QUANTUM COMMUNICATION

DR. CHANDRASHEKAR JATOTH
Assistant Professor

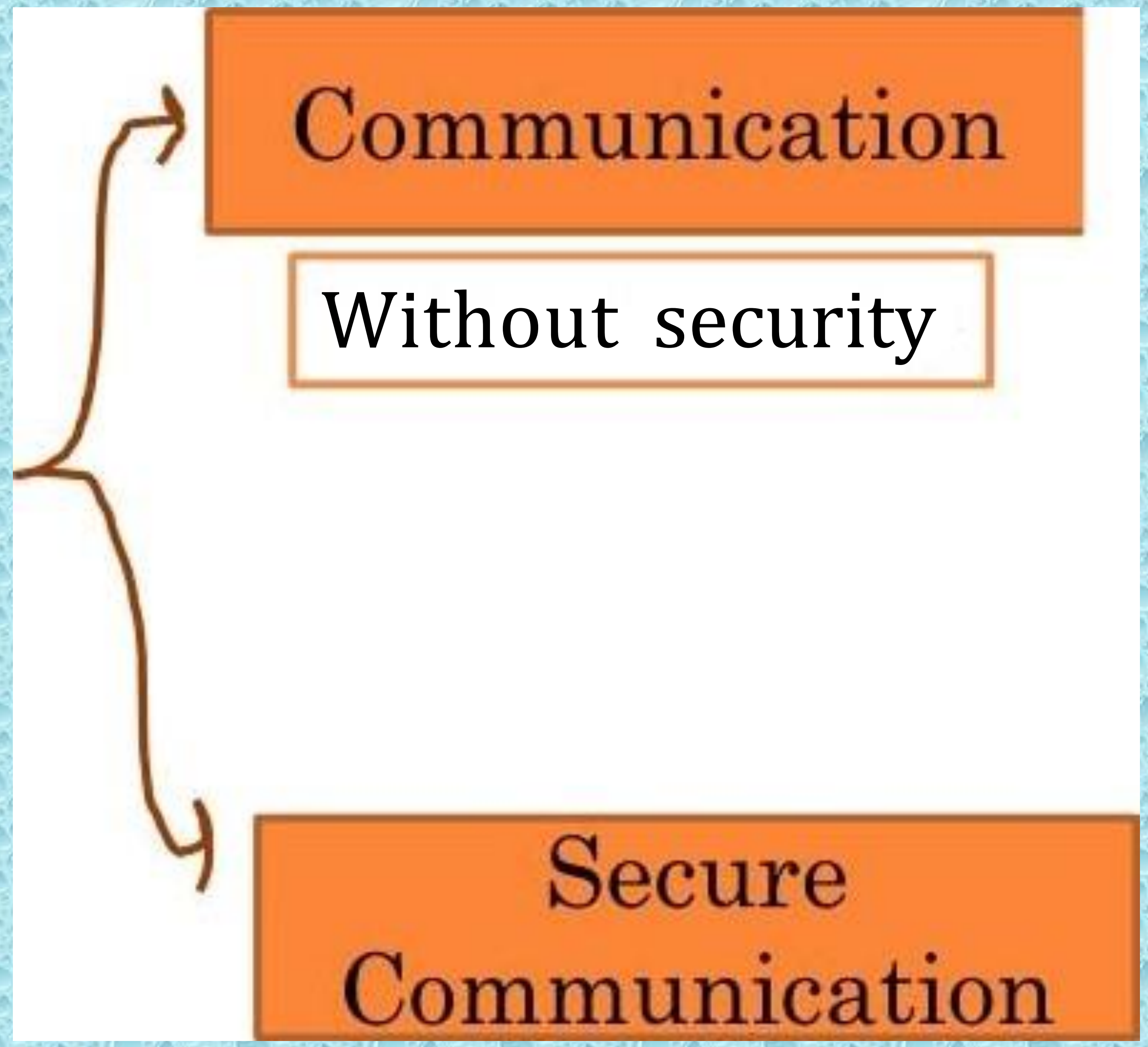
Communication

Without security

Communication

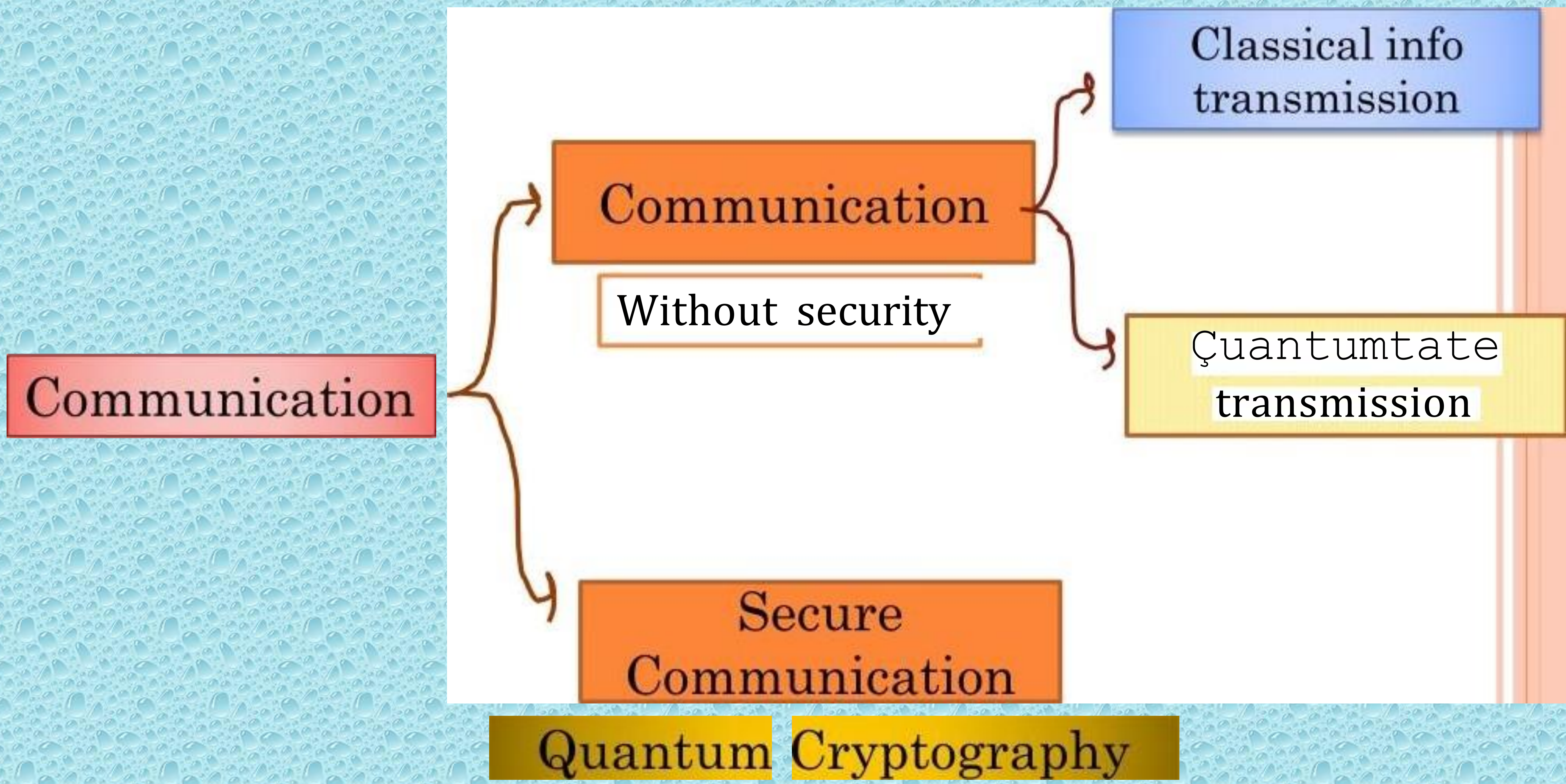
OUTLINE

Communication



Quantum Cryptography

OUTLINE


Communication
Communication
Without security
Classical info transmission
Çuantumtate transmission
Secure Communication
Quantum Cryptography

COMMUNICATION

What is Communication?

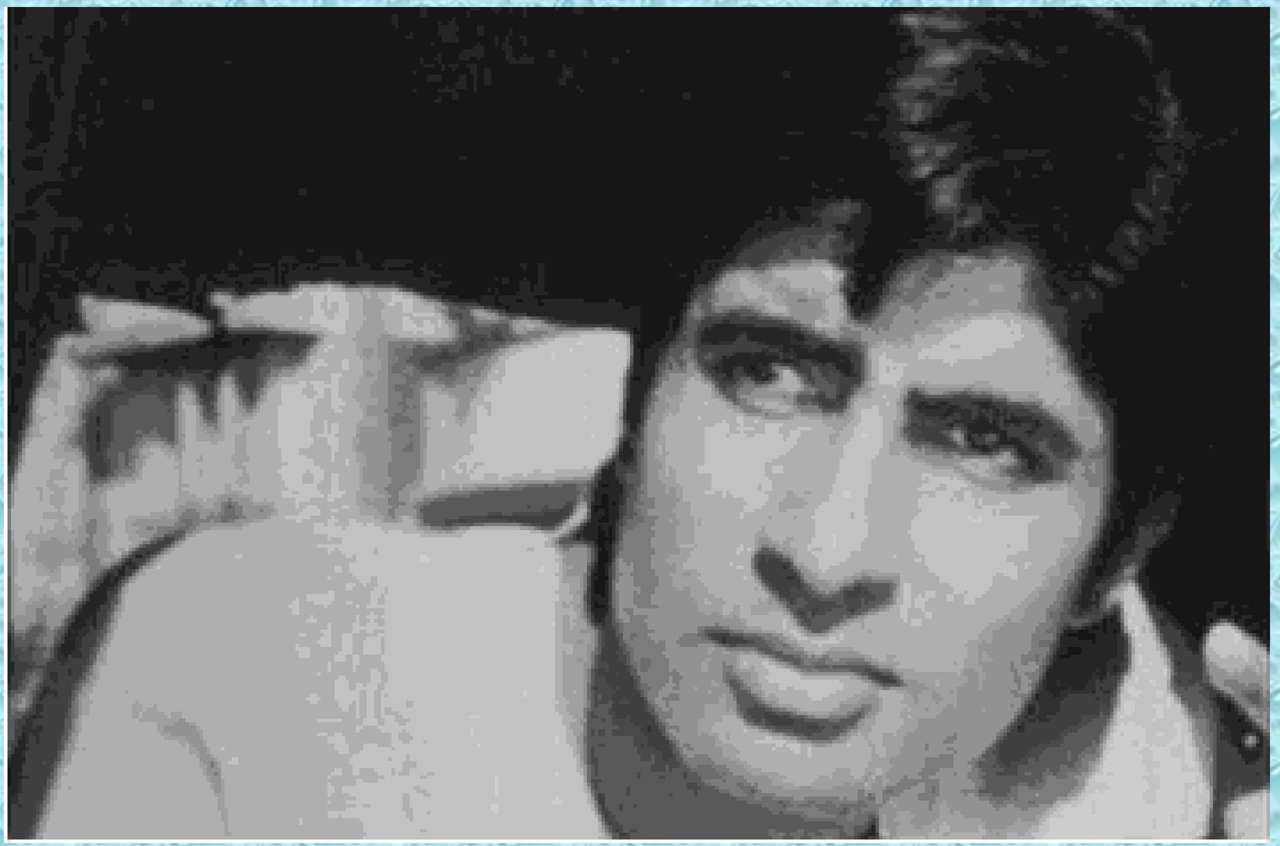
What is Communication?

At least 2 parties

WHAT IS COMMUNICATION?

At least 2 parties

Sender



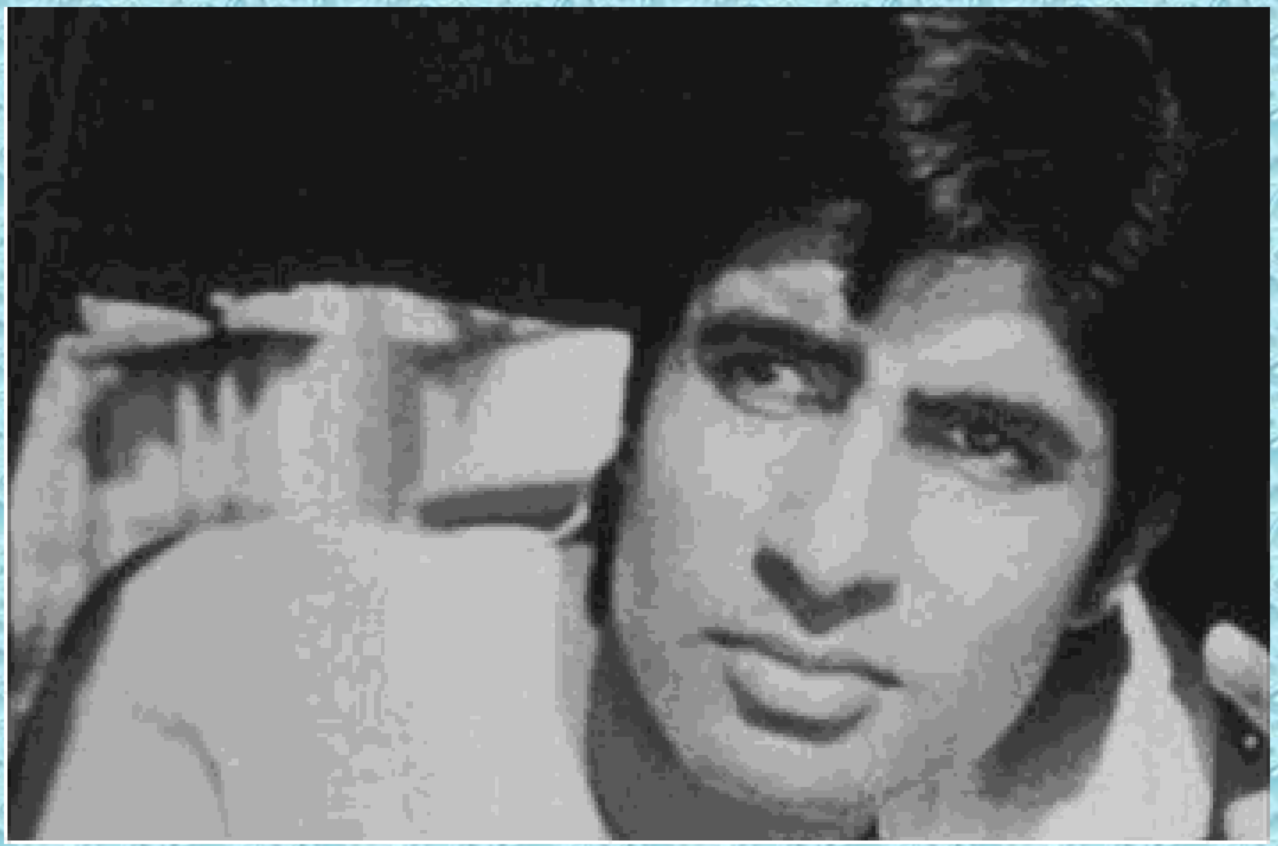
Receiver

What is Communication ?

At least 2 parties

Sender

Alice

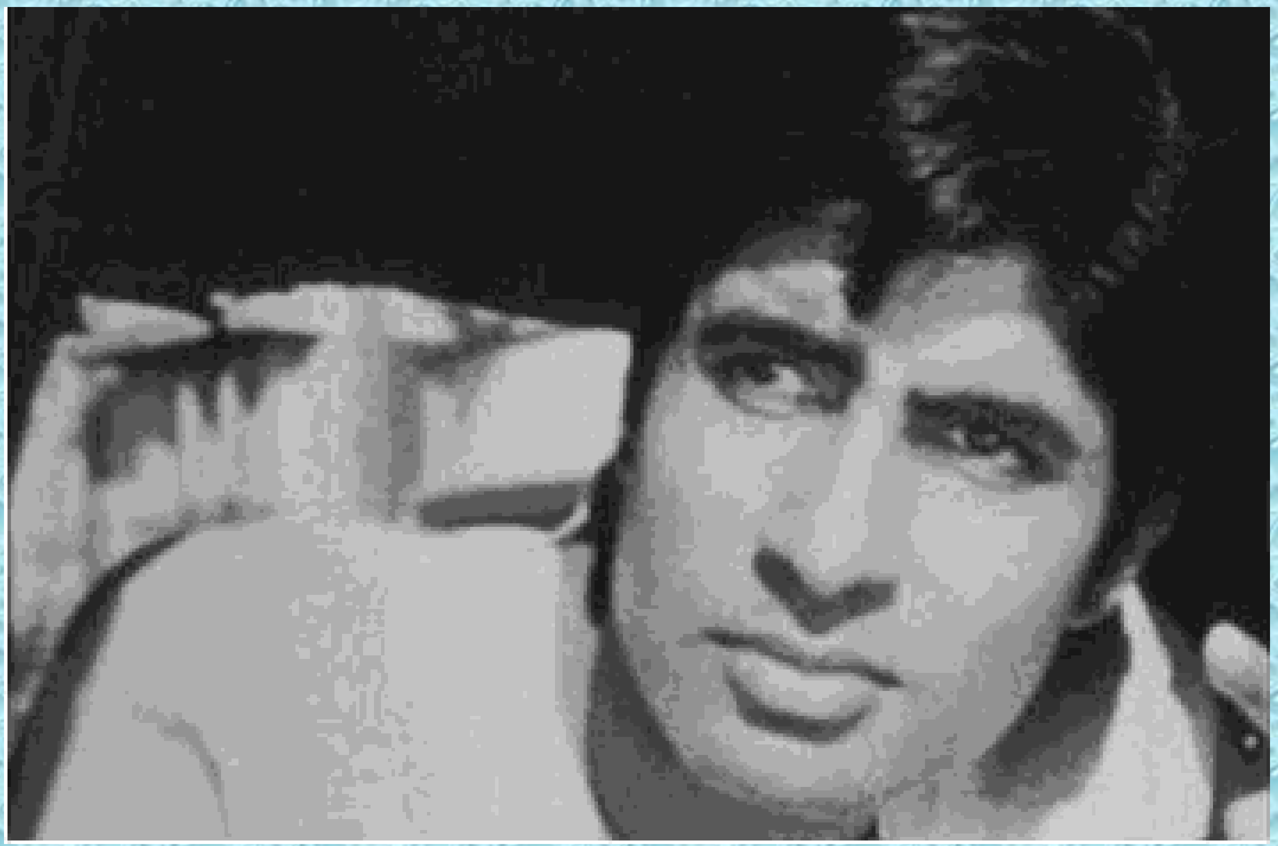


Receiver

Bob

WHAT IS COMMUNICATION ?

At least 2 parties



Sender

Alice

Receiver

Bob

a process by which
’nformation is sent by a sender to a rece'ver
via some medium

WHAT IS COMMUNICATION ?

Alice (Encoder) encodes

Sends

Bob (Decoder)
receives & decodes

WHAT IS COMMUNICATION?

Information is physcal

---Landauer

What is Communication?

Information's physical

---Landauer

information must be encoded in, and decoded from a physical system.

WHAT IS COMMUNICATION?

Information ’s phys'c al

---Landauer

information must be encoded in, and decoded from a physical system.

Classical World

encoding/decoding

red-green balls,

sign of charge of a particle.

Only orthogonal states

WHAT IS COMMUNICATION ?

Information 's phys'ca1

---I.andauer

information must be encoded in, and decoded from a physical system.

Classical World

encoding/decoding

rcd-cmcn balls,

sign of charge of a particle.

Only orthogonal states

Quantum World Nonorthogonal states

WHAT IS COMMUNICATION?

Information s phys cal

---Landauer

Do quantum states advantageous?

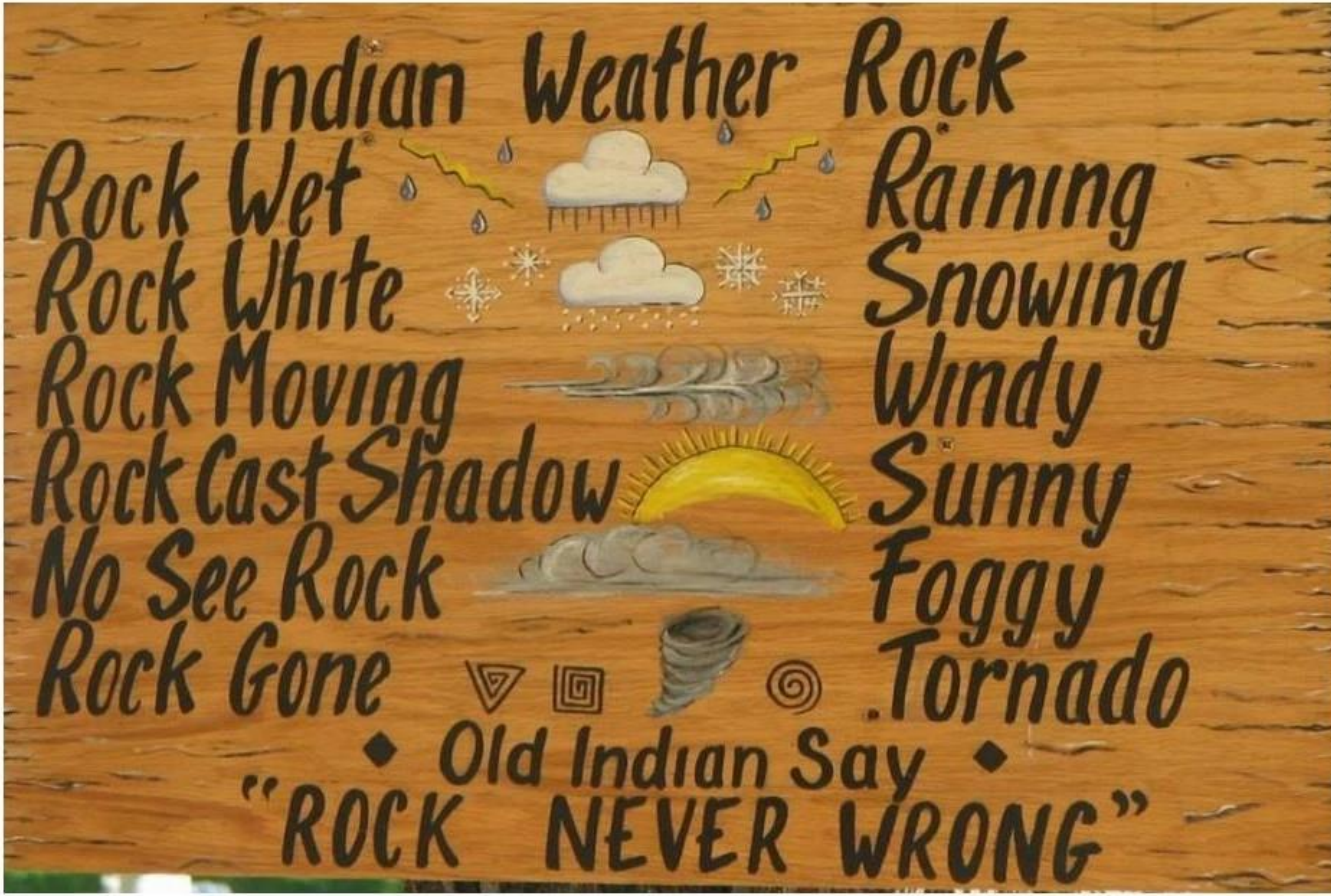
Classical Information Transmission via Quantum States

Part 1

Quantum Dense Coding

Bennett & Wiesner, PRL 1992

CLASSICAL PROTOCOL



Classical Protocol

Sunny

CLASSICAL PROTOCOL

Sunny

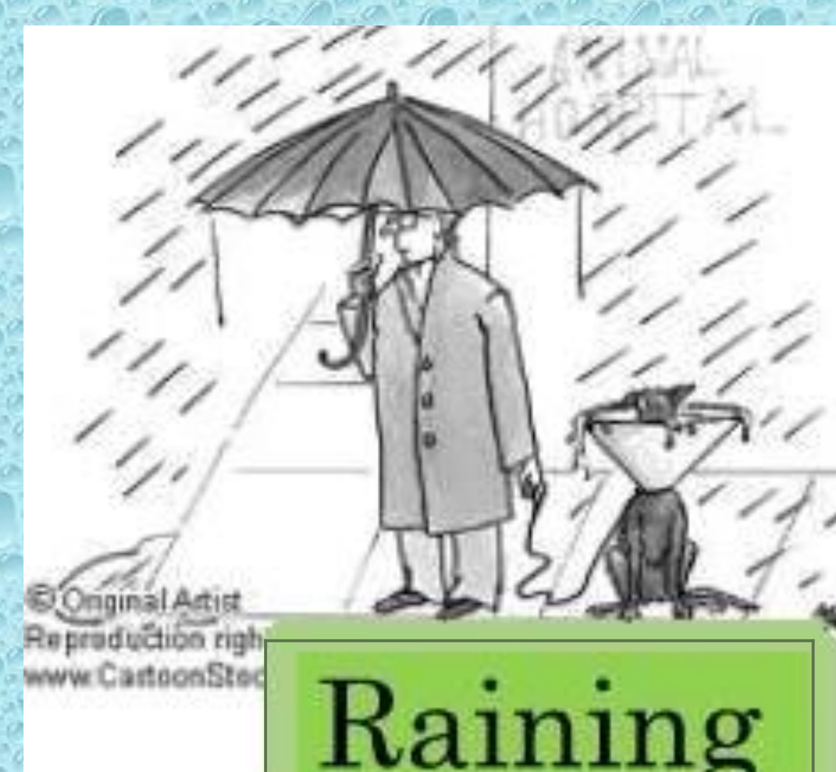
Windy

CLASSICAL PROTOCOL

Sunny

Windy

Snowing



Raining

CLASSICAL PROTOCOL

Sunny

Windy

Snowing

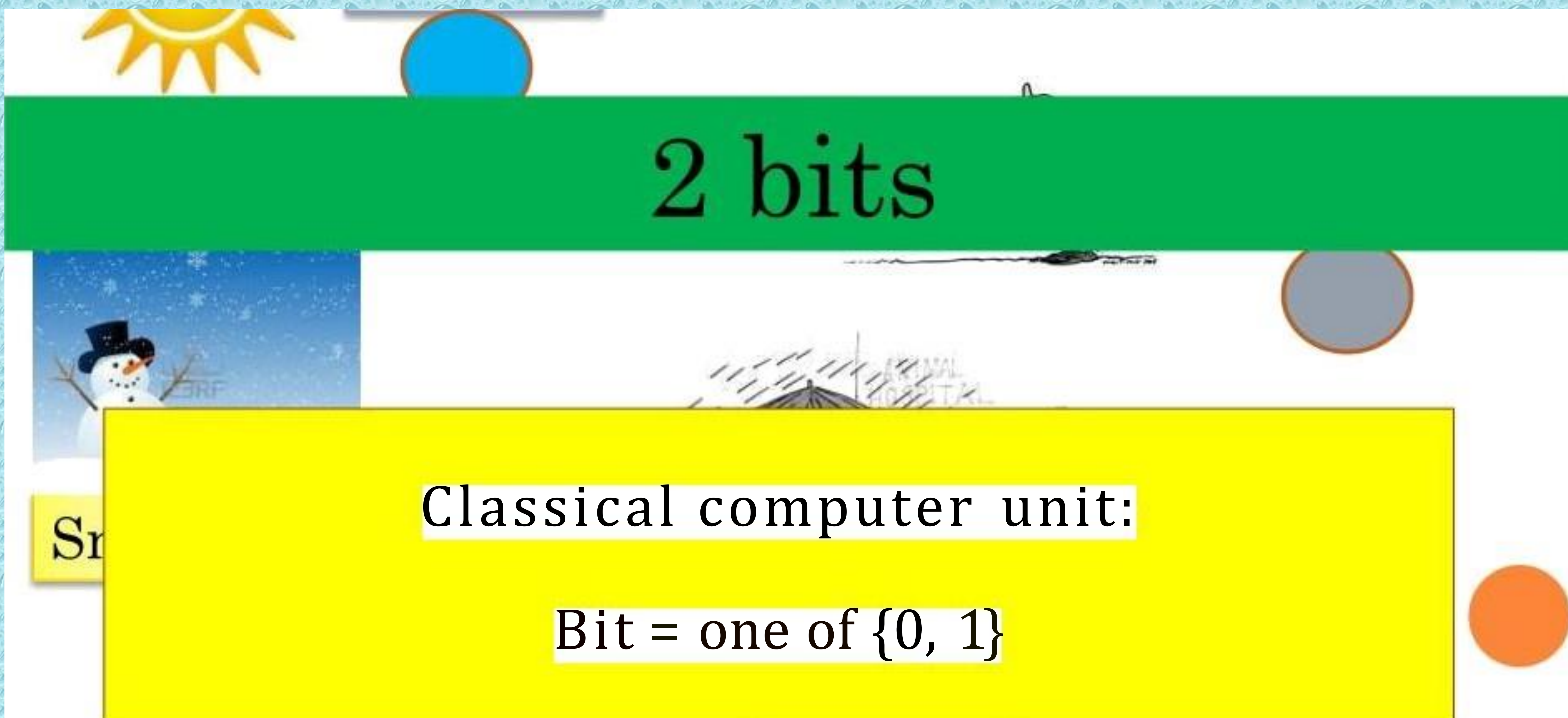
Raining

CLASSICAL PROTOCOL

Sunny

Classical Protocol

funny



2 bits

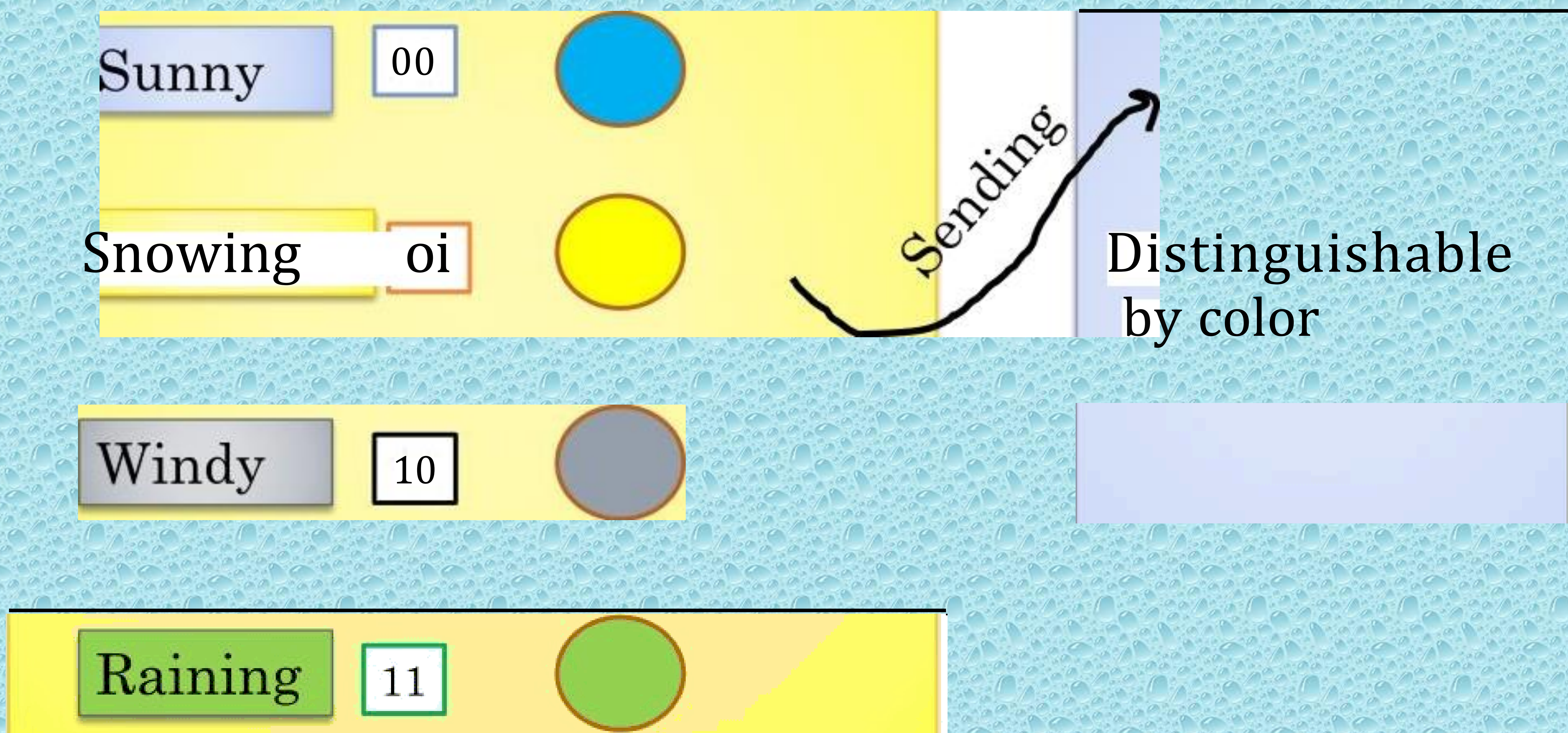
Classical computer unit:

Bit = one of $\{0, 1\}$

CLASSICAL PROTOCOL

Alice Bob

Message Fncoding Decoding



CLASSICAL PROTOCOL

Alice

Bob

Message

Fncoding

Decoding

Sunny

2 bits → 4 dimension

by color

Windy

Raining

What abt Quantum?

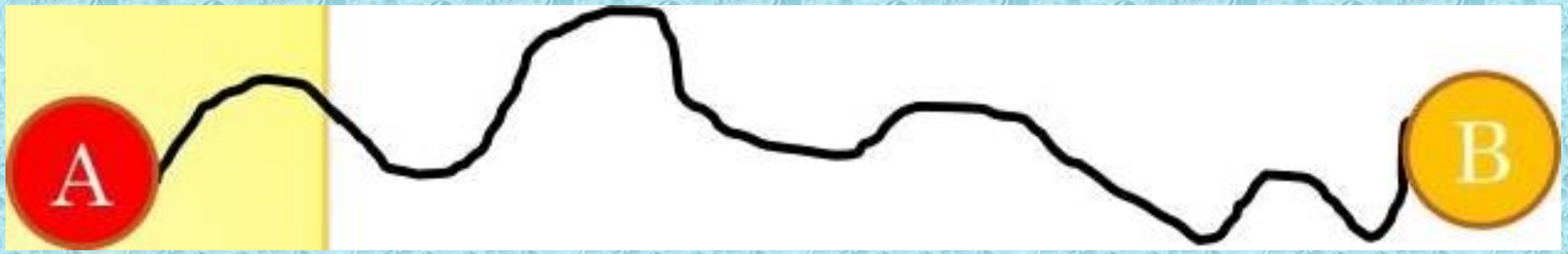
QUANTUM PROTOCOL

Alice

Bob

Message

Sunny



Snowing

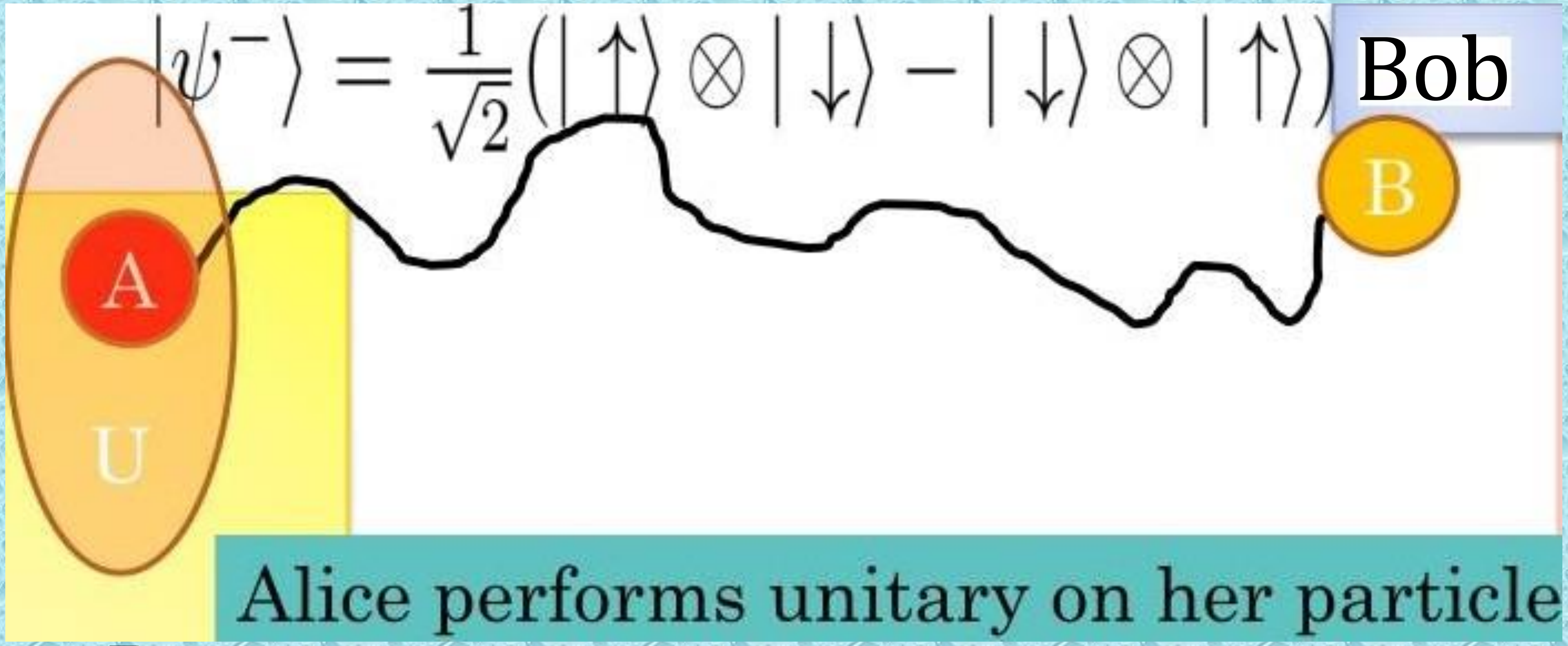
$$|\psi^-\rangle \; \frac{}{\sqrt{2}} \; |\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle)$$

Windy

Ringlet state

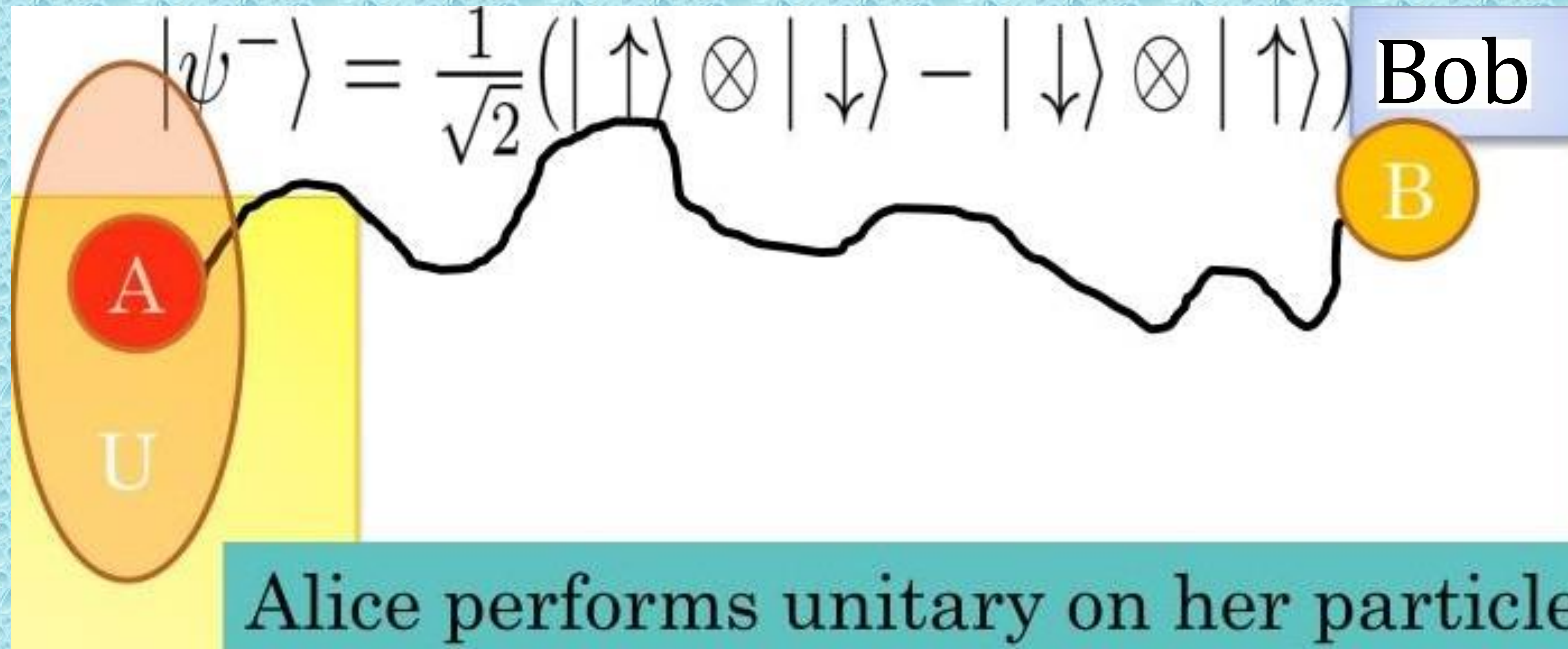
Raining

Alice



Message	
Sunny	I
Snowing	σ_z
Windy	σ_x
Raining	σ_y

Alice

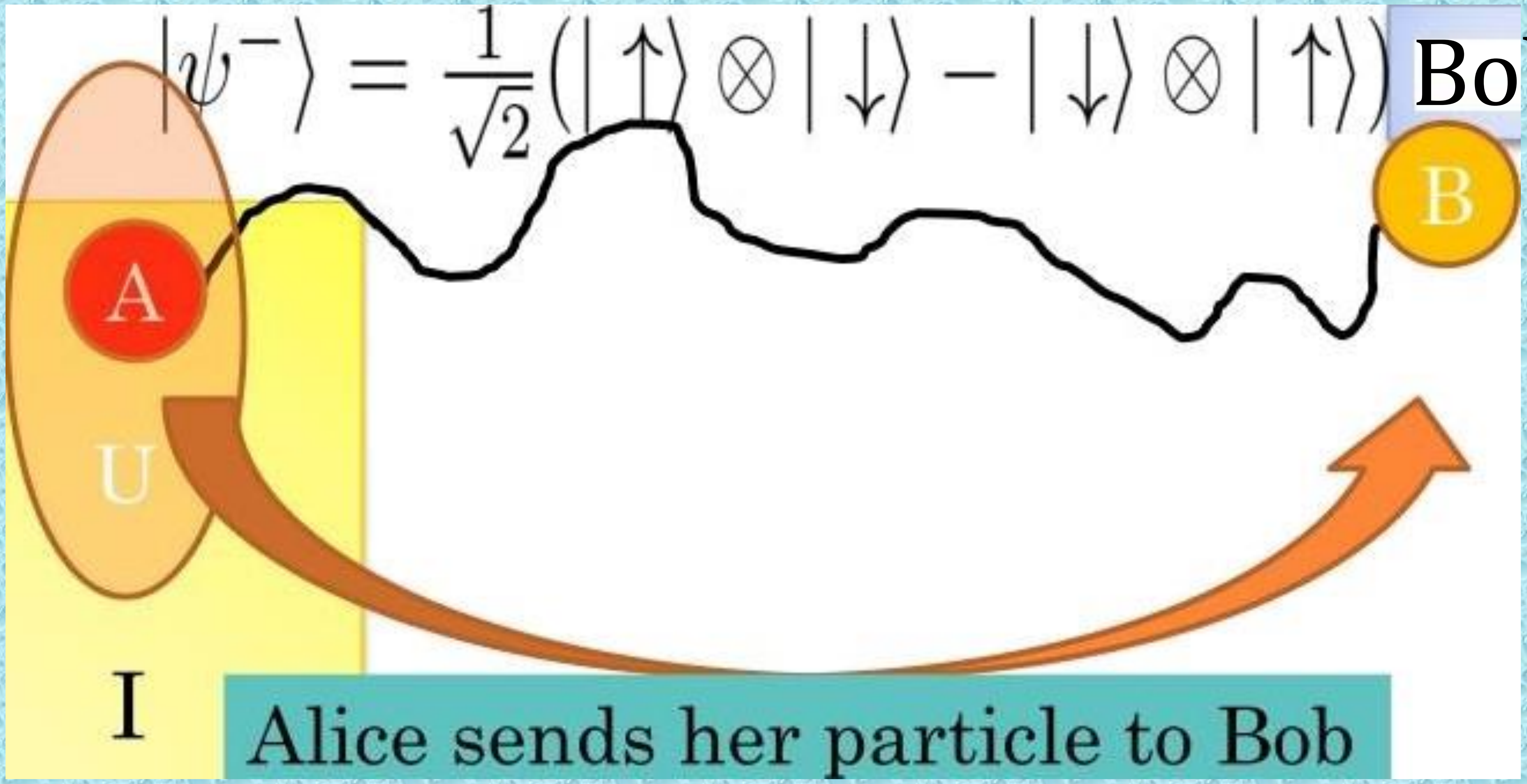


Message	
Sunny	I
Snowing	σ_z
Windy	σ_x
Raining	σ_y

Creates 4 orthogonal states

Singlet, Triplets

Alice



Bob

Message

Sunny

Snowing σ_z

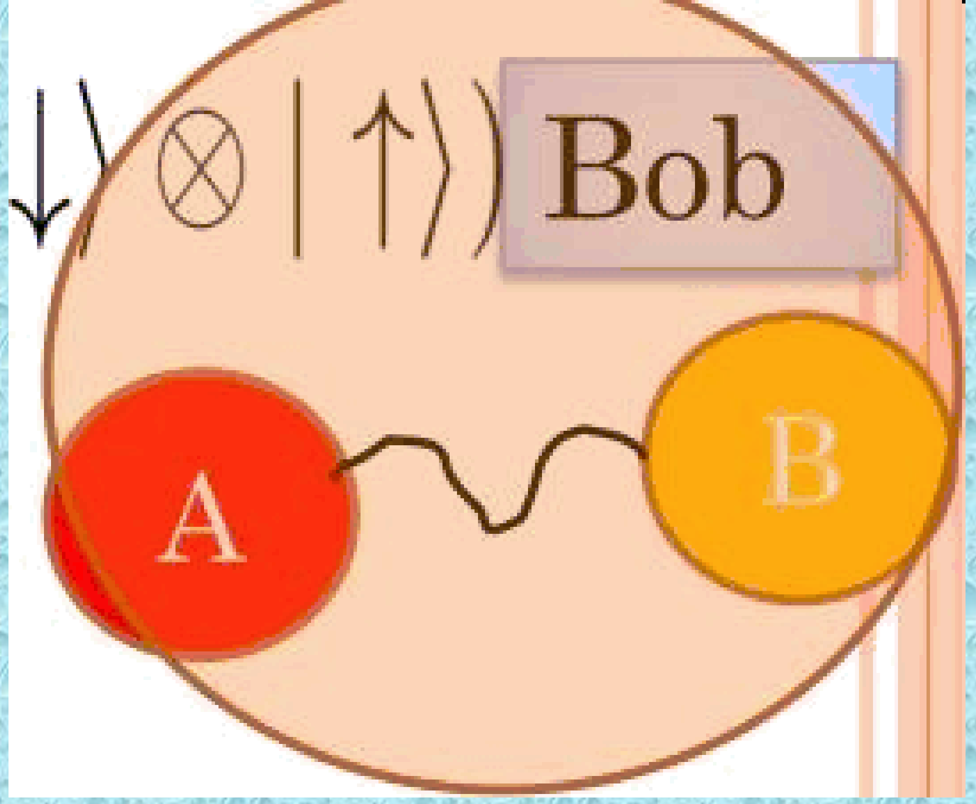
Windy σ_x

Raining σ_y

Alice

$\psi^-\rangle = \frac{}{\sqrt{2}}(| \quad | \quad |\downarrow\rangle \otimes |\uparrow\rangle)$

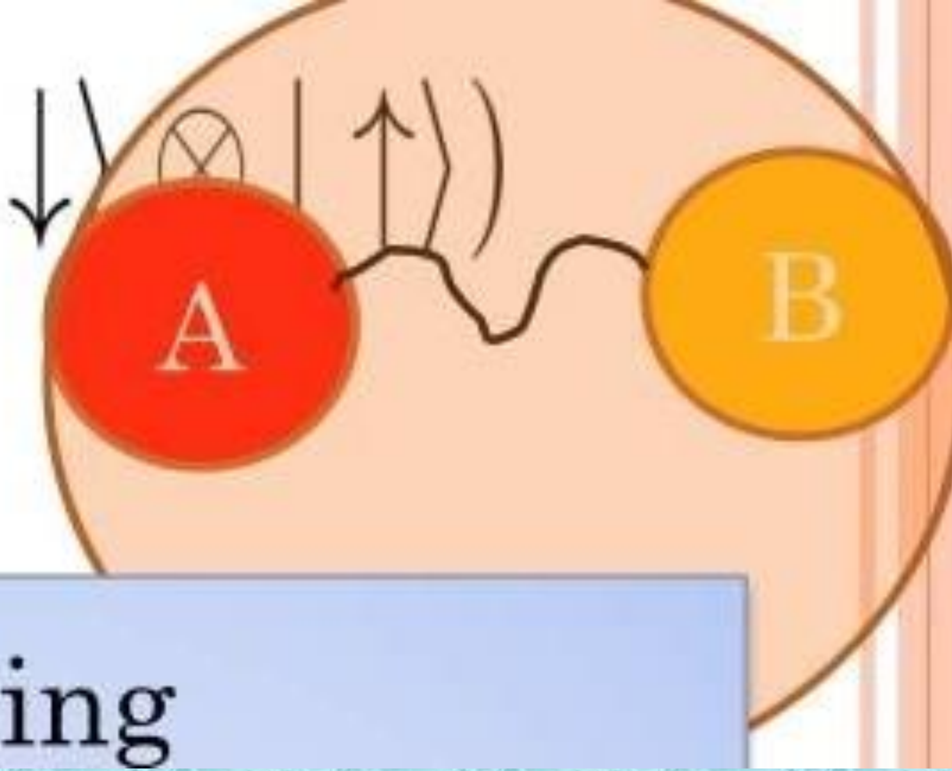
Bob



Message	
Sunny	I
Snowing	σ_z
Windy	σ_x
Raining	σ_y

Bob has 2 particles:
one of the triplets or singlet

$$\psi^-\rangle = \frac{}{\sqrt{2}}(\ \uparrow\rangle \otimes \ \downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle)$$



Alice Bob

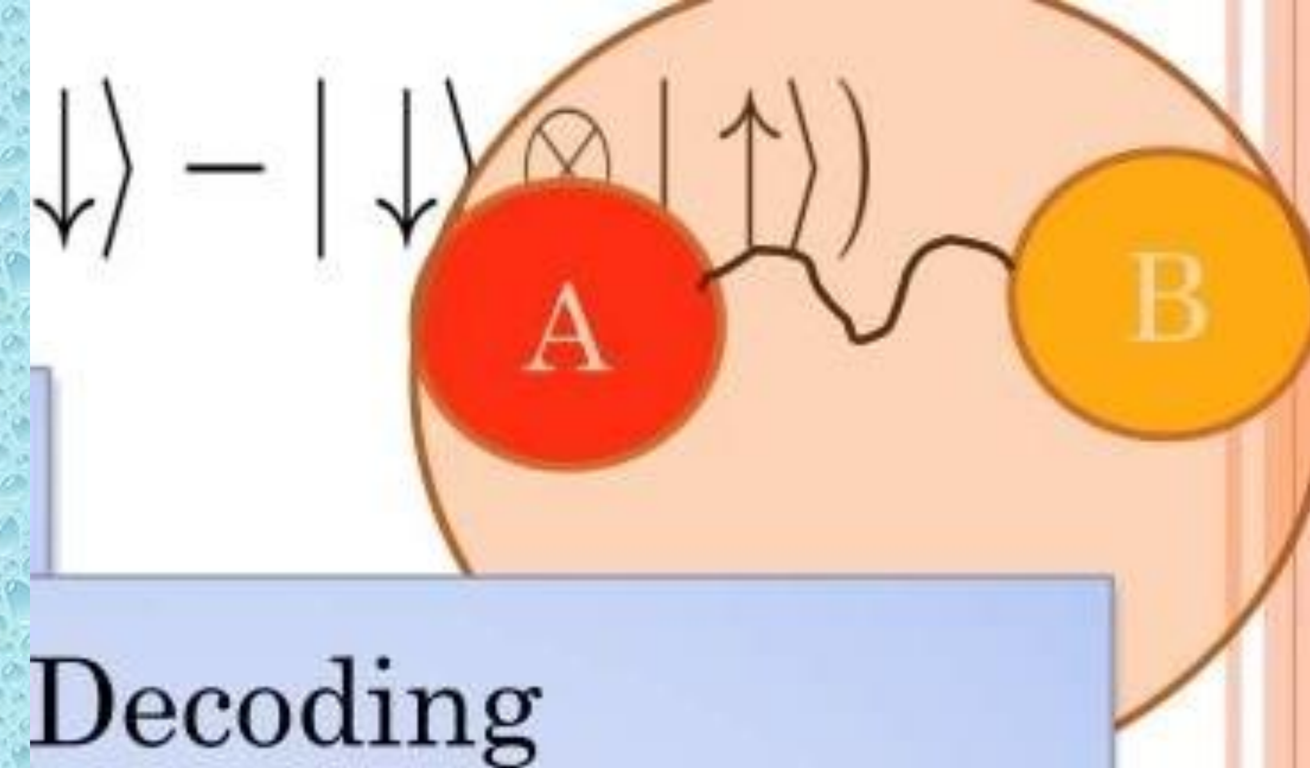
Decoding

Message

Sunny	I	
Snowing	σ_z	
Windy	σ_x	
Raining	σ_y	

4 orthogonal states
Possible to distinguish

$$\psi^-\rangle = \frac{}{\sqrt{2}}(\ \uparrow\rangle \otimes \ \downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle)$$

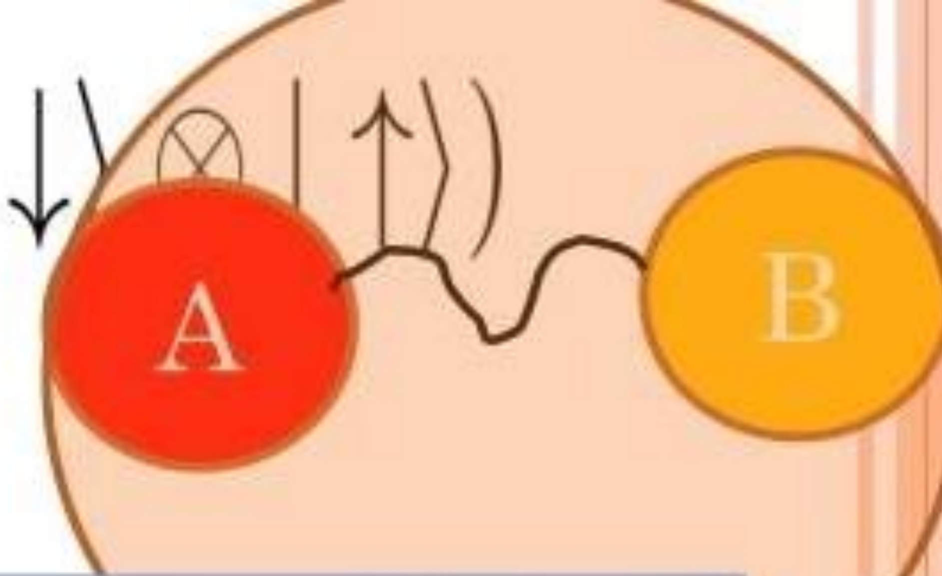


Alice Bob

Message

Sunny	I	
Snowing	σ_z	4 orthogonal states Possible to distinguish
Windy	σ_x	
Raining	σ_y	Decodes message

$$\psi^-\rangle = \frac{}{\sqrt{2}}(\uparrow\rangle \otimes \downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle)$$



Alice

Bob

Decoding

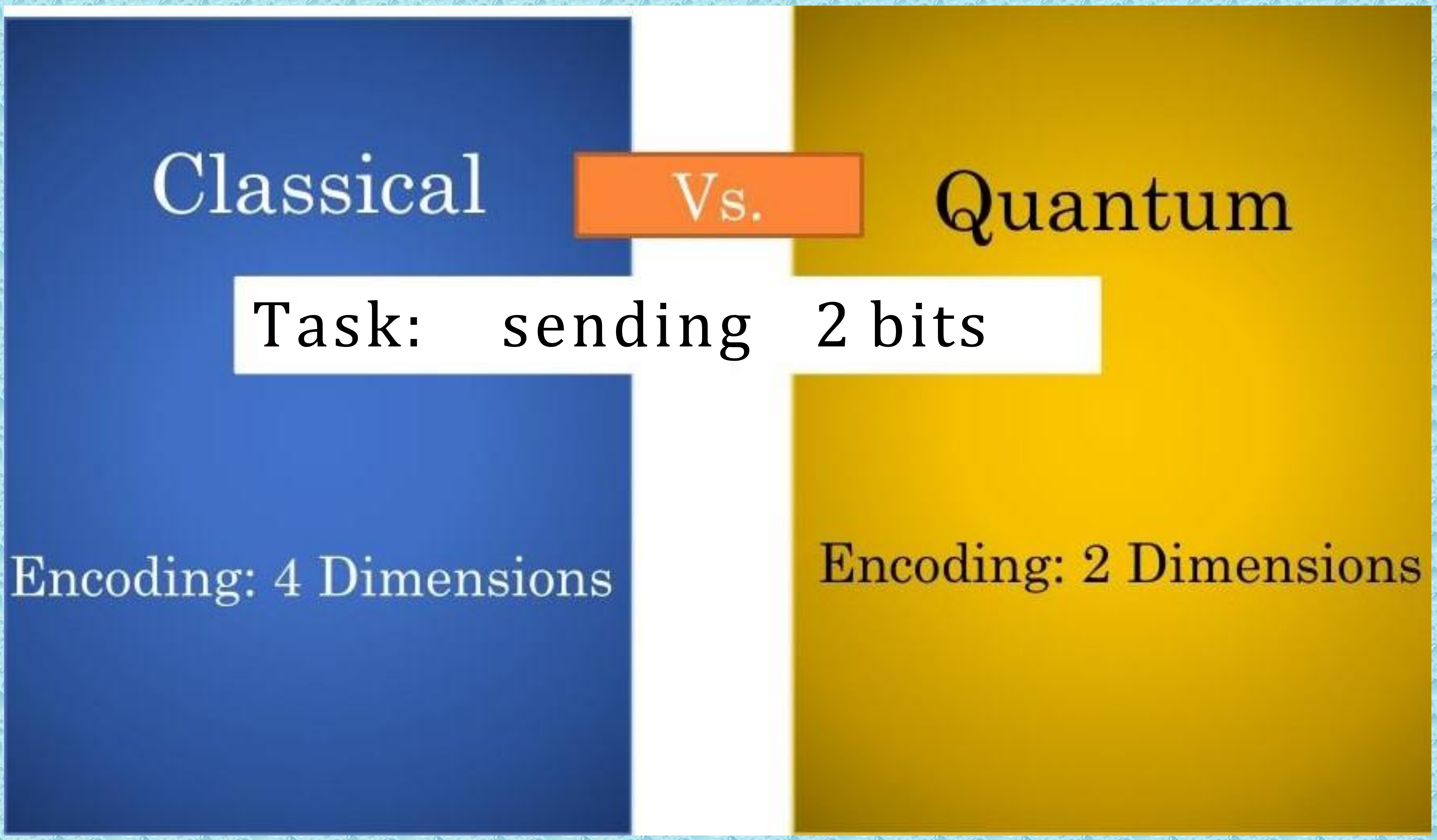
Message

Sunny	I	
Windy	σ_x	
Raining	σ_y	

2 bits → 2 dimension

Possible to distinguish

MORAL


Classical
Vs.
Quantum
Task: sending 2 bits
Encoding: 4 Dimensions
Encoding: 2 Dimensions

MORAL

Classical

Vs.

Quantum

Task: sending 2 bits

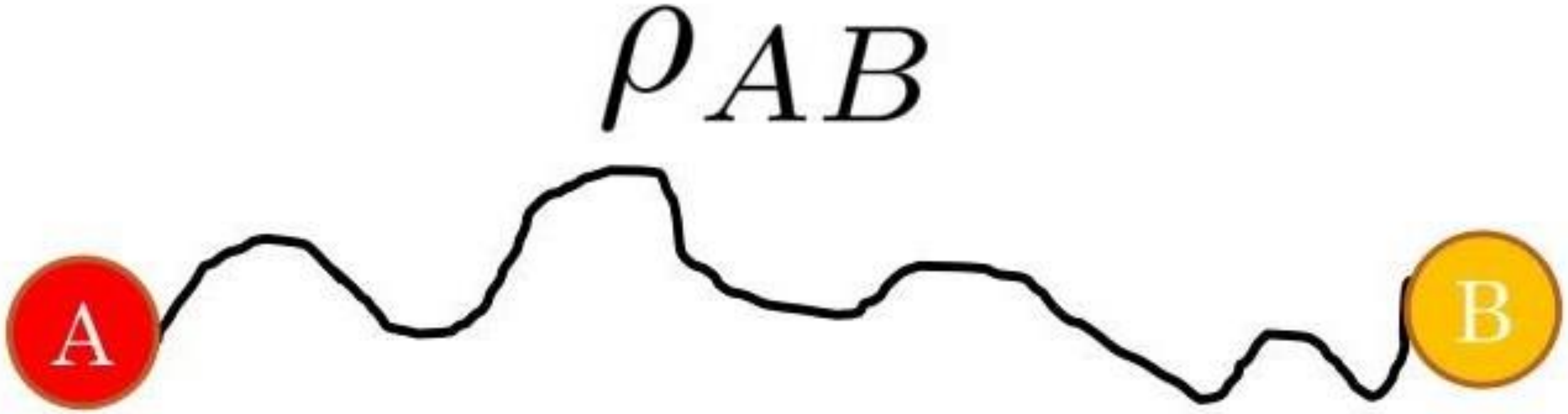
Encoding: 4 Dimensions

Encoding: 2 Dimensions

Bennett & Weisner, PRL ***69****, 2881 ('92).*

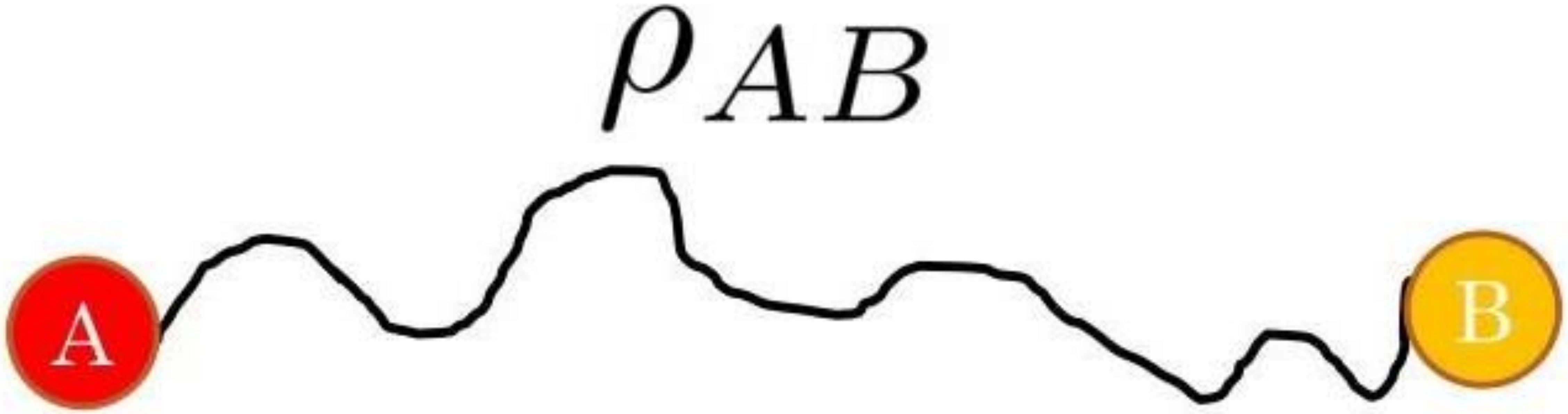
DENSE CODING FOR ARBITRARY STATE

Hiroshima, J. Phys. A ’01;
Ziman & Buzek, PRA ’03,
Bruss, D’Ariano, Lewenstein, Macchiavello, ASD, Sen, PRL’ 04



Alice & Bob share a state ρ_{AB}

Encoding



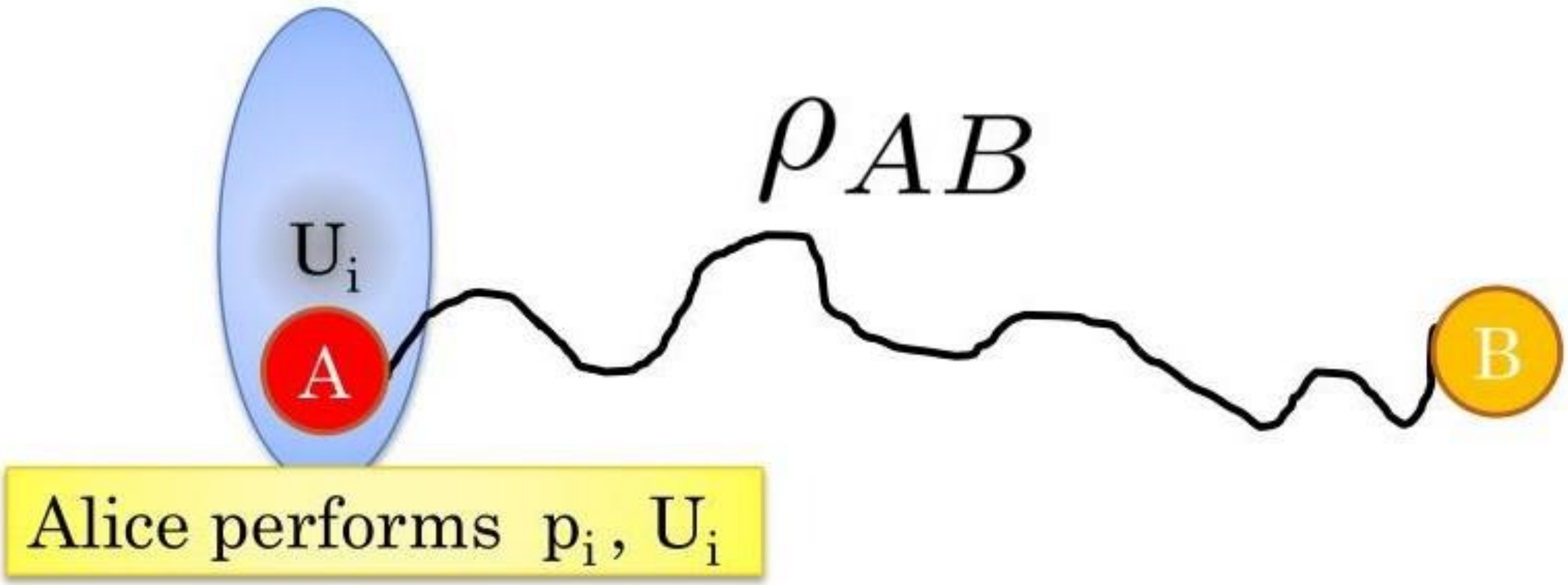
Alice's aim:
to send classical info i

Encoding

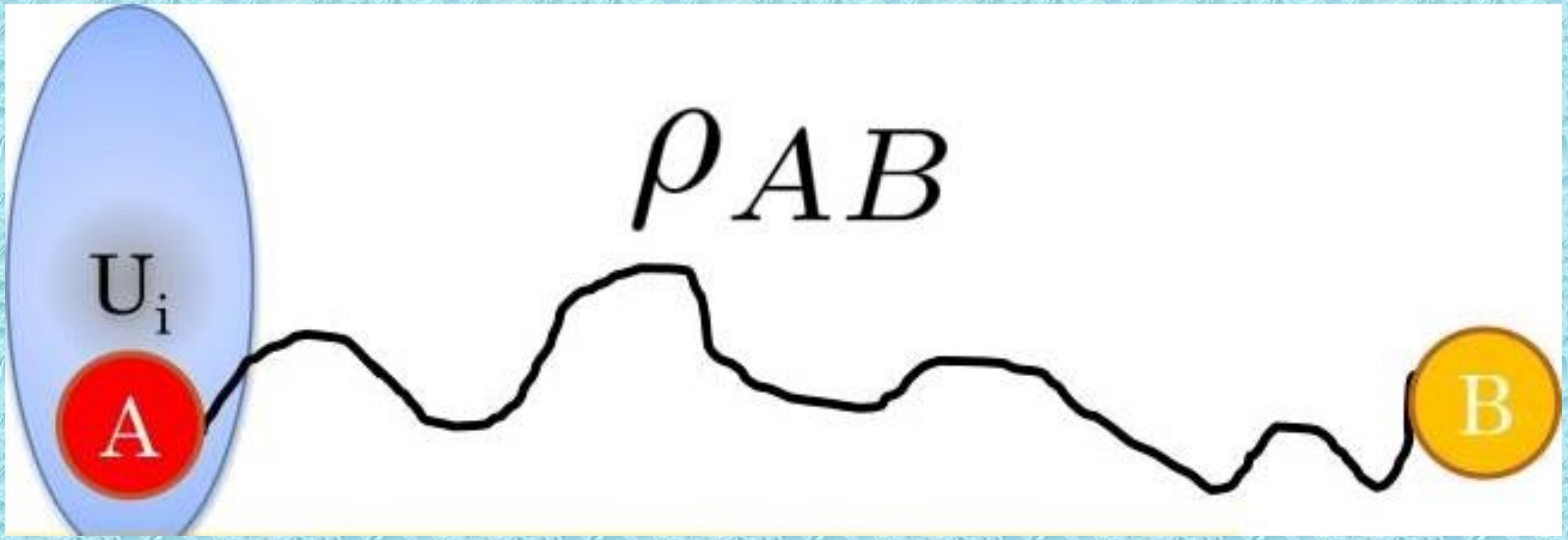
ρ_{AB}

Alice s aim:
to send classical info i
which occurs with probability p_i

Encoding



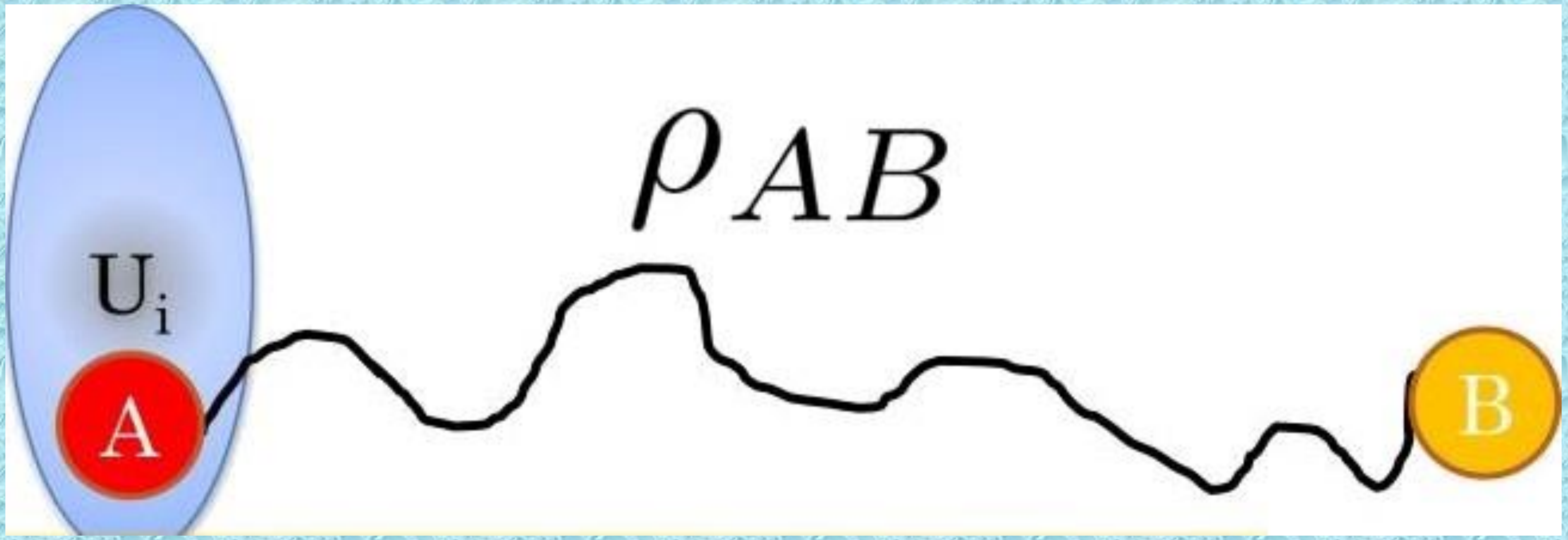
Encoding



Alice performs p_i U_i

she produces the ensemble $\mathcal{E} = \{p_i, \rho_i\}$

Encoding

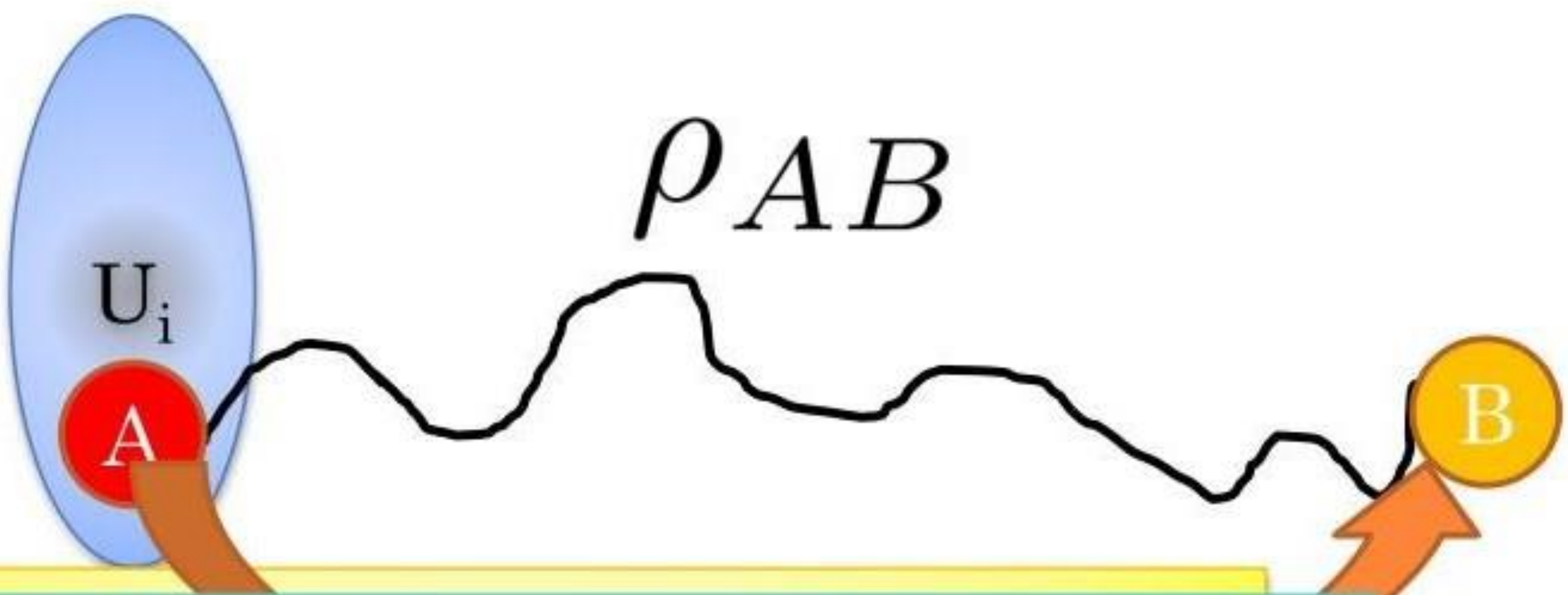


Alice performs p_i U_i

she produces the ensemble 6 = {p_i p_i}

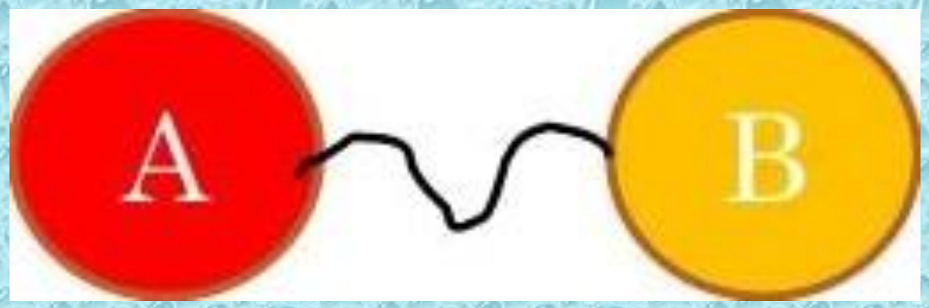
$$pt = U_i^A \otimes I^B PA_B (U_i^A) \otimes I^B$$

Sending



Alice sends her particle to Bob

Decoding

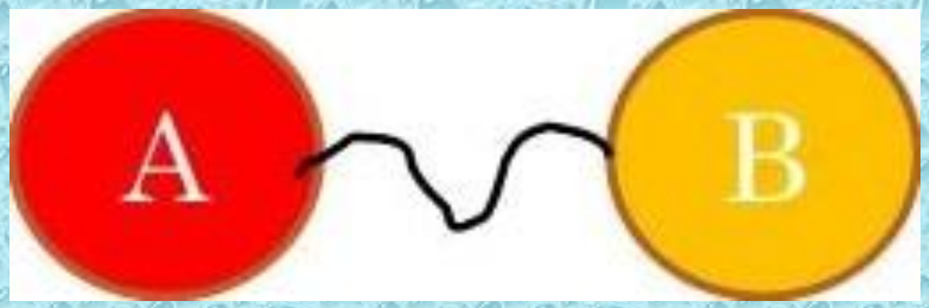


Alice

Bob

Decoding

Alice



Bob's task:
Gather info abt i

Quantum Communication

- Quantum Communication enables secure information exchange using quantum mechanics principles.
- Keywords: Quantum Bits (Qubits), Quantum States, Information Security
- Unlike classical communication, quantum communication utilizes the properties of quantum mechanics, such as superposition and entanglement, to enhance security and efficiency.
- The Quantum Internet enables quantum devices to exchange information using quantum states such as qubits.
- Keywords: Quantum Signals, Qubits, Entanglement, Quantum Teleportation
- Difference from Classical Internet: Classical bits operate on binary values (0s and 1s), while quantum bits (qubits) can exist in a superposition of states, providing enhanced security and computational power.

Quantum vs classical communication

- **Conventional Communication Systems**
- Transmitter sends data as a sequence of bits (0s and 1s).
- The bit sequence undergoes several processing steps before reaching the receiver.
- Transmission is based solely on bits.
- If any branch or interference occurs between the receiver and transmitter, it can be detected.
- **Quantum Communication Systems**

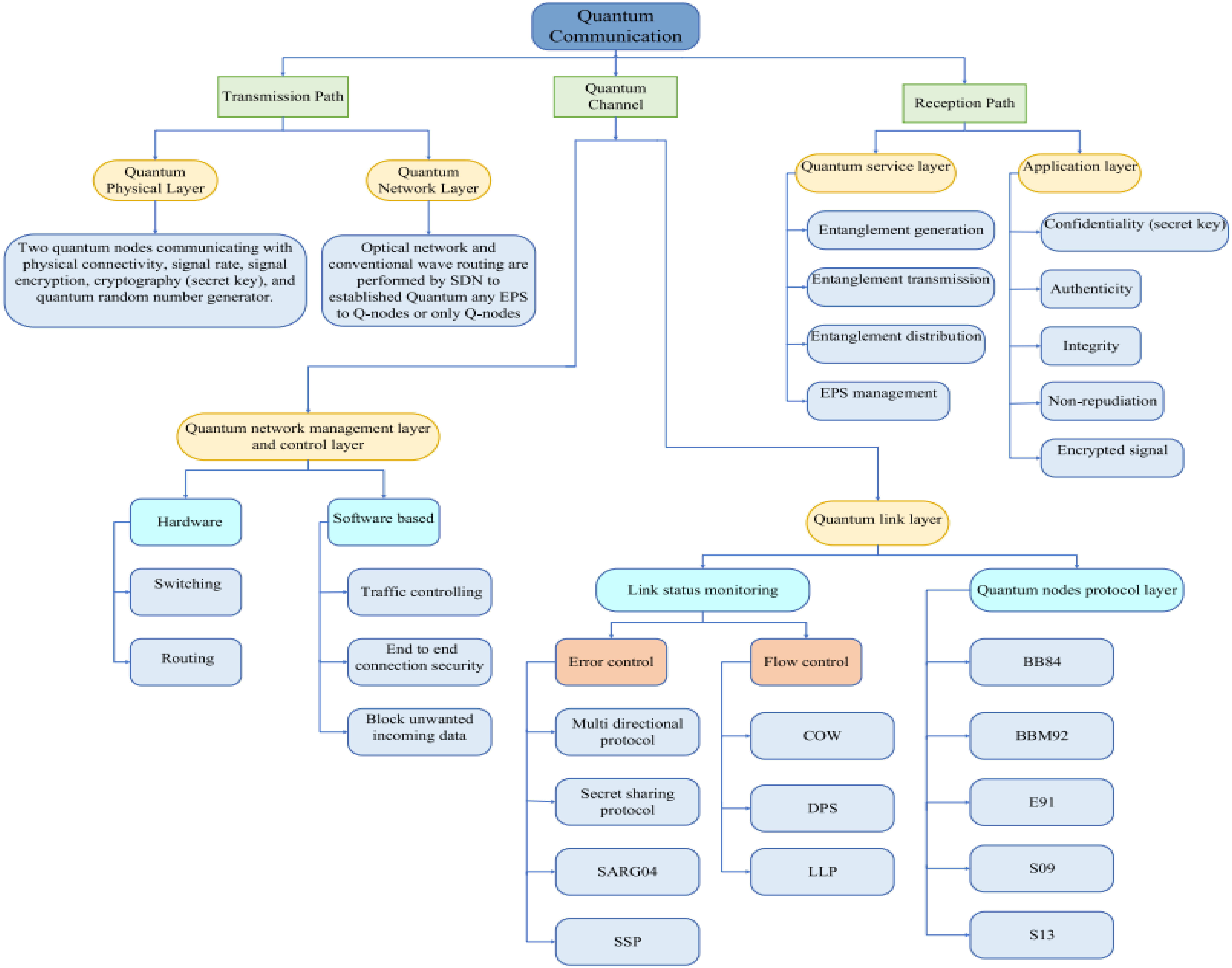
- Transmitter sends data as qubits.
- A single qubit can represent two bits of information.
- In general, **n** qubits can represent 2n2^n2n bits of information.
- The presence of branches or interference between the receiver and transmitter cannot be detected due to:
    - Entangled particles.
    - Quantum states.

Key Concepts:

Superposition: A fundamental property allowing qubits to be in multiple states simultaneously.

Entanglement: A phenomenon where qubits become correlated, so the state of one qubit affects the state of another, no matter the distance.

Quantum Teleportation: The process of transferring quantum states between qubits using entanglement and classical communication.


Quantum Communication
Transmission Path
Quantum Channel
Reception Path
Quantum Physical Layer
Quantum Network Layer
Two quantum nodes communicating with physical connectivity, signal rate, signal encryption, cryptography (secret key), and quantum random number generator.
Optical network and conventional wave routing are performed by SDN to established Quantum any EPS to Q-nodes or only Q-nodes
Quantum service layer
Application layer
Entanglement generation
Entanglement transmission
Entanglement distribution
EPS management
Confidentiality (secret key)
Authenticity
Integrity
Non-repudiation
Encrypted signal
Quantum network management layer and control layer
Hardware
Switching
Routing
Software based
Traffic controlling
End to end connection security
Block unwanted incoming data
Quantum link layer
Link status monitoring
Quantum nodes protocol layer
Error control
Multi directional protocol
Secret sharing protocol
SARG04
SSP
Flow control
COW
DPS
LLP
BB84
BBM92
E91
S09
S13

BB84 PROTOCOL

- This protocol is mainly designed based on Heisenberg's uncertainty principle and which is also familiarized as BB84 protocol.

- Steps of BB84 protocol are as:

- **Step 1:** Alice selects an n arbitrary bit using a flipping coin.

- **Step 2:** Alice must flip the coin n times more to determine the basis, for each matching corresponding arbitrary bit.

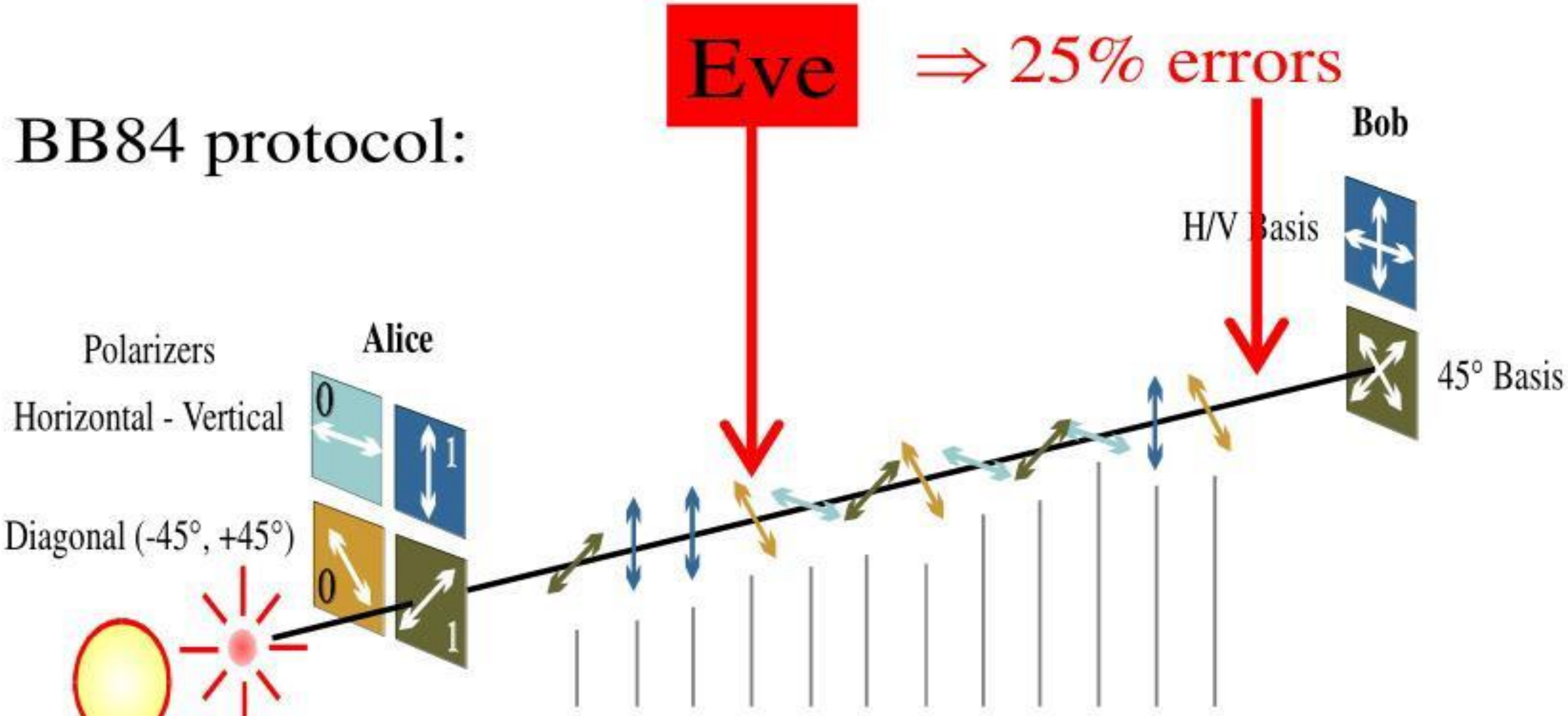
- **Step 3:** Bob receives the arbitrary bits that Alice prepared in their corresponding bases.

- **Step 4:** Bob does not know the source corresponding to each arbitrary bit. Now, he tosses the coin n number of times. So that he can measures the received qubits in the obtained number of basis after tossing the coin. Bob declares the receiving of states.

- **Step 5:** Alice and Bob use a classical channel to publicly compare their bases. They discard bits where their bases disagree, resulting in \(n/2 \) bits. Bob then randomly selects \(n/4 \) bits from the remaining \(n/2 \) bits and compares them. If the discrepancies exceed a permissible threshold, they discard the entire series, indicating potential eavesdropping by Eve; otherwise, the remaining bits form their shared key.

Geneva University GAP Optique

BB84 protocol:



Alice's Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob's Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0

BBM92 PROTOCOL

- Both classical information and quantum information are mixed in this protocol.
- **Step 1:** Alice generates strings of EPR pairs q with the size n and then transmits strings of qubits qb from every single EPR pair with the size of n to Bob via a quantum channel. The other strings if qubits qa remain from every single pair with the size of n.

- **Step 2:** Alice generates a string of bits with the size of n arbitrary, which is denoted as Ba.

- **Step 3:** Bob receives qb and then randomly generates string of bits Bb with the size of n.

- **Step 4:** Now, Alice measures every single qubit of qb corresponding to bits Ba if Bai = 0, the**Step 6:** n it uses x axis; else if Bai = 1, then it uses z axis.

- **Step 5:** After that, Bob measures every single qubit of qb corresponding to the bits of Bb if Bbi = 0, then it will use x axis; else if Bbi = 1, then it will use z axis.

- Bob transmits his measurement axis by choices by Bb to Alice via the public channel & after receiving Bb, Alice transmits her axis choice Ba to Bob via the public channel and the Bob receives Ba.

- **Step 7:** Alice and Bob discard instances where measurements are taken on different axes or where detection fails due to imperfect quantum efficiency. The remaining instances are then used to generate their private key \(K_{a,b} \).

E91 PROTOCOL

- In 1991, E91 protocol was first proposed by A. Ekert.
- He tested eavesdropping by using generalized Bell's theorem. In order to generate identical random numbers at distant locations, his method utilized Bohm's version of the EPR.
- E91 is composed of the following steps

- **Step 1:** Alice and Bob obtain their entangled photons from a prime source, in one out of four utmost entangled states ($|\psi 1\rangle$ to $|\psi 4\rangle$ Consider the source produce EPR pair $|\psi 3\rangle$

- **Step 2:** Now, Alice measures her particle, which she received from entangle pair among any of the 0-, 45-, and 90-degree bases.

- **Step 3:** Next, Bob measures his particle, which he received from entangle pair among any of the 45, 90, and 135 degree bases.

- **Step 4:** After that, Alice and Bob measure the particle in a same base and remove the particle from a different base. If the base is the same, they obtain a common key. If any bits or particles remain that are known by shifted key.

- **Step 5:** Finally, Alice and Bob check the system and then make the decision by interchanging the key's hashes, either accepting or throwaway the keys.