *incompatible* measurements at once
- We can apply these ideas to build technologies
  - Quantum cryptography is based on quantum measurement

Prerequisite Knowledge

- Light is a wave with a **polarization**
  - Crossed polarizers should be familiar
- Light is emitted in units called **photons**
  - Previous encounter with the photoelectric effect
- The Cartesian plane and vector components
  - If advanced, can be taught using formal linear algebra
  - Otherwise, perfectly possible to avoid

Opening Question

What is a quantum measurement?

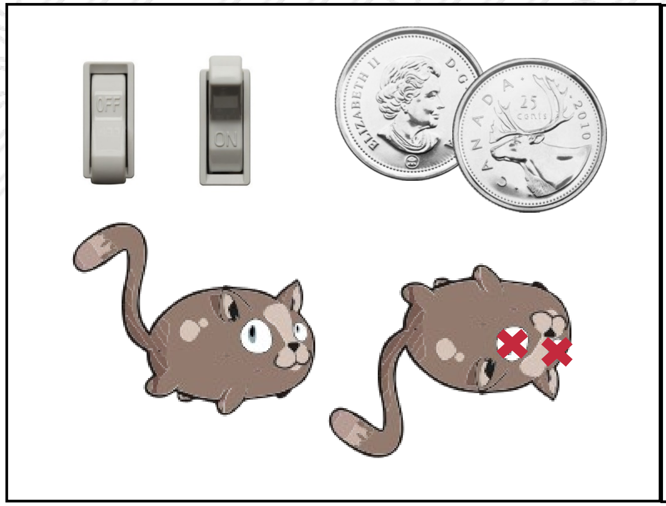
Mutually Exclusive States

A **quantum measurement** distinguishes between two or more **mutually exclusive states**.

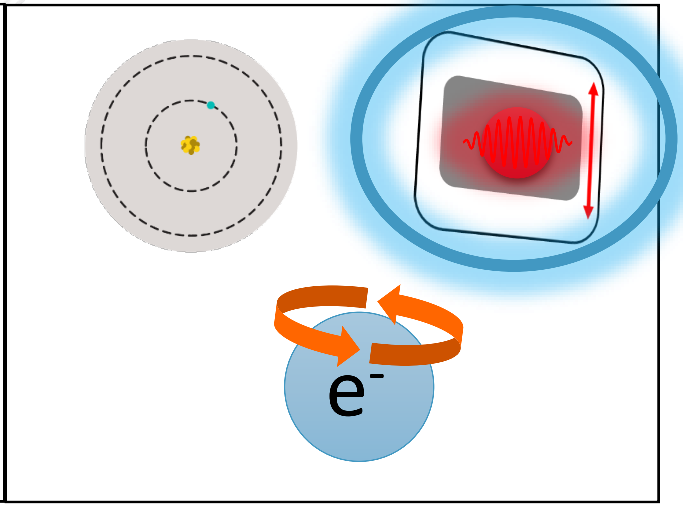
Two states are **mutually exclusive** if being found in one state means it definitely isn't in the other.

The measurement tells us which of the two states our object was in.

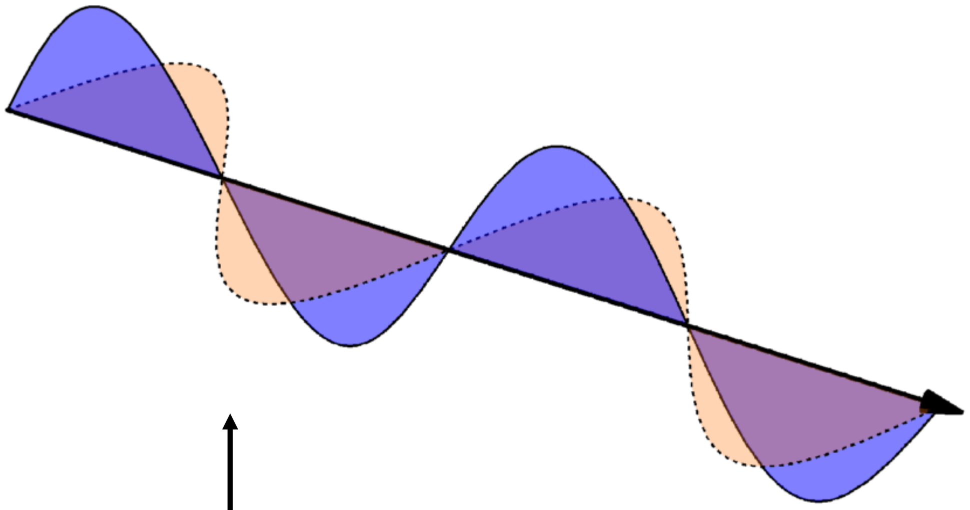
Classical Examples

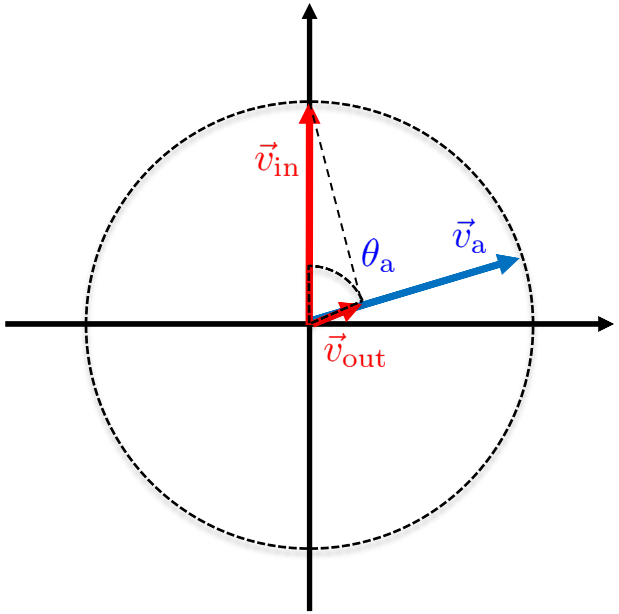


Quantum Examples

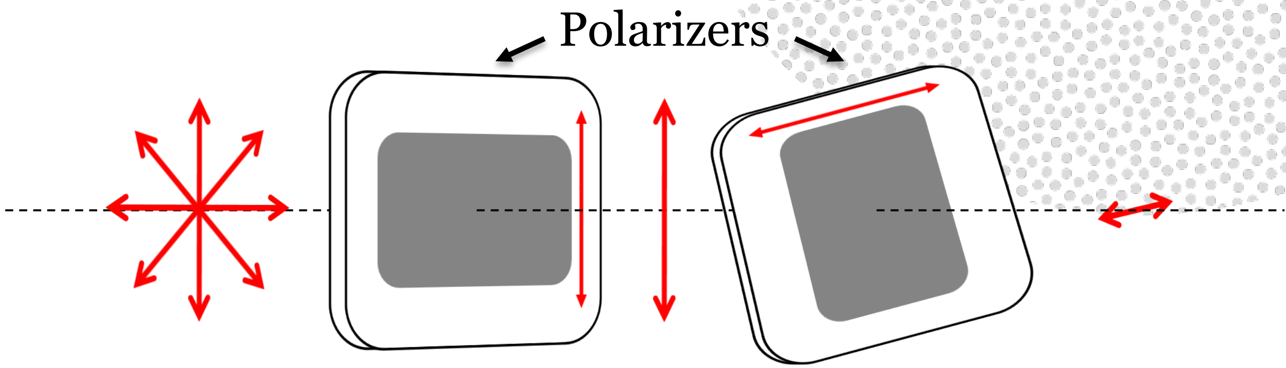


Polarization of Light: Wave Picture





$$I_{\text{out}} = ||\vec{v}_{\text{out}}||^2$$
$$= |\vec{v}_{\text{in}} \cdot \vec{v}_{\text{a}}|^2$$

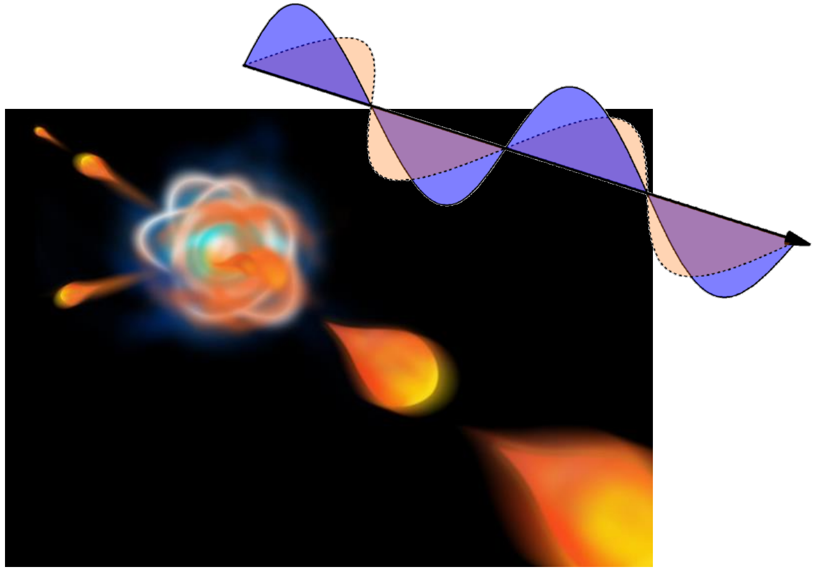


$$I_{out} = I_{in} \cos^2 \theta$$

Malus' Law

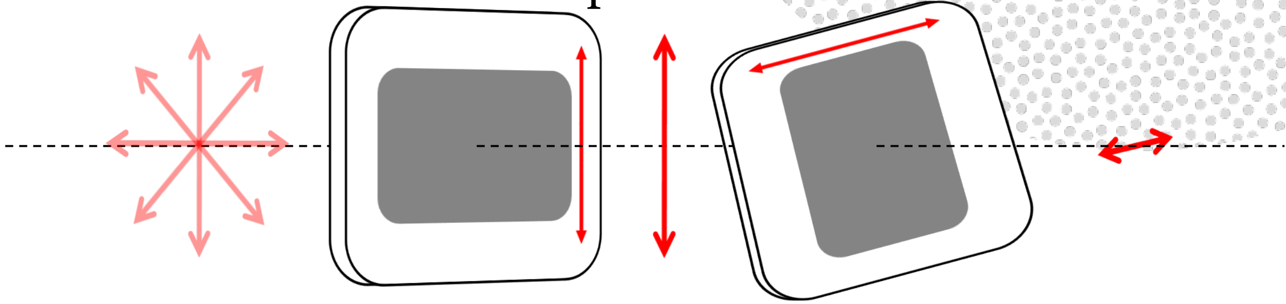
The intensity of light that makes it through the analyzer depends on the angle between the analyzer and the light's polarization.

Polarization of Light: Photon Picture



Light is made up of **photons.**
What happens to a
single photon of light
at a polarizer?

<u>One</u>
vertically polarized
photon



Two possibilities:

1) The photon passes through the analyzer
2) The photon is absorbed

$$\mathrm{Prob}(out) = \cos^2\theta$$

We must consider the **<u>probability</u>**
of each event occurring

Malus' Law with Photons

A horizontally polarized single photon is incident on a polarizer at angle θ.
What are the probabilities of it being absorbed or transmitted?

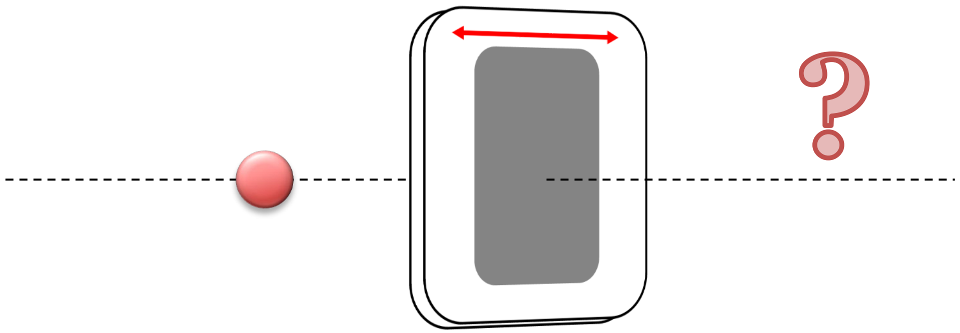
		$\theta = 0°$	$45°$	$-45°$	$-30°$	$60°$	$90°$	
$\frac{I_{out}}{I_{in}} = \cos^2\theta$	I_{out}/I_{in}	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{4}$	0	Wave picture
$Prob(out) = \cos^2\theta$	**Probability transmitted**	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{4}$	0	Photon picture
$Prob(abs) = \sin^2\theta$	**Probability being absorbed**	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{3}{4}$	1	

Mathematically, no difference between wave and photon picture.
But the **interpretation** differs greatly.

Breakout Session

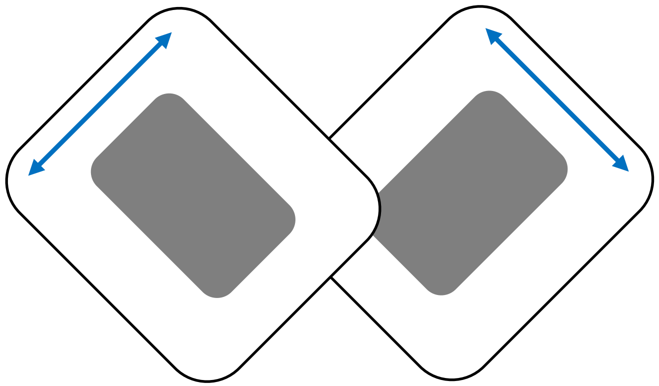
1. Which polarization states are **mutually exclusive**?

2. If a photon makes it through a horizontal polarizer, what can we conclude about its polarization state before and after the polarizer?

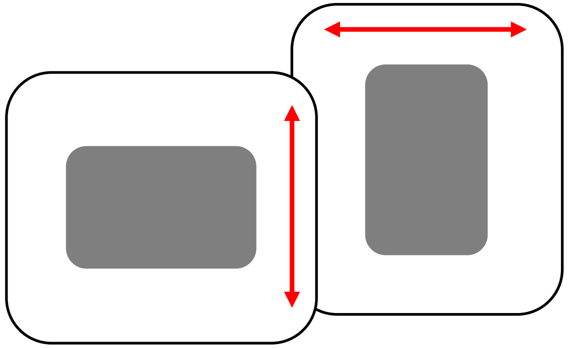


Polarization Measurements

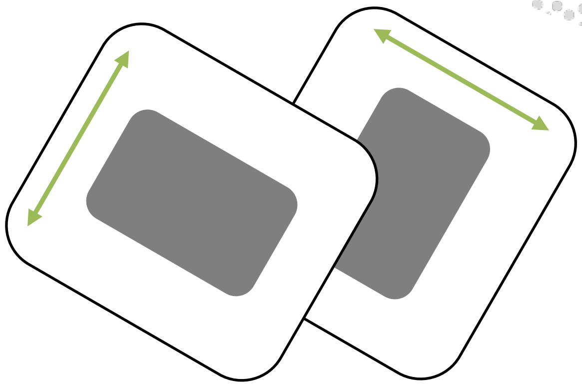
The polarizer asks the photons a question, such as:



Are you
+45° or -45°
polarized?



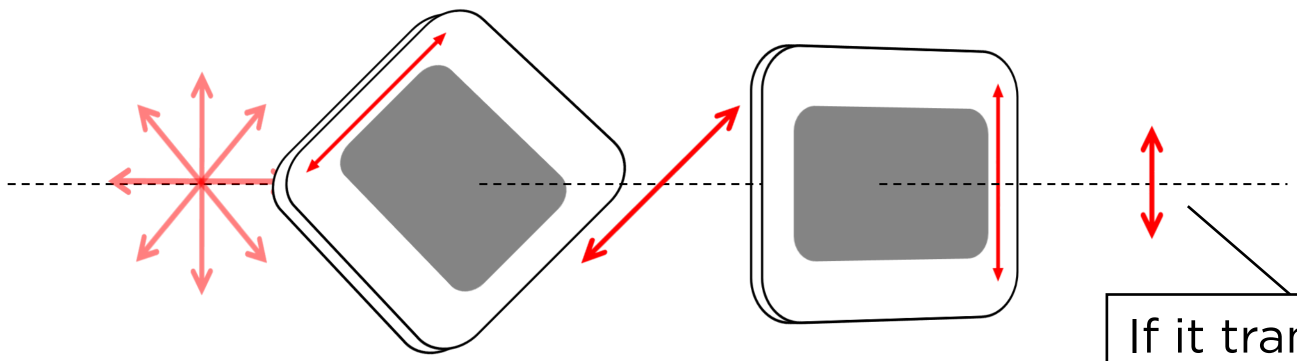
Are you
horizontally
or vertically
polarized?



Are you
+30° or -60°
polarized?

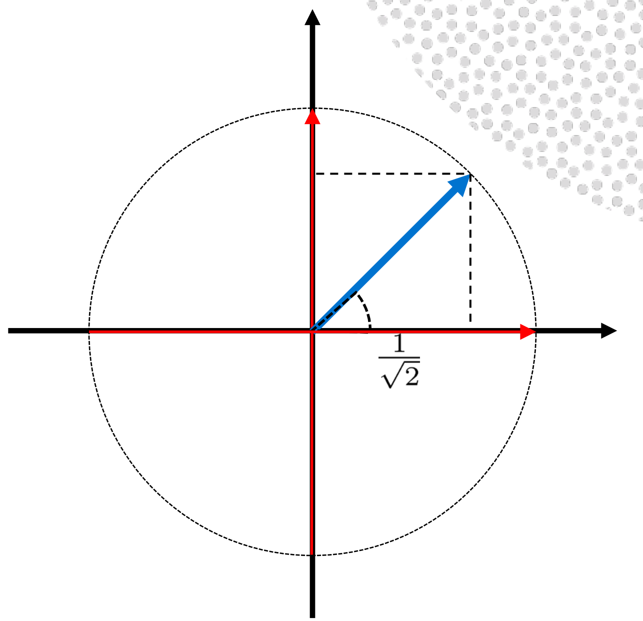
A pair of mutually exclusive quantum states is called a **measurement basis**

Asking questions with polarizers



To solve, we need to describe it in the HV **basis**

If it transmits, it is now vertically polarized

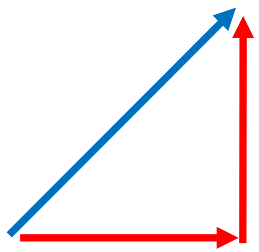


$$\nearrow = \frac{1}{\sqrt{2}}\left(\rightarrow + \uparrow\right)$$

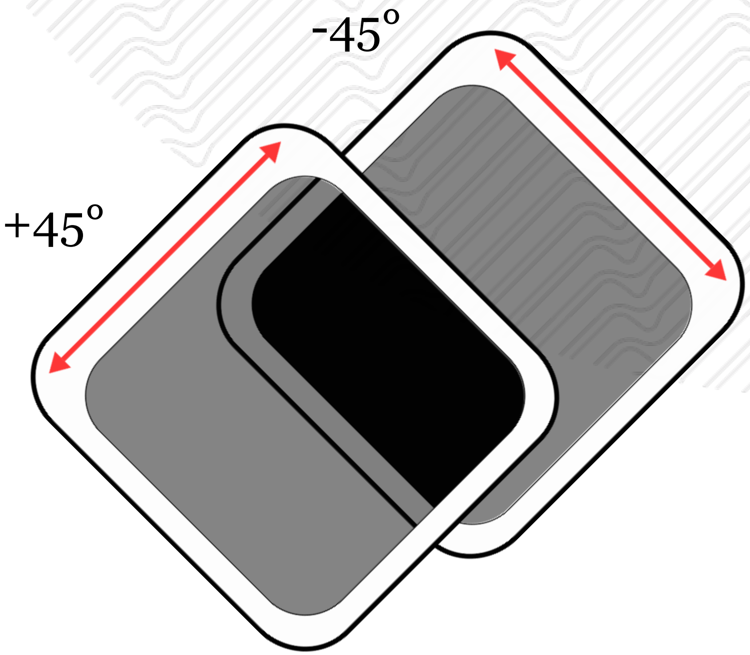
50% Probability Transmitted

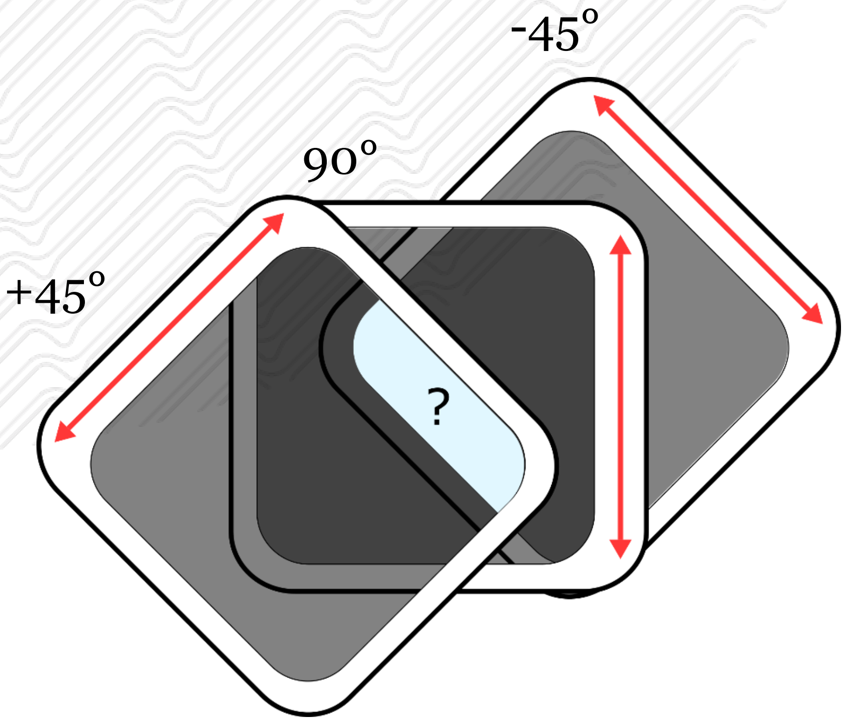
50% Probability Absorbed

Intuitively, can think about as vector addition



Polarization beyond Malus' Law

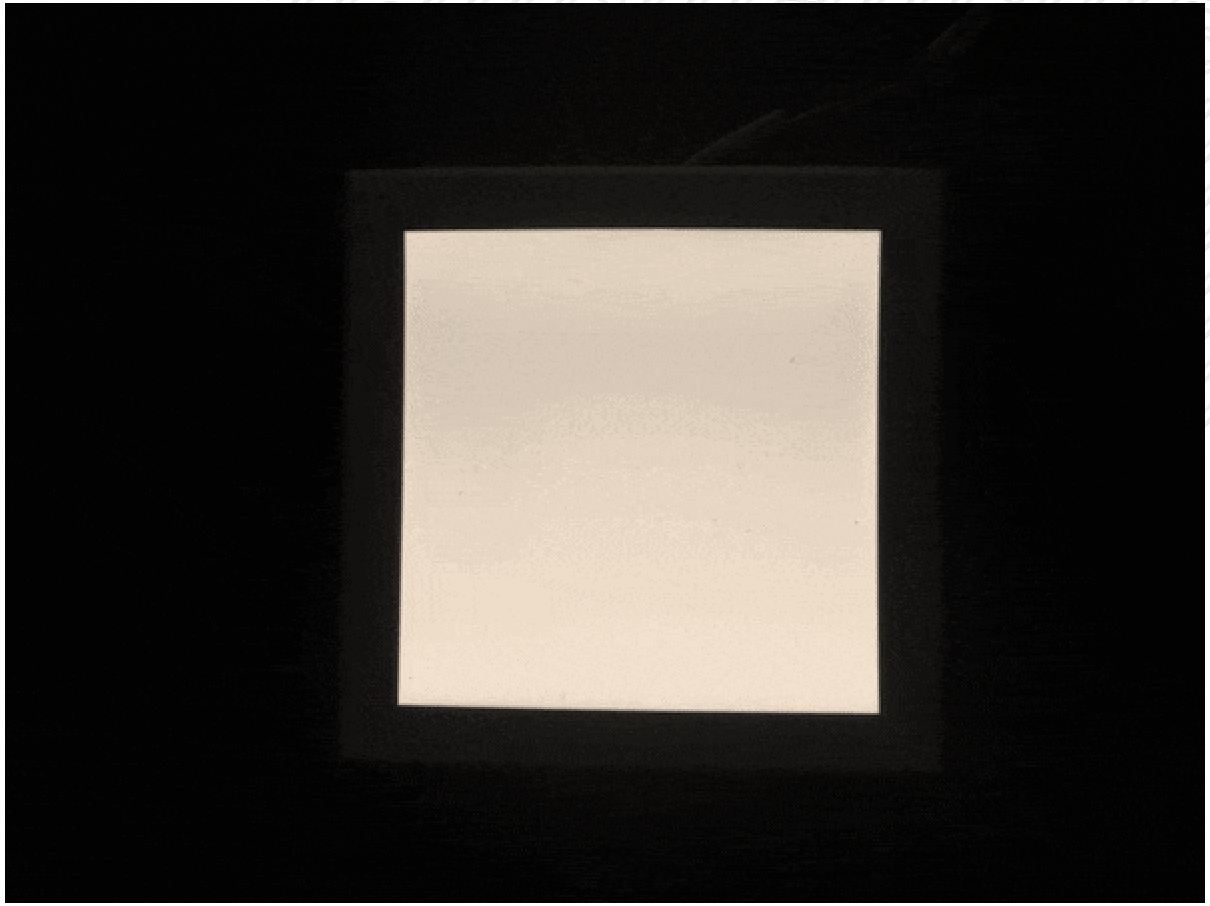


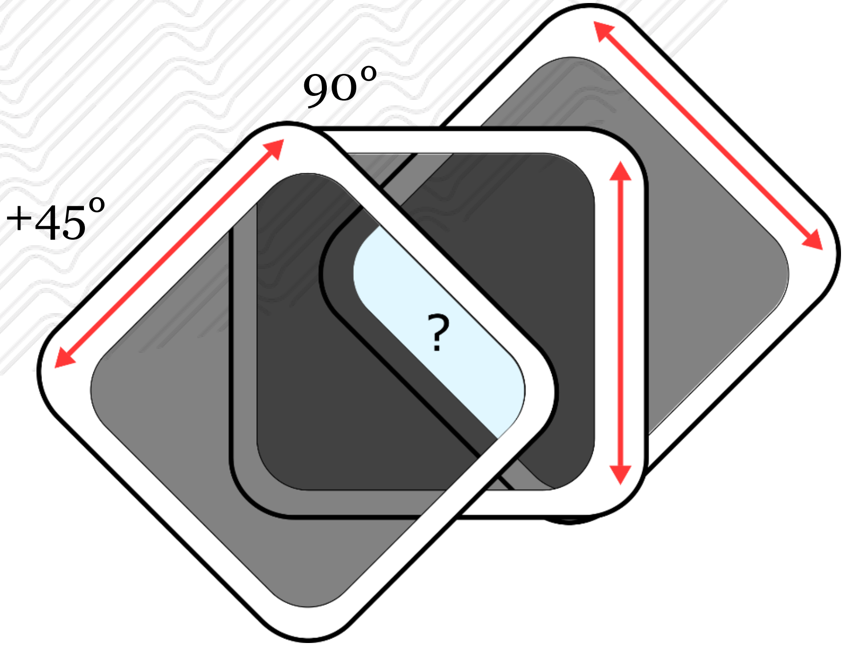


Two crossed polarizers
No light passes through

Three polarizers
???

Polarization beyond Malus' Law

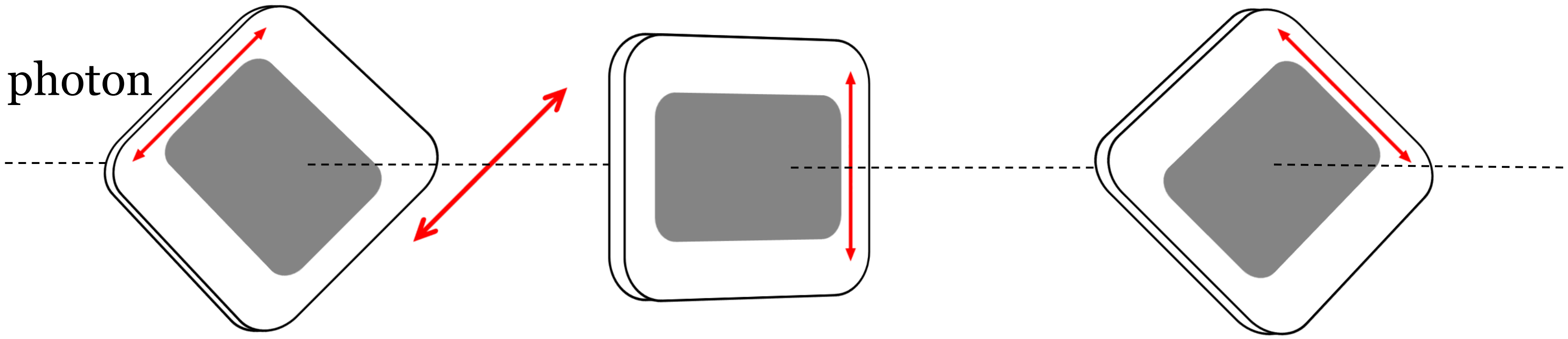




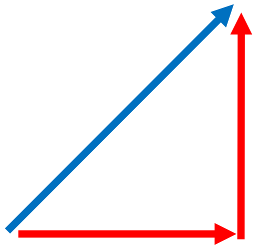
Three polarizers
???

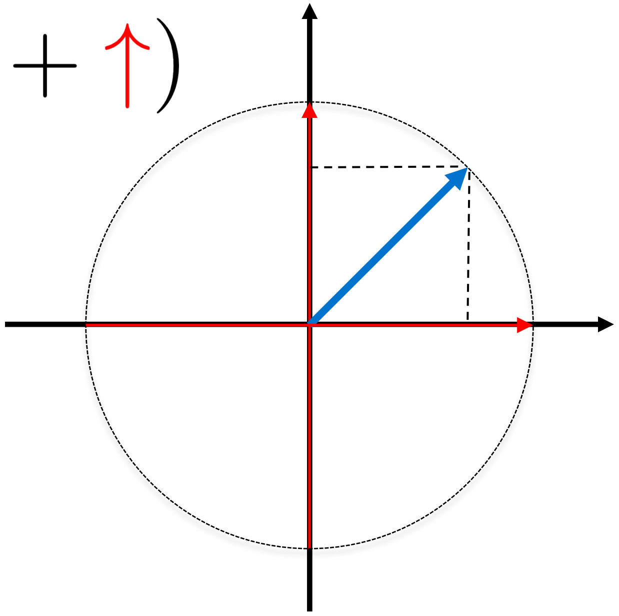
Superposition and Measurement

<u>One</u>
+45°-polarized photon



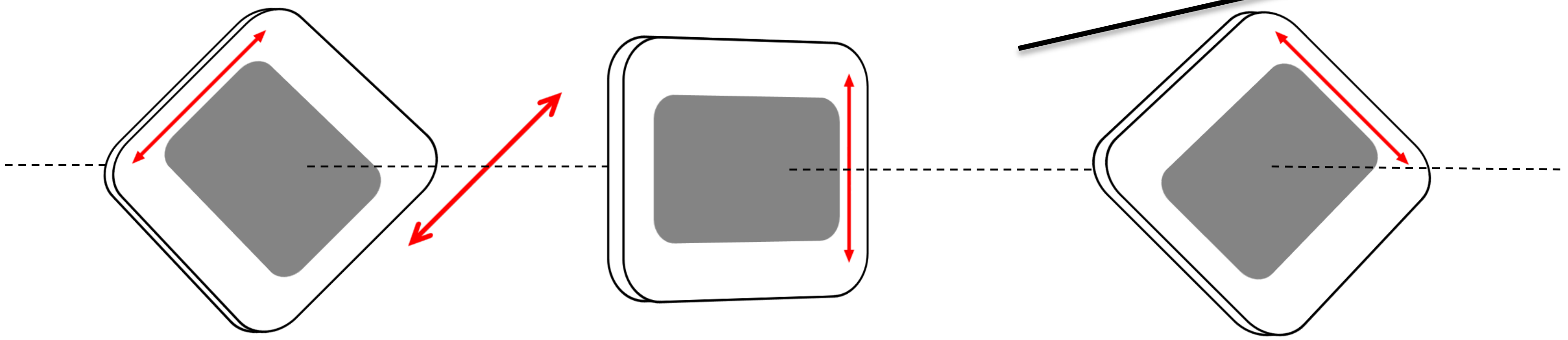
$$\nearrow = \frac{1}{\sqrt{2}}\left(\rightarrow + \uparrow\right)$$





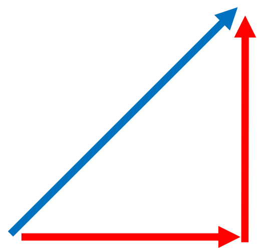
Superposition and Measurement

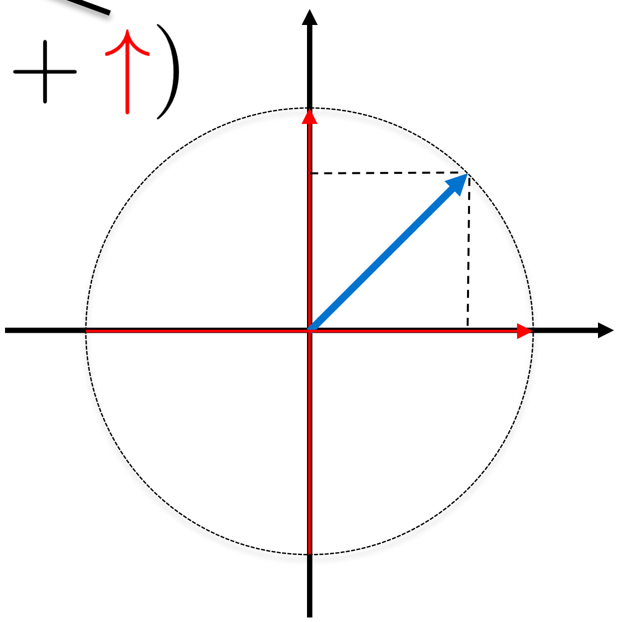
If it transmits, it's definitely **vertical** now



Transmits with 50% probability

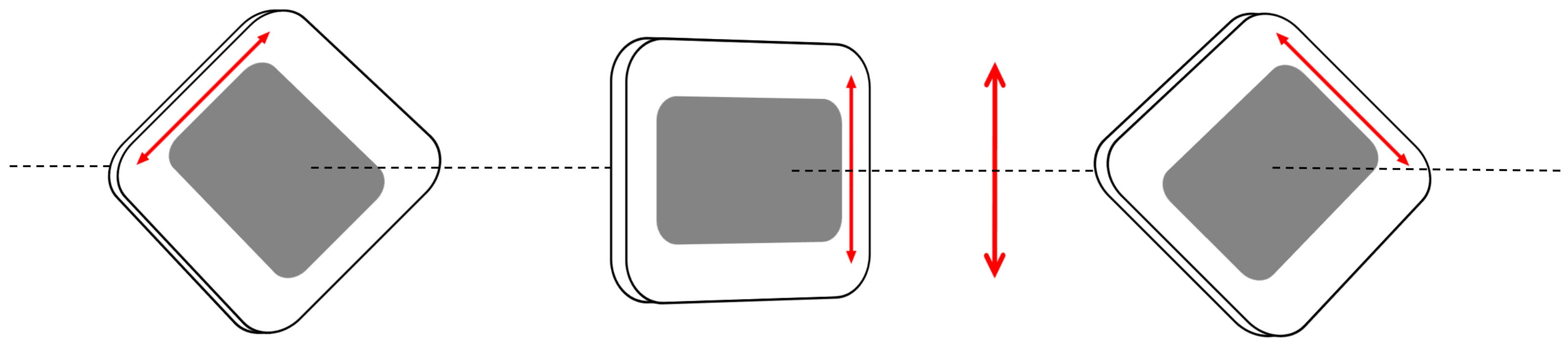
$$\nearrow = \frac{1}{\sqrt{2}}\left(\rightarrow + \uparrow\right)$$



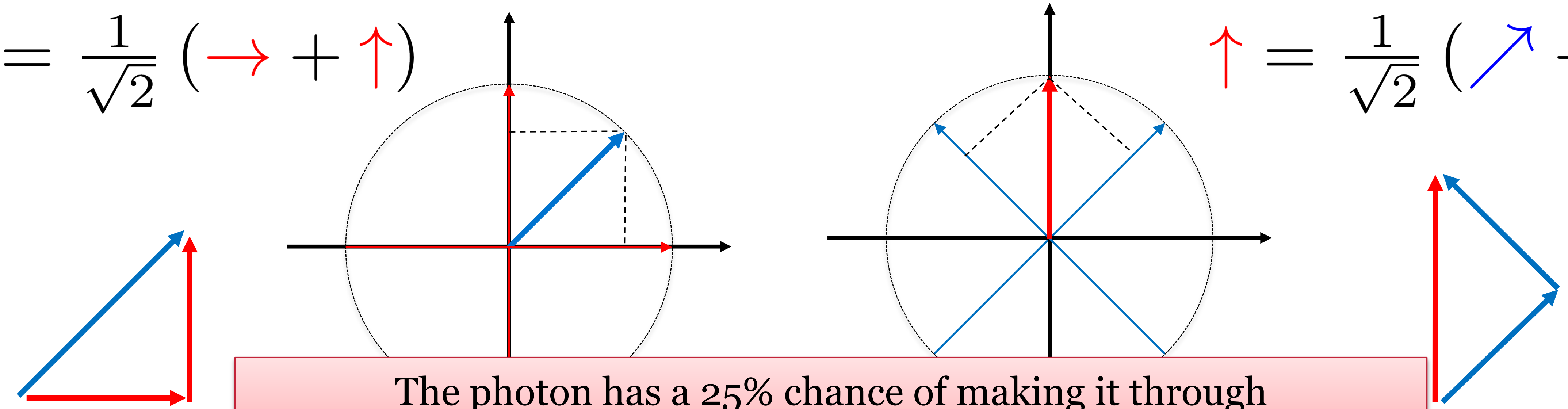


Superposition and Measurement

Transmits again with 50% probability



$$\nearrow = \frac{1}{\sqrt{2}}\left(\rightarrow + \uparrow\right) \qquad \uparrow = \frac{1}{\sqrt{2}}\left(\nearrow - \searrow\right)$$



The photon has a 25% chance of making it through

Measurement changes the state!

The Two Golden Rules

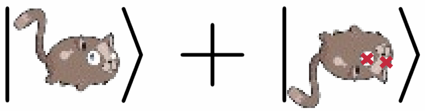
Rule #1
Superposition

A photon can behave

as if it is both

“here” and “there”

$$\rightarrow + \uparrow$$



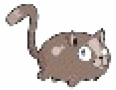
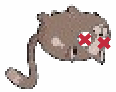
Rule #2
Measurement uncertainty

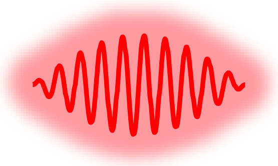
When asked where it is,

the photon will be found either

“here” or “there”

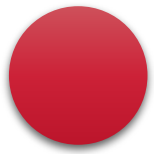
$$\rightarrow \quad OR \quad \uparrow$$

 OR 



Wave behaviour

Particle behaviour



Which of the following states is a superposition state?

A. Horizontal polarization

$$\rightarrow = \frac{\nearrow + \searrow}{\sqrt{2}}$$

B. Vertical polarization

$$\uparrow = \frac{\nearrow - \searrow}{\sqrt{2}}$$

C. +45° diagonal polarization

$$\nearrow = \frac{\rightarrow + \uparrow}{\sqrt{2}}$$

D. None are superposition states

E. All could be superposition states

The Two Golden Rules of Quantum Mechanics

$$\nearrow = \frac{\rightarrow + \uparrow}{\sqrt{2}}$$

$$\searrow = \frac{\rightarrow - \uparrow}{\sqrt{2}}$$

The particle is both
"→" AND "↑"
at the same time

BUT

When measured in the → /↑ basis,
it will be found as
"→" OR "↑"
randomly

$$\rightarrow = \frac{\nearrow + \searrow}{\sqrt{2}}$$

$$\uparrow = \frac{\nearrow - \searrow}{\sqrt{2}}$$

The particle is both
"↗" AND "↘"
at the same time

BUT

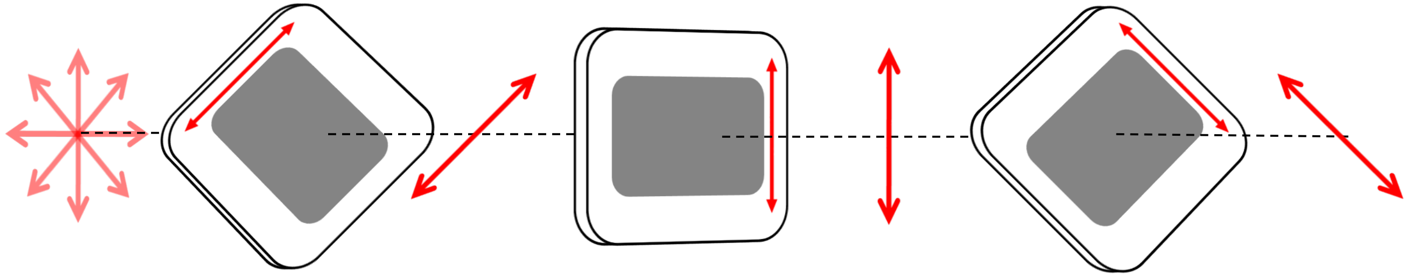
When measured in the ↗ /↘ basis,
it will be found as
"↗" OR "↘"
randomly

Measurement Basis
Defines which "question"
I ask the particle

Superposition
Always relative to the basis
in which we are measuring

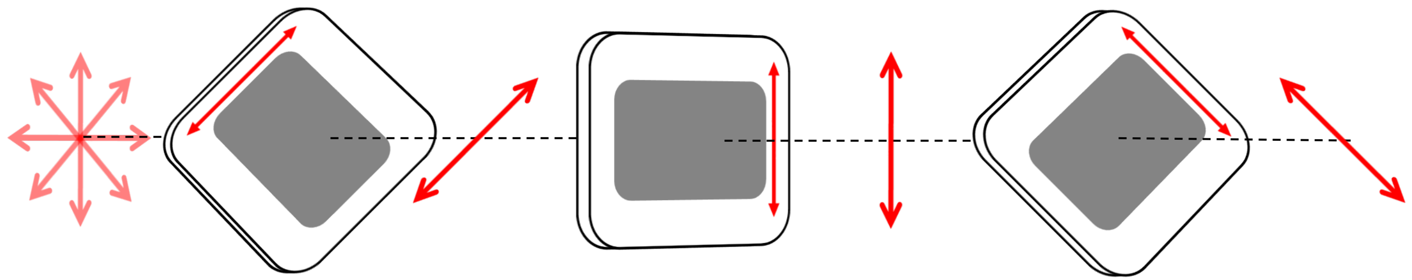
Summary

- Superposition is a *relative* concept, depending on the *measurement basis* being used
- The act of *measurement* changes the state
- Most quantum measurements are *incompatible*



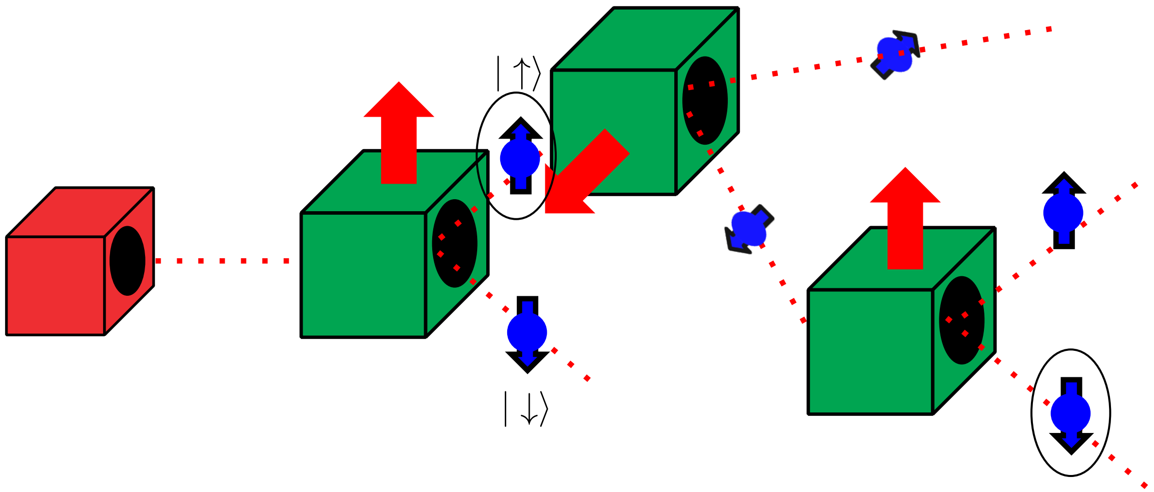
Polarization and Spin

The three-polarizer experiment is mathematically equivalent to the Stern-Gerlach experiment



Polarized Photons

Spin-Polarized Electrons



Check out the simulation on QuVis!
www.st-andrews.ac.uk/physics/quvis/
"Measurement Uncertainty" Demo

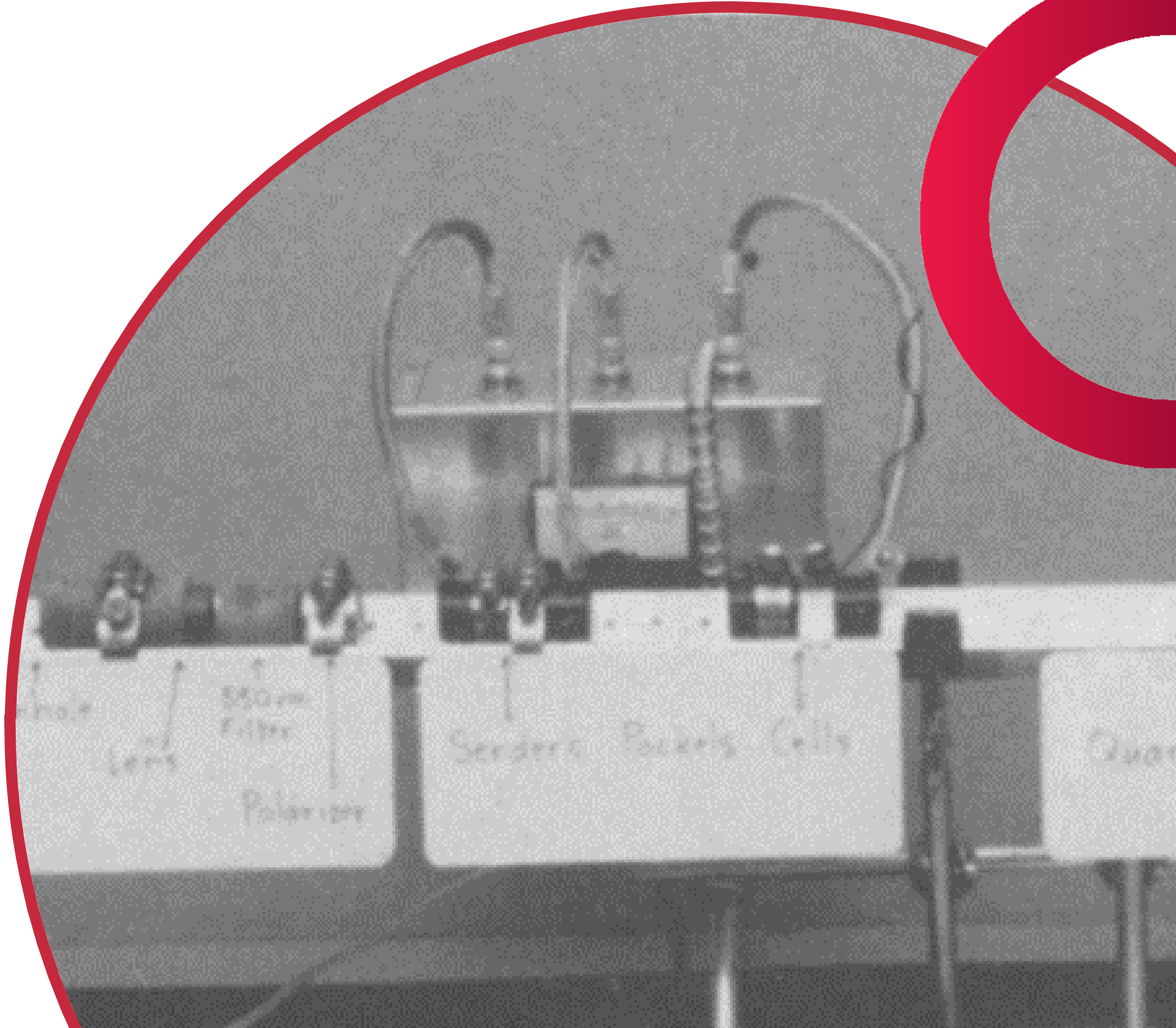
Question Break

Break Time

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

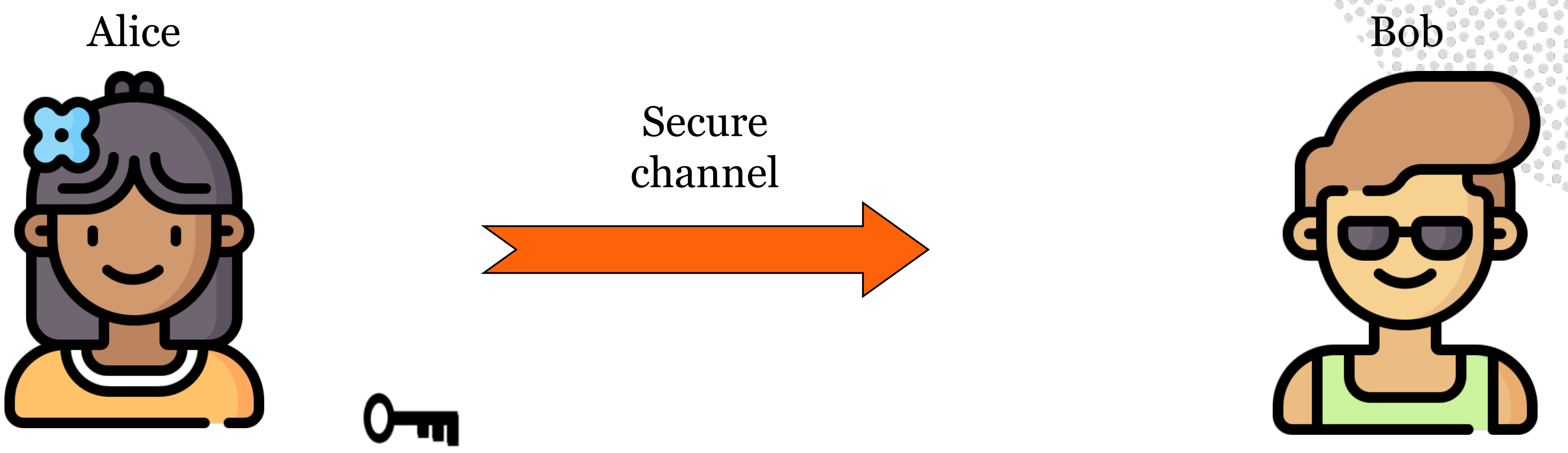
QUANTUM CRYPTOGRAPHY



The Science of Secrets

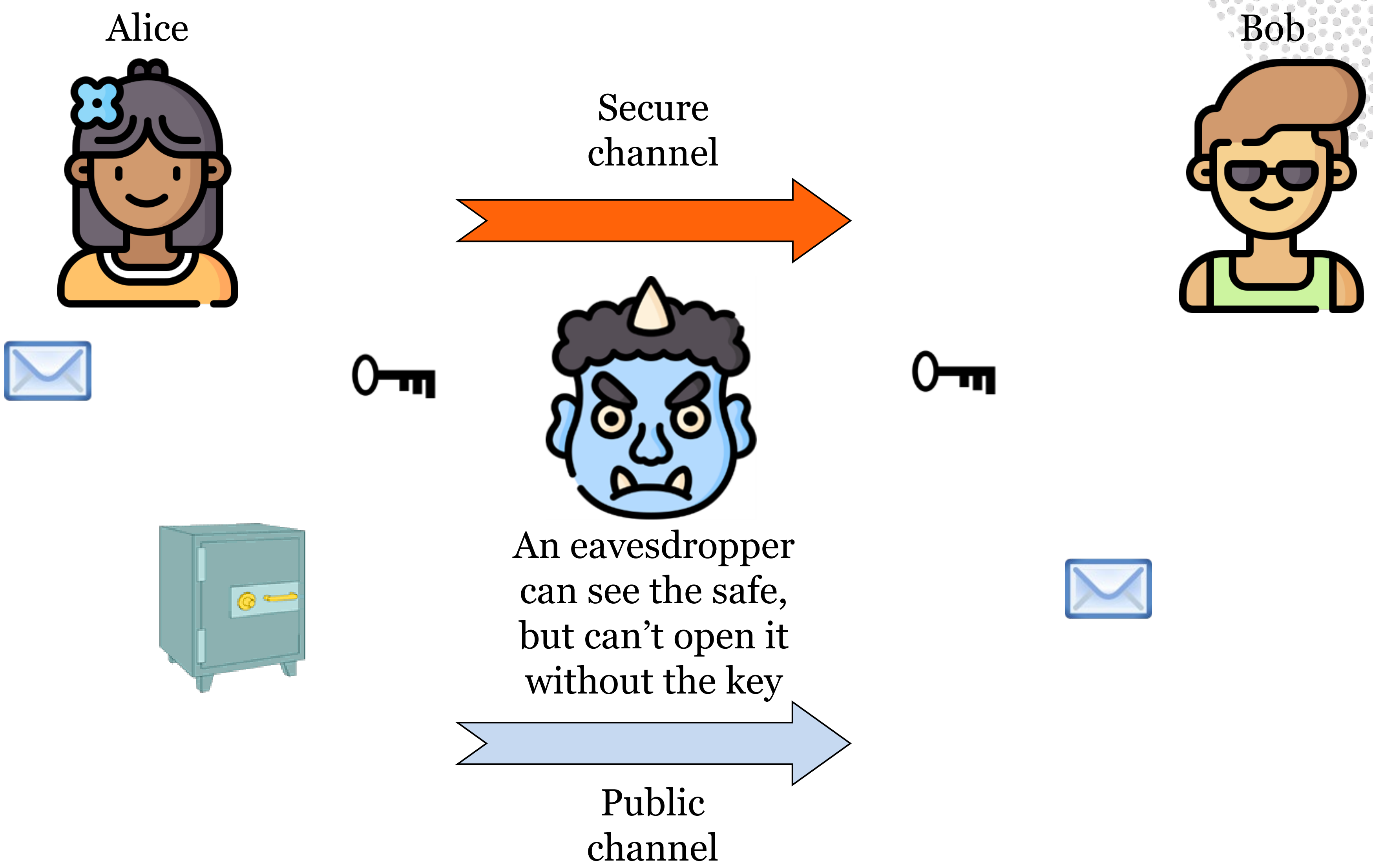
Cryptography

Keys and Security



Alice and Bob use a secure channel to share **identical** copies of a key

Keys and Security

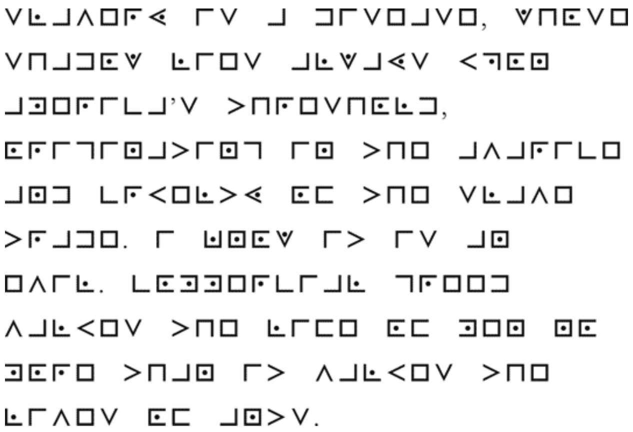


Keys

- In real life, the key is <u>**information**</u>
- Alice and Bob have the information, but the eavesdropper doesn't

Safe
Key: The PIN Number

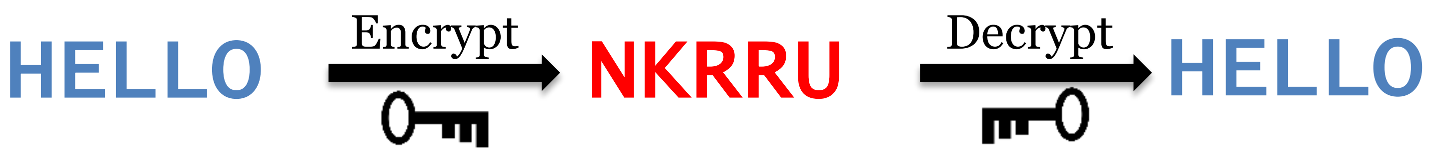
Door Lock
Key: Which pins to press



Secret Code
Key: Translation back to English

The Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F



 = 6 letter shift

 = NKRRU ciphertext

Big Problem!
If you know **<u>one</u>** encrypted letter,
you know **<u>the whole message</u>**!

The One-Time Pad (aka Vernam cipher)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

A different Caesar cipher for each letter

HELLO — Encrypt → SUXOI — Decrypt → HELLO

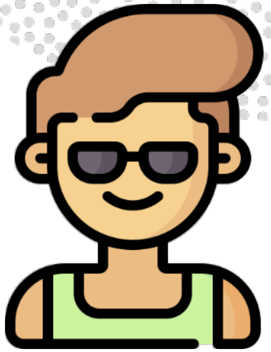

 = 5 random shifts

 = SUXOI ciphertext

The One-Time Pad

Message	01101000
Key	01001001
Cipher	00100001

Cipher	00100001
Key	01001001
Message	01101000



Message Bit / Key Bit

	Key Bit 0	Key Bit 1
Message Bit 0	0	1
Message Bit 1	1	0

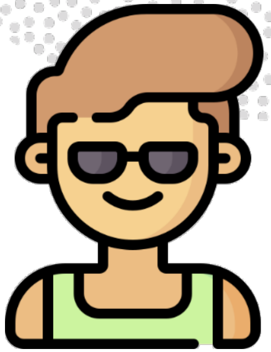
Alice and Bob share a long random binary string

Encode and decode by adding mod-2 (XOR)

The One-Time Pad

Message	01101000
Key	01001001
Cipher	00100001

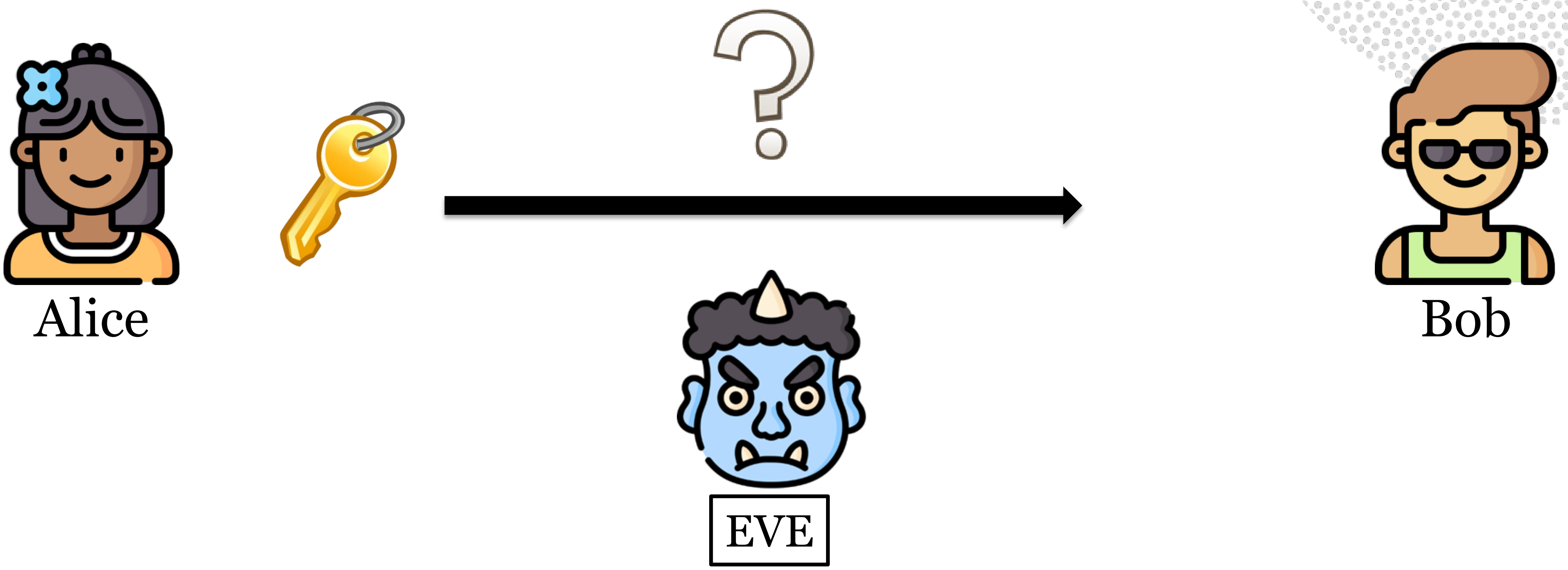
Cipher	00100001
Key	01001001
Message	01101000



8-bit key
2^8 possible keys
Number of possible keys = Number of possible messages

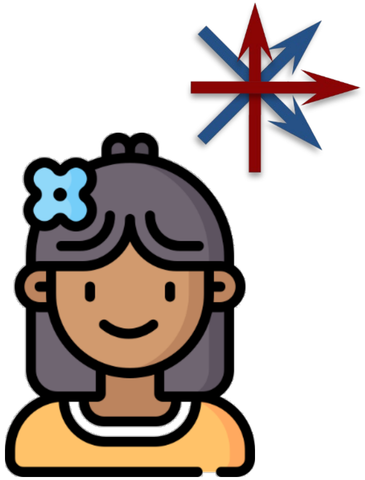
Perfectly secure!
But we're forgetting something…

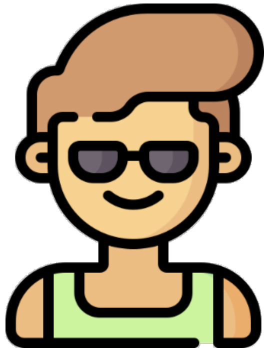
One-Time Pad Big-Time Problem



How do Alice and Bob securely share the key
in the first place?

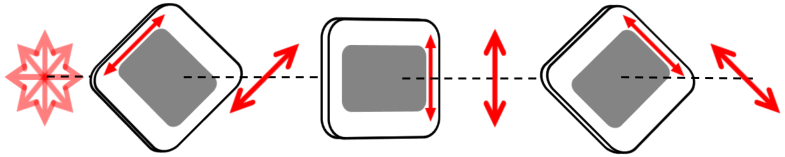
Quantum Key Distribution





Alice and Bob generate the key by sending polarization-encoded photons to each other

Quantum Key Distribution

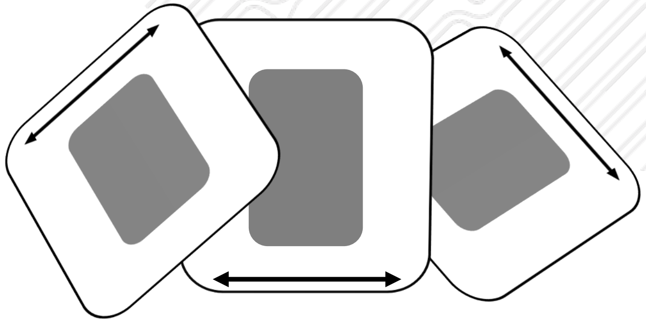


Remember the three polarizers?

If the eavesdropper intercepts,
they'll disturb the polarization state

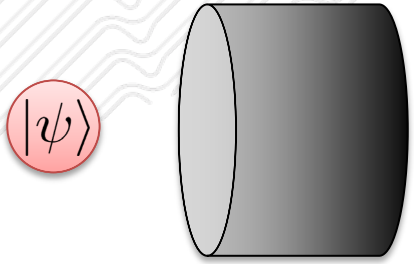
The Heart of QKD

Measurement Disturbance



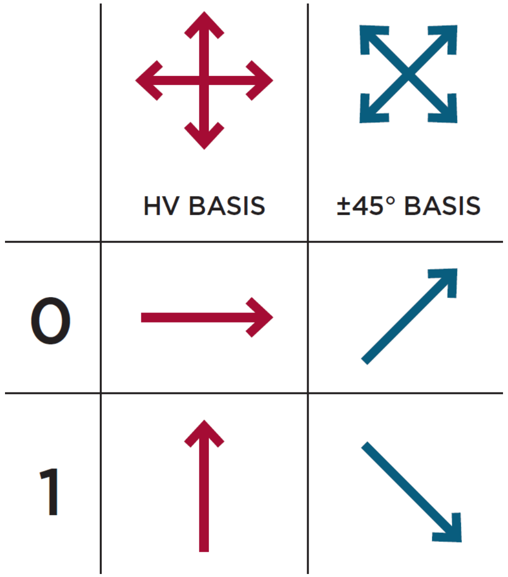
When we measure a quantum state,
we disturb it

The No-Cloning Theorem

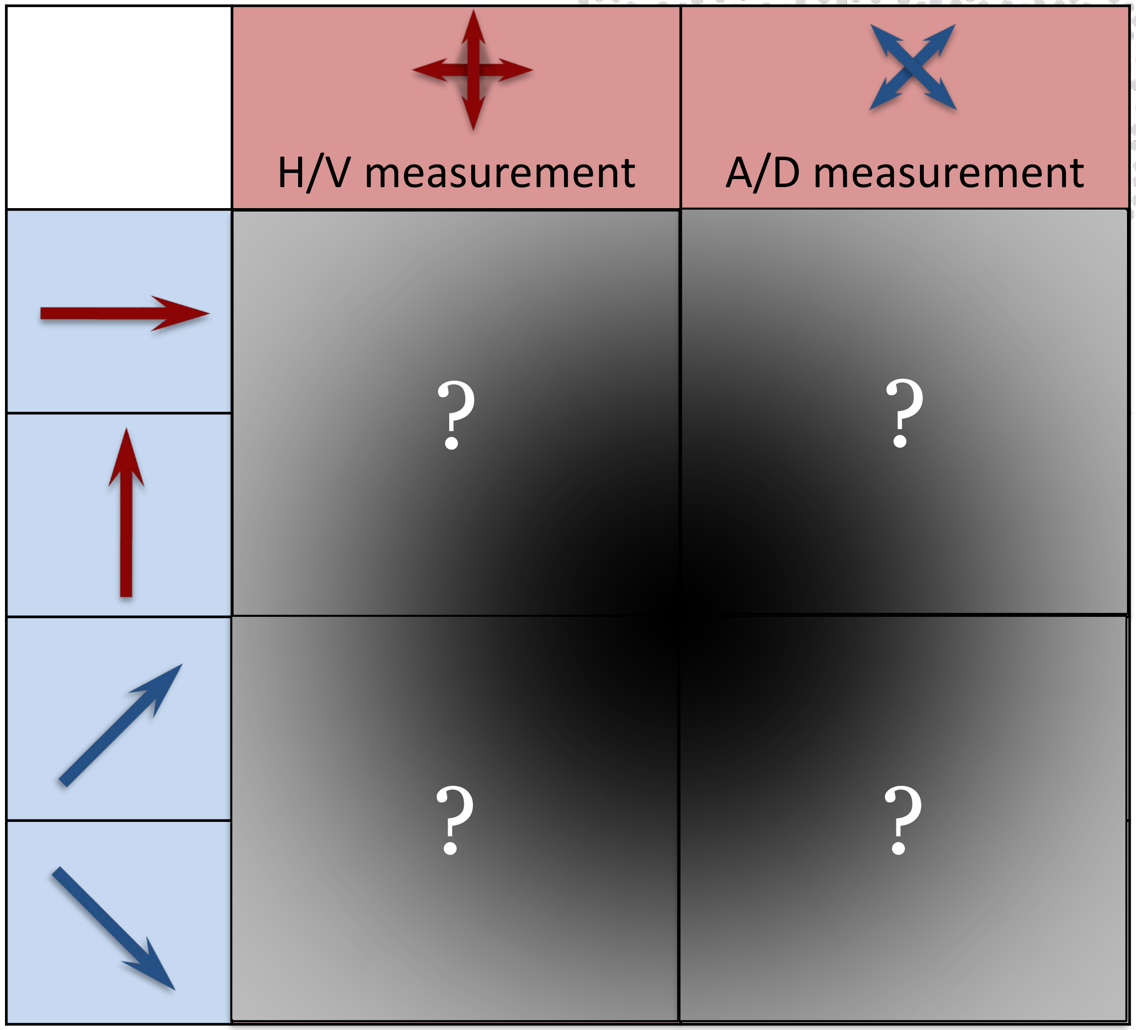


FORBIDDEN

Polarization Qubits



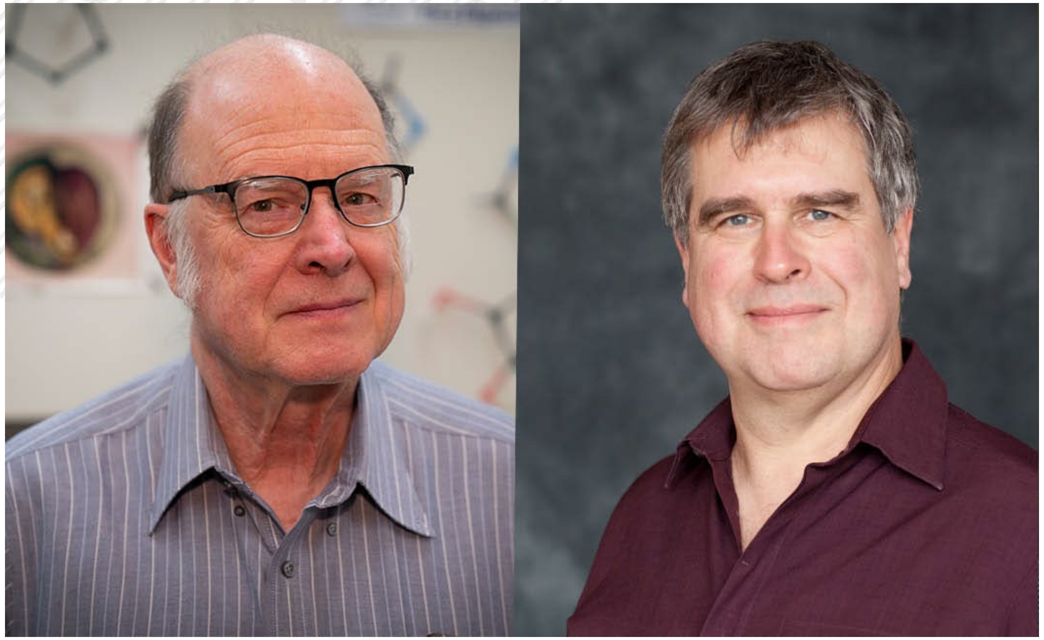
Encode binary "0" or "1" as a polarization state, with two possible bases



Question Break

Quantum Key Distribution (QKD)

- QKD uses single-photon signals to establish a **secure secret key**
- Eavesdroppers are detected due to **measurement disturbance**
- Many protocols exist, including some using entanglement
- The most well-known is the Bennett-Brassard (BB84) protocol

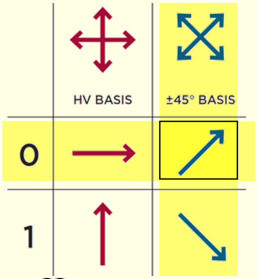


Charles Bennett (left), IBM Research
Giles Brassard (right), Université de Montréal

The BB84 Protocol

Step 1
Alice chooses
"0" or "1" randomly

Step 2
Alice chooses the
H/V or ±45° basis randomly



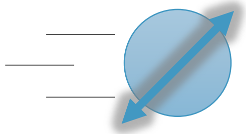
"0"
"±45°"

Alice's Lab

Step 7
Repeat and repeat until a long, random binary string is built

Step 8
Estimate the error rate in the string

Step 3
Alice encodes the appropriate qubit
and sends it to Bob as a single photon



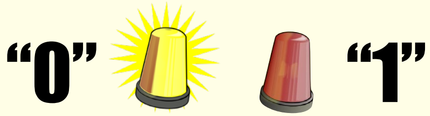
Step 6
Alice and Bob publicly announce which bases they used,
keeping their bit values secret

I used the ±45° basis

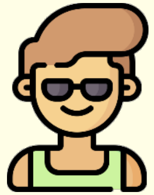
I used the ±45° basis

Step 4
Bob randomly chooses
a measurement basis

Step 5
Bob records the result
of his measurement



"±45°"
"0"



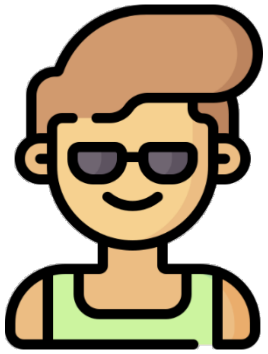
Bob's Lab

BB84 Example

1. Alice chooses a RANDOM bit

2. Alice chooses a RANDOM basis

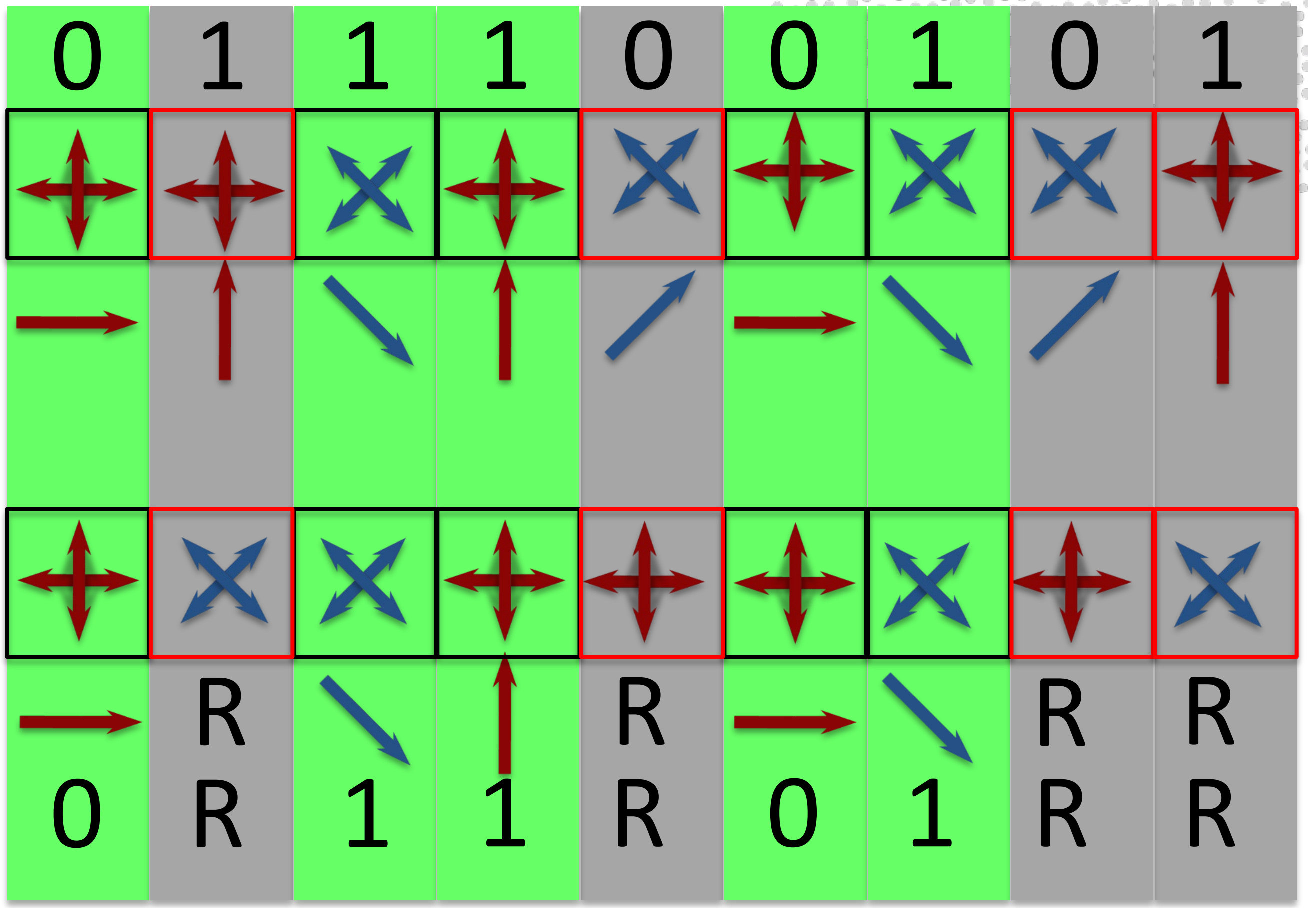
3. Alice send the state to Bob



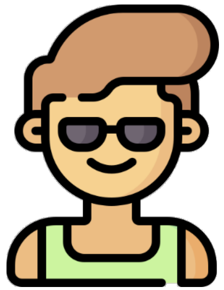
4. Bob measures in a RANDOM basis

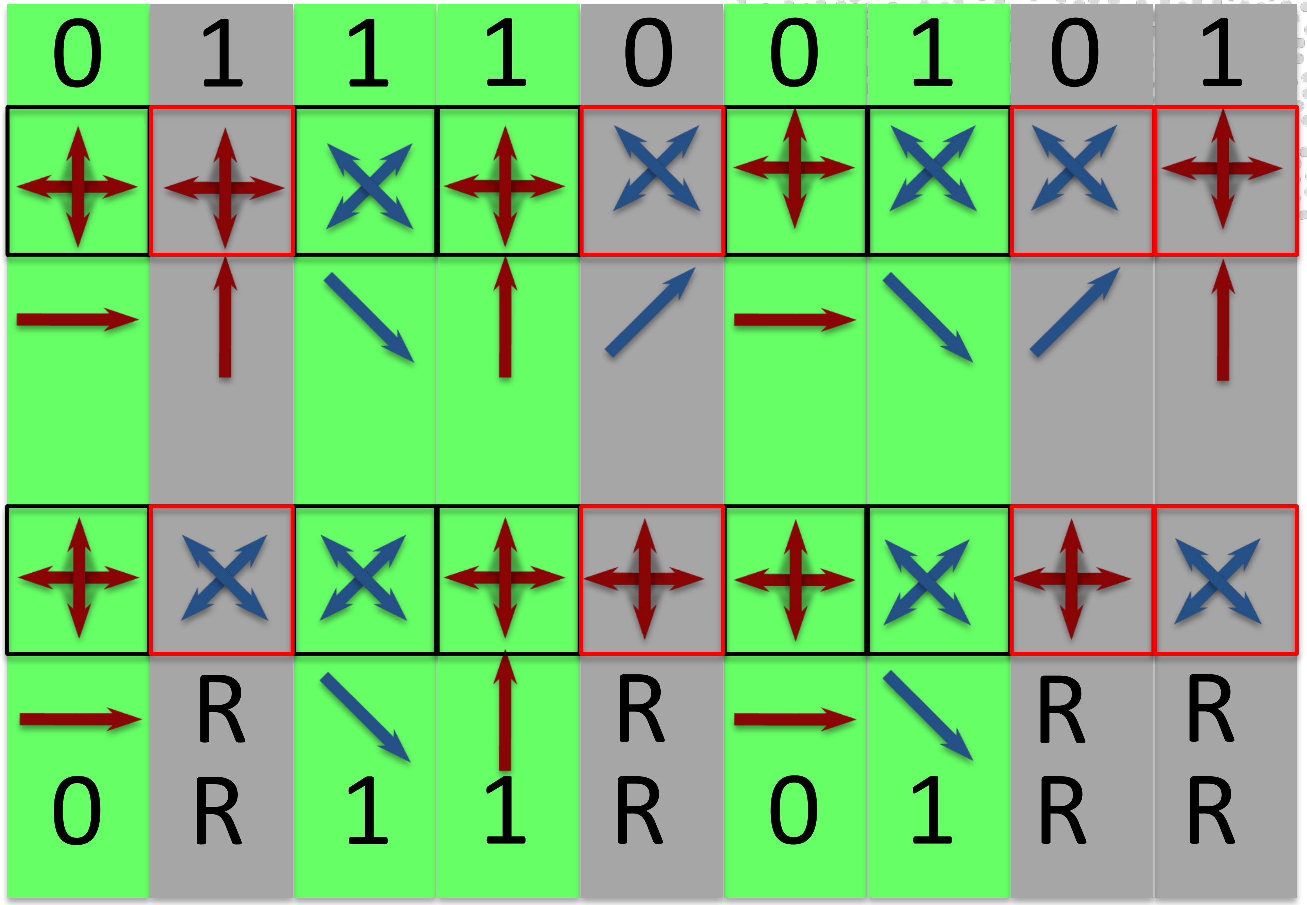
5. Bob records the bit

6. Alice and Bob announce the basis



BB84 Example





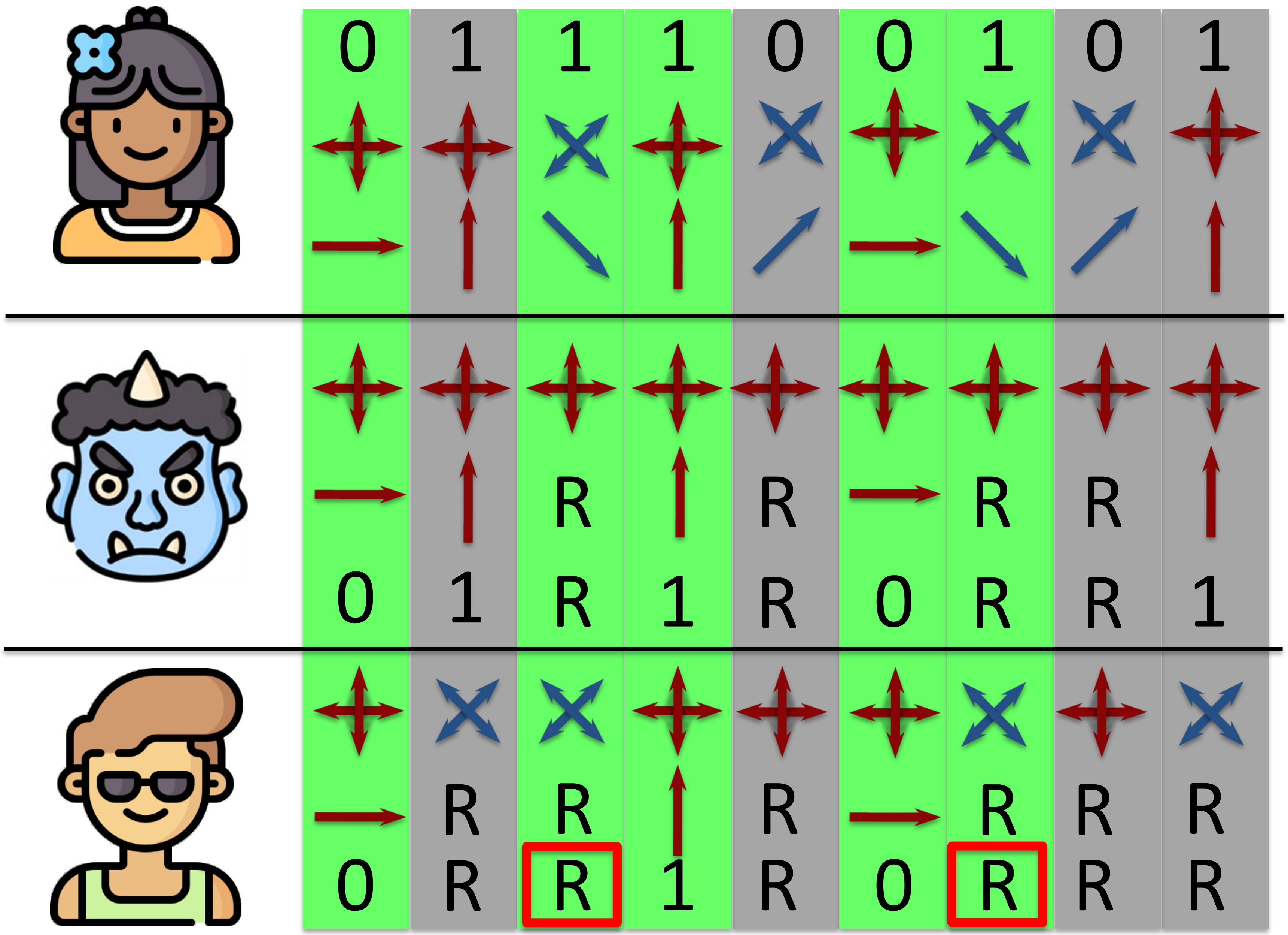
<u>Basis Reconciliation</u>

Alice and Bob discard all bits where their bases didn't match

This leaves them with the secret key

01101

What if there's an eavesdropper?


0 1 1 1 0 0 1 0 1
0 1 R 1 R 0 R R 1
R R R R R R R
0 R R 1 R 0 R R R

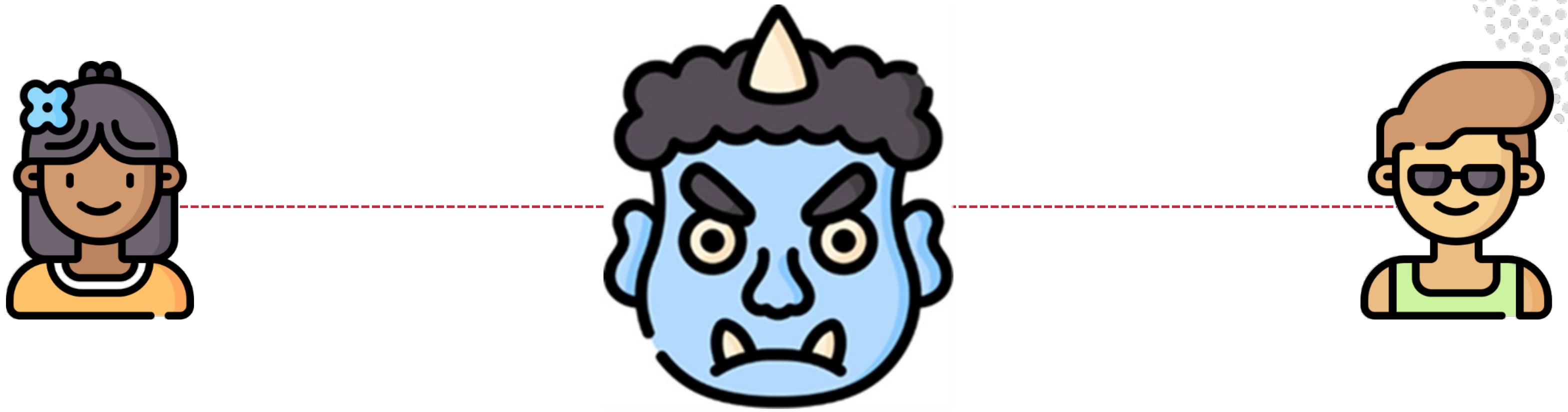
Breakout Session

1. What is the probability that Eve introduces an error for one photon?

2. What is probability that Eve does NOT introduce an error within 100 photons?

3. Why did Alice and Bob need to choose their bases randomly?

Error Estimation & Correction

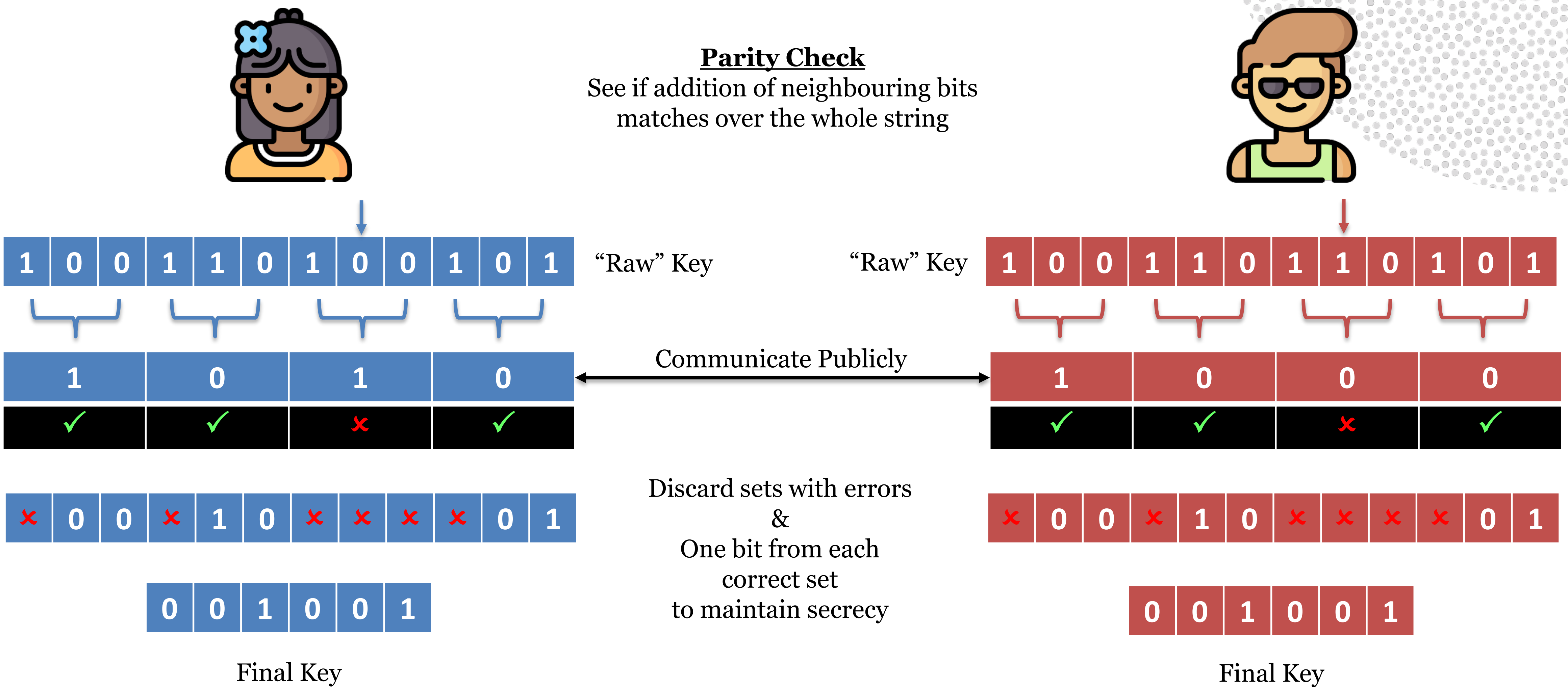


The presence of Eve unavoidably introduces errors into Alice and Bob’s key

By sacrificing some bits to estimate the error, Alice and Bob can either:

Detect the presence of the eavesdropper
OR
Guarantee that no eavesdropper was present

Error Estimation and Correction

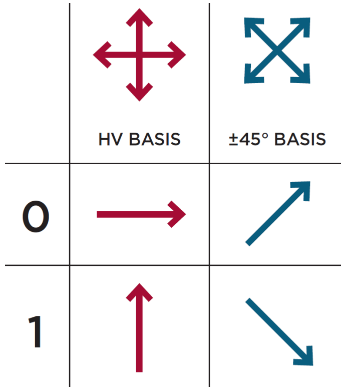


QKD Common Misconceptions

- We're not sending a message, we're sharing a key
  - The randomness is good!
  - No sensitive information is sent until the key is set
  - If Alice chooses her states non-randomly, Eve can hack

Message	01101000
Key	01001001
Cipher	00100001

- Announcing the bases gives no information about the key
  - They can share that over a public channel



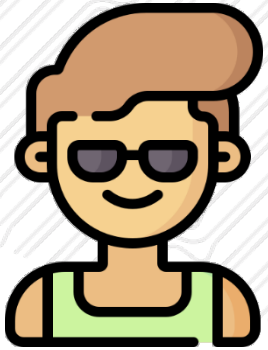
Question Break

Quantum Coins Activity

Instructions on Slack

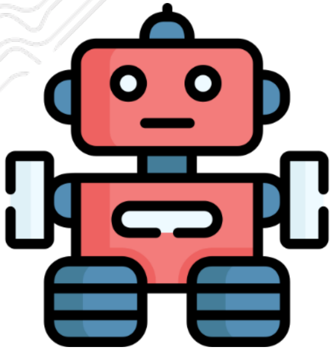
Group divides into four teams

Alice
Sends
qubits



Bob
Measures
qubits

Eve
Intercepts
qubits

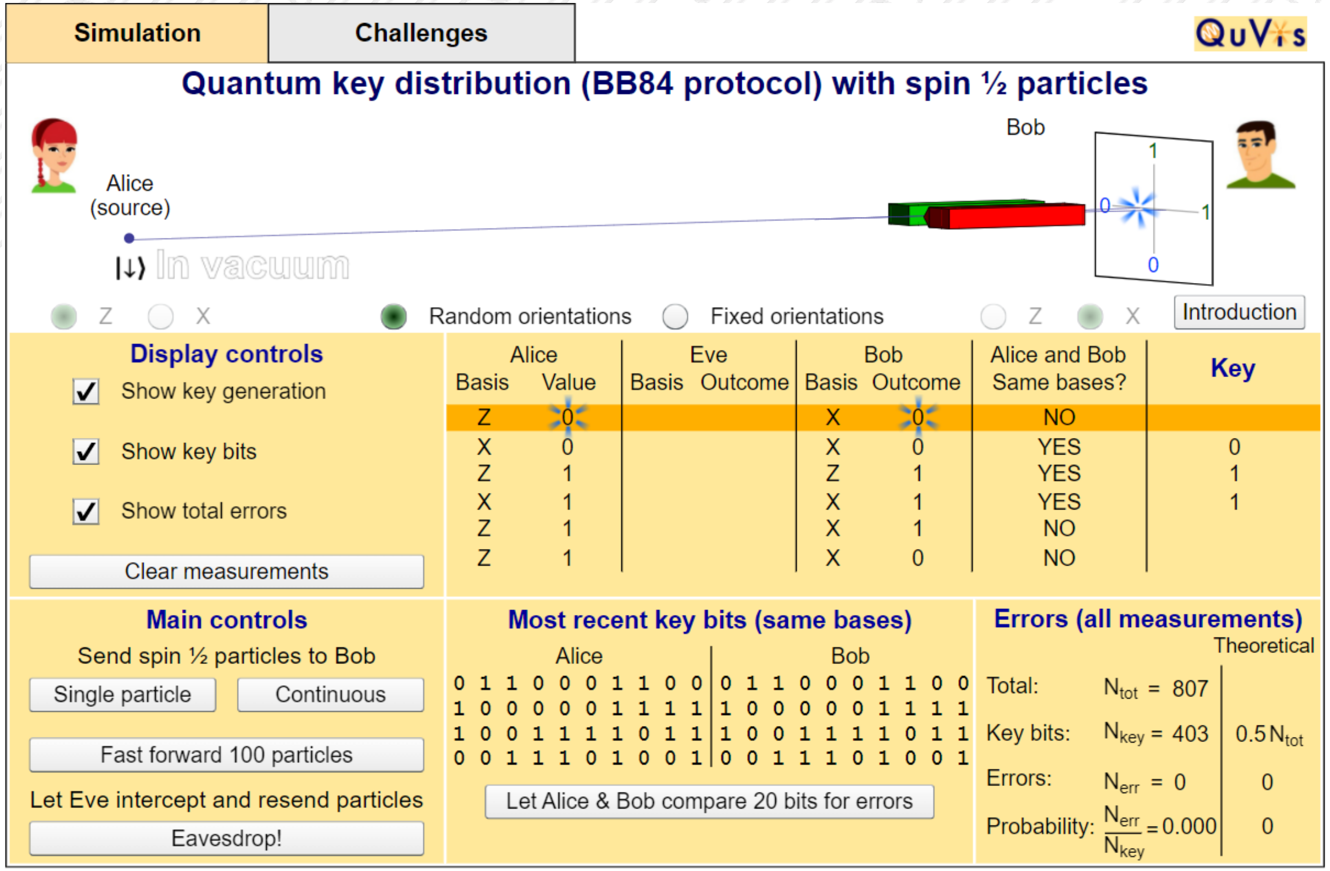


Moderator
Enforces
quantum rules

Model the photon's state as a coin in one of two boxes
Whenever one is measured, the other is shaken

Possible confusion from one quantum state
represented with two objects/boxes

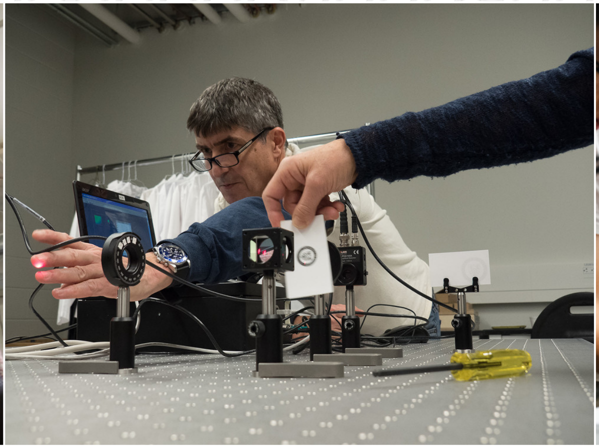
QKD Simulators

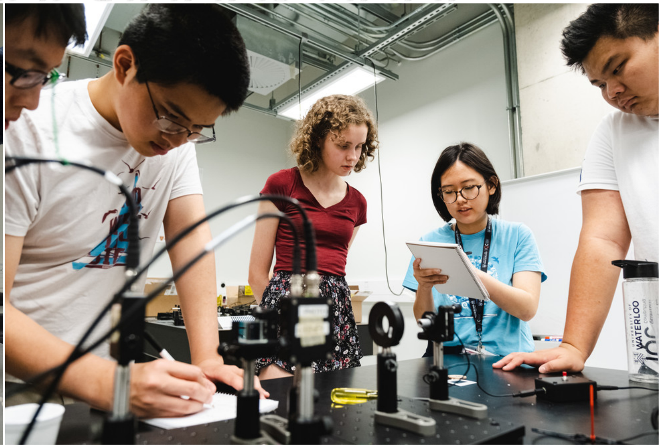


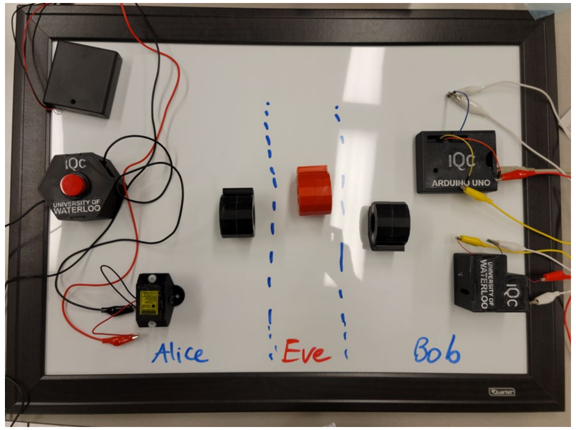
Simulator from QuVis (St. Andrew's University)

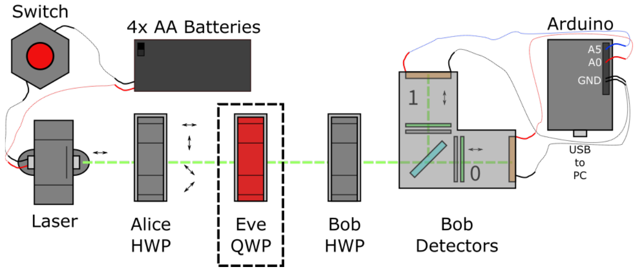
Uses electron spin rather than polarization

QKD Laser Activity









Homebuilt version
w/ 3D-printed models
~$150 USD
Student test groups needed!

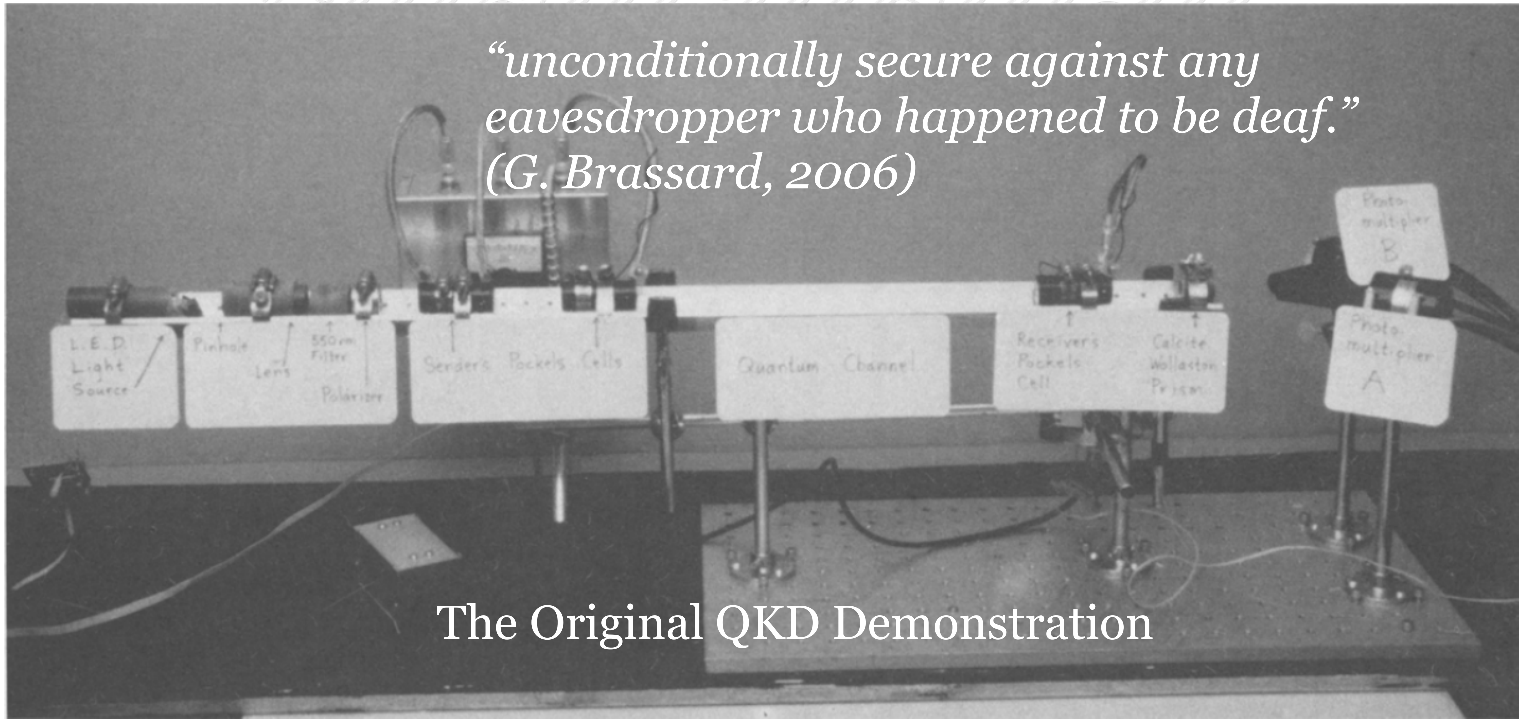
Superposition, Measurement, and Quantum Cryptography

Applications & Technology

Hacking QKD

QKD security is guaranteed by the laws of physics!

But compromised by the reality of engineering

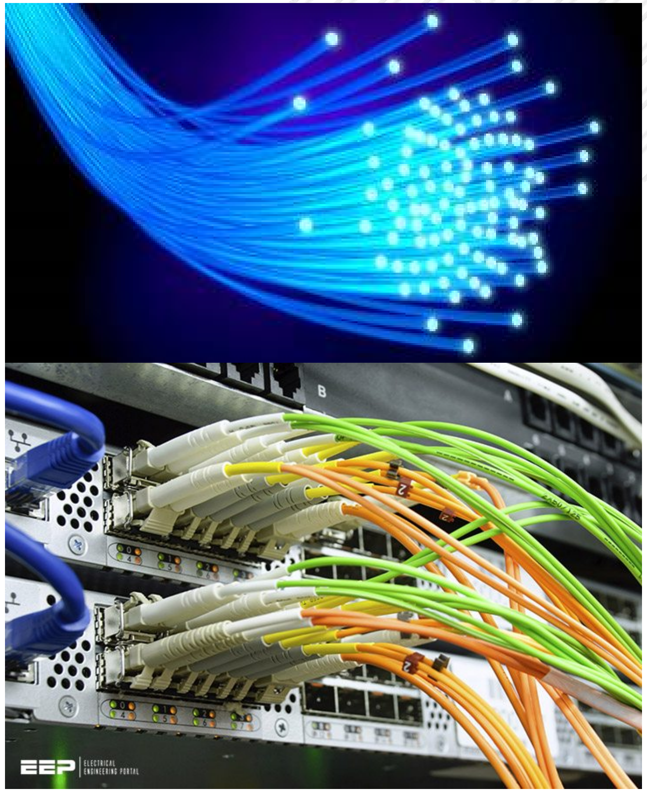


"unconditionally secure against any eavesdropper who happened to be deaf." *(G. Brassard, 2006)*

The Original QKD Demonstration

Sending Photons over Long Distances

Optical fibre

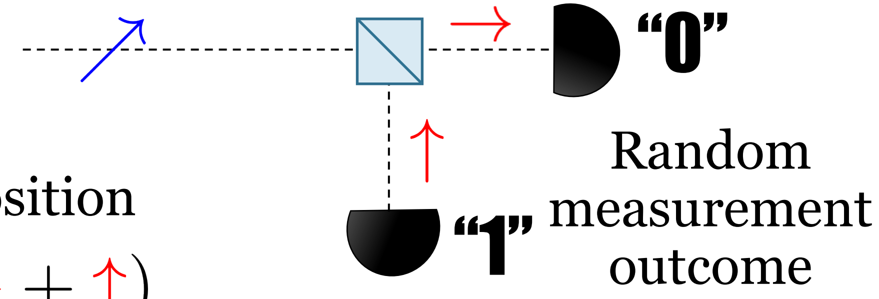


Free-space / Satellites

Quantum Random-Number Generators

101100100101110110010011100000111110111010101010101100001011111000000001111000000000111101110010

- Most computers generate "pseudo" random numbers
  - The sequence looks random enough, but is perfectly predictable
- Quantum mechanics is *truly* random
  - The sequence is unpredictable, even if we know the quantum states



50/50 superposition

$$\nearrow = \frac{1}{\sqrt{2}}\left(\rightarrow + \uparrow\right)$$

idQuantique QRNG

Summary

- Quantum systems can carry **information**
- Measurement in one **basis** disturbs the other
- These ideas can be used for **information security**

Thanks for joining!

The next session will be tomorrow at 7pm ET on
Wave-Particle Duality and Quantum Computing

Lingering questions?
Please ask on the #quantum-questions channel