Quantum mechanics basics

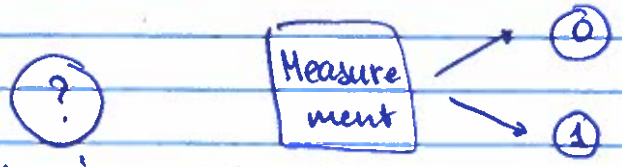
Classical bit / coin

Two possible states "0" and "1"

head tail

* A coin can only be in one of two states, and if it is in one, it cannot be in the other.

Since these two states completely describe the entirely of possible states of the coin, they form a complete basis.

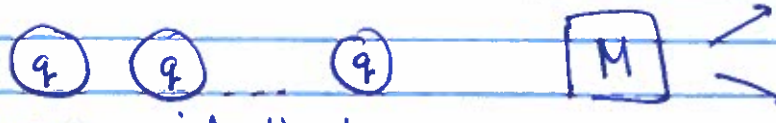


two possible mutually exclusive outcomes

coin in unknown state

This picture is identical for both classical and quantum world

Difference? Sometimes random outcome



many identical quantum coins

Quantum lingvo

a coin in a state "0" : $|0\rangle$

" " " " "1" : $|1\rangle$

Quantum superposition of two states : quantum state (wave function)

$|q\rangle = c_0|0\rangle + c_1|1\rangle$

c_0, c_1 – probability amplitudes (not probabilities)

Probability to measure the coin in the state '0' $p_0 = |c_0|^2$

and in state "1" : $p_1 = |c_1|^2$

Since these are the only to outcomes

$|c_0|^2 + |c_1|^2 = 1$

Notice that $|q_1\rangle = c_0|0\rangle + c_1|1\rangle$

and $|q_2\rangle = c_0|0\rangle - c_1|1\rangle$

will give exactly the same measurement outcome distribution, even though these are different quantum states.

Such superpositions of two basis states are called qubit (quantum bits)

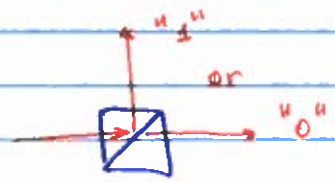
Instead of two well-defined states for a bit, a qubit can be in infinitely large number of combinations of the two

Photons as qubits

To declare something a qubit, we need to find some characteristic that, if measured, can be in only two states

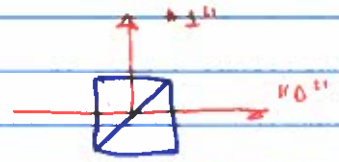
Photonic qubits

Polarization encoding



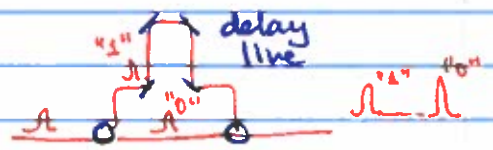
polarizing Beam Splitter (PBS)

Dual-rail encoding



non-polarizing Beam Splitter (nPBS)

Time-bin encoding



In principal, a quantum system can have more than 2 possible states

H-atom



$|n=3\rangle$

$|n=2\rangle$

$|n=1\rangle$

An electron in an hydrogen atom can be in a superposition of several energy states

$|\psi\rangle = C_1|n=1\rangle + C_2|n=2\rangle + C_3|n=3\rangle$

$|C_i|^2$ – probability to be in the state $n=i$

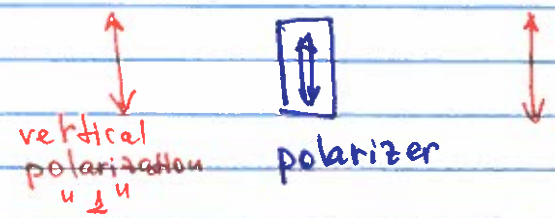
Measurement can change the state of the particle

In quantum mechanics a measurement is an active operation, not a passive observation. Mathematically, it is performed by operators

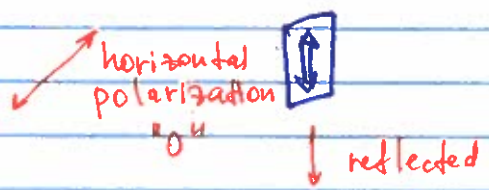
There are special states for each measurement that are not changed by this measurement. They are called eigen states, and they give known outcome of the measurement, known as eigenvalue
Any other state gets "messed up"

$|0\rangle$ → "0/1" meter → $|0\rangle$ – eigenstate
eigenvalue – "0"

$|1\rangle$ → "0/1" meter → $|1\rangle$ eigenstate
eigenvalue – "1"



1 photon passed



0 photons passed

Any other qubit state is a superposition

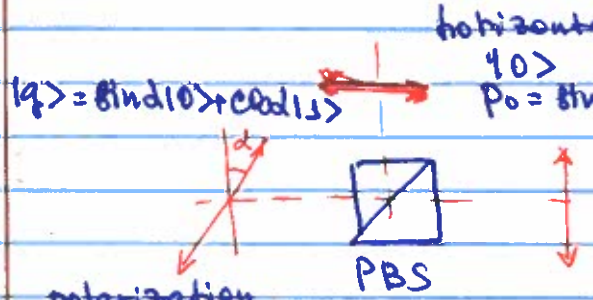
$|q\rangle = c_0|0\rangle + c_1|1\rangle$ → "0/1" meter

$|0\rangle$ in $|c_0|^2$ fraction of expts

$|1\rangle$ in $|c_1|^2$ fraction of experiments

different state

$|q\rangle = \sin\alpha|0\rangle + \cos\alpha|1\rangle$



polarization at an angle

two distinct outcomes

This property of single photons is a basis for quantum cryptography protocols.

Since it is impossible to reconstruct a quantum state of a photon from a single measurement, one cannot make a copy of a quantum state "no cloning" theorem

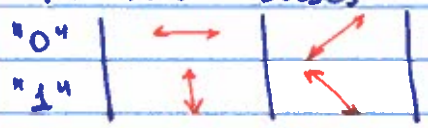
Two possible qubit bases

$|0\rangle \& |1\rangle$ ↔ & ↕

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ↗ & ↖

Alice

Can send qubits in two bases



Bob

Can measure arriving photons in either basis and record the outcome

PBS at 0° or PBS at 45°

PBS 0°

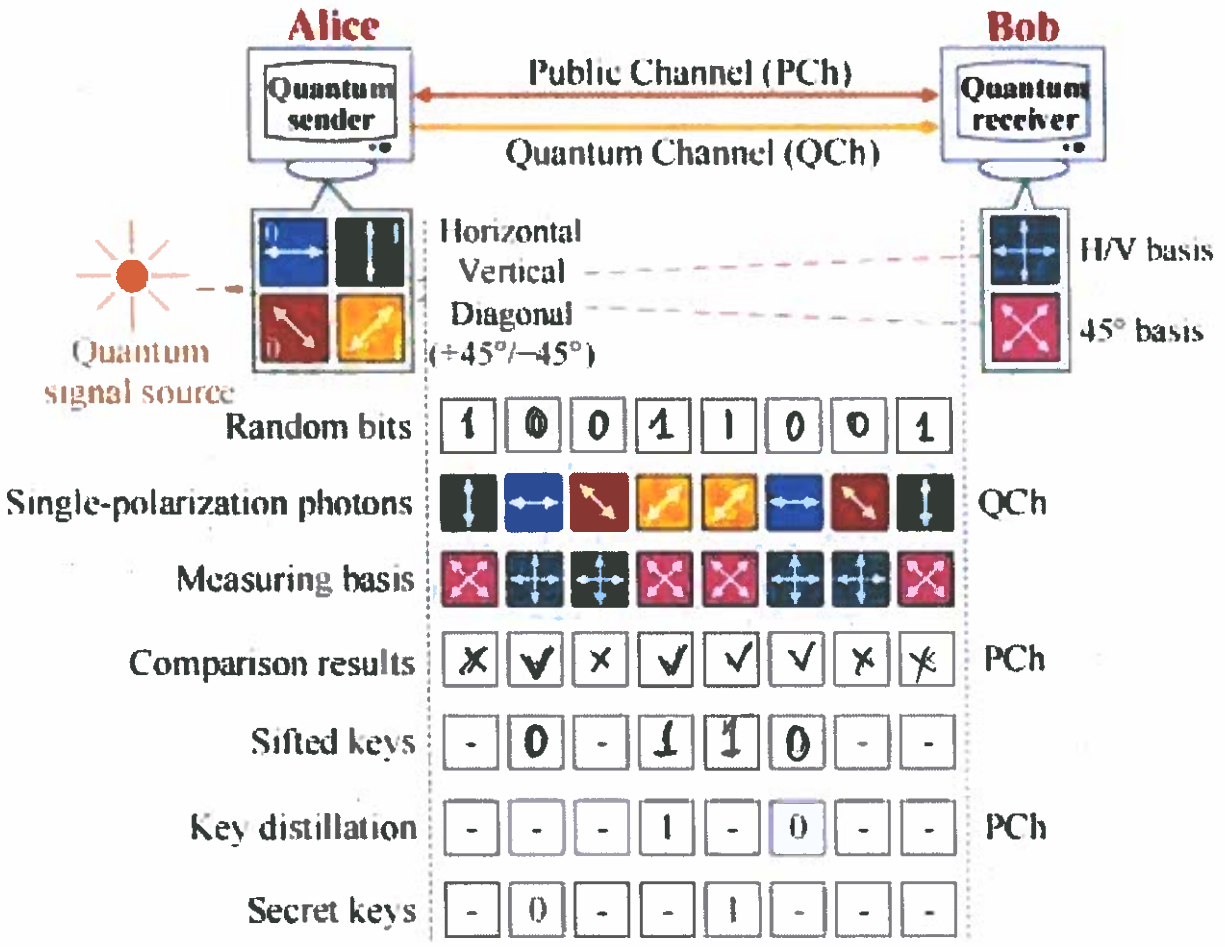
input	outputs	
↔	0	100%
↕	100%	0
⤢	50%	50%
⤡	50%	50%

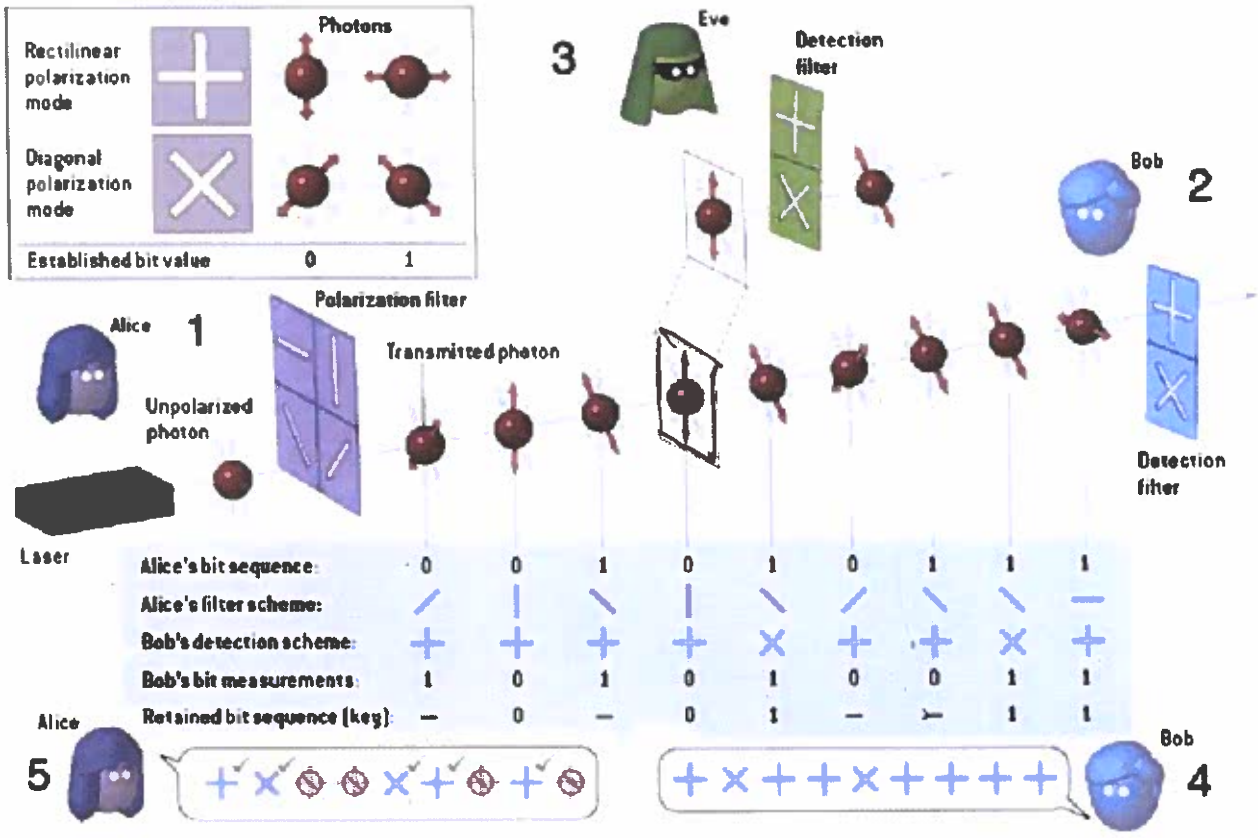
] indistinguishable

PBS 45°

input	outputs	
↔	50%	50%
↕	50%	50%
⤢	0°	100%
⤡	100%	0

] indistinguishable


Alice
Bob
Quantum sender
Quantum receiver
Public Channel (PCh)
Quantum Channel (QCh)
Horizontal
Vertical
Diagonal
(+45°/−45°)
H/V basis
45° basis
Quantum signal source
Random bits
Single-polarization photons
Measuring basis
Comparison results
Sifted keys
Key distillation
Secret keys
QCh
PCh
PCh


Photons
Rectilinear polarization mode
Diagonal polarization mode
Established bit value 0 1
3
Eve
Detection filter
Bob
2
Alice
1
Polarization filter
Transmitted photon
Unpolarized photon
Laser
Detection filter
Alice's bit sequence: 0 0 1 0 1 0 1 1 1
Alice's filter scheme:
Bob's detection scheme:
Bob's bit measurements: 1 0 1 0 1 0 0 1 1
Retained bit sequence (key): – 0 – 0 1 – – 1 1
Alice
5
Bob
4