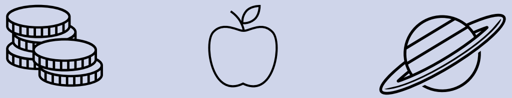
Entangled Systems and Application in QKD

Vu Quang Minh

Computer Communications Laboratory, The University of Aizu

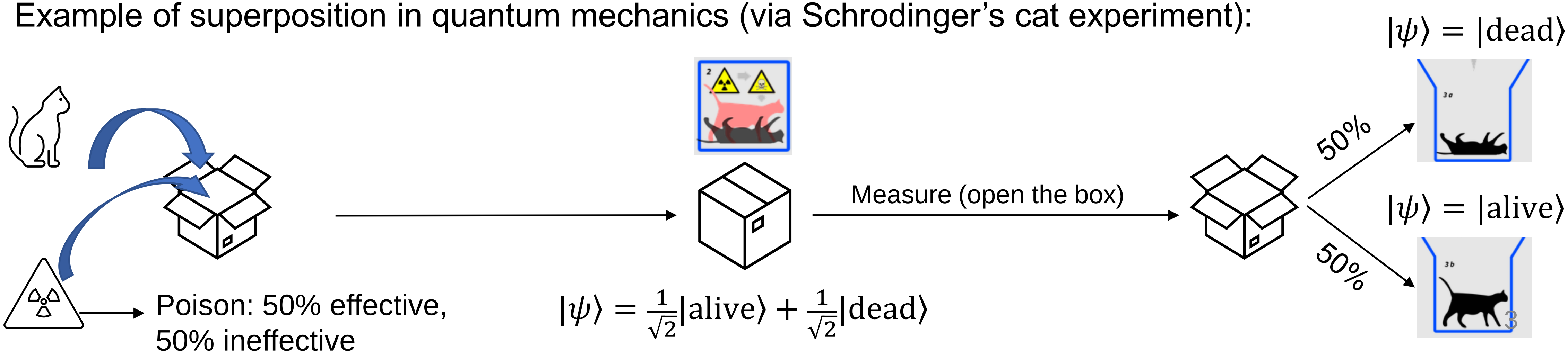
Contents

Wave function & Superposition

Classical Mechanics	Quantum Mechanics
It deals with macroscopic objects 	It deals microscopic (very small) particles Electrons, photons
Each object is in a deterministic state	These particles are in two or more states simultaneously (superposition)

→ The wavefunction ($|\psi\rangle$) is used to describe the states of particles in quantum mechanics

Example of superposition in quantum mechanics (via Schrodinger's cat experiment):



Single Quantum Bit (Qubit) System

- This is a system with two basis state $|0\rangle$ and $|1\rangle$
- Example: Electron spin, polarization of a photon
- The wave function for a single qubit system is the superposition of state $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α, β are real number, $\alpha^2 + \beta^2 = 1$

- We can not get the information of the qubit in the system until we measure it

Premeasured wave function	Measurement outcome	Probability of outcome	Post-measured wave function
$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$	0	α^2	$\|0\rangle$
	1	β^2	$\|1\rangle$
$\|\psi\rangle = \frac{1}{2}\|0\rangle + \frac{\sqrt{3}}{2}\|1\rangle$	0	$\left(\frac{1}{2}\right)^2 = 25\%$	$\|0\rangle$
	1	$\left(\frac{\sqrt{3}}{2}\right)^2 = 75\%$	$\|1\rangle$

Two Qubit System

- We consider a system of two qubits

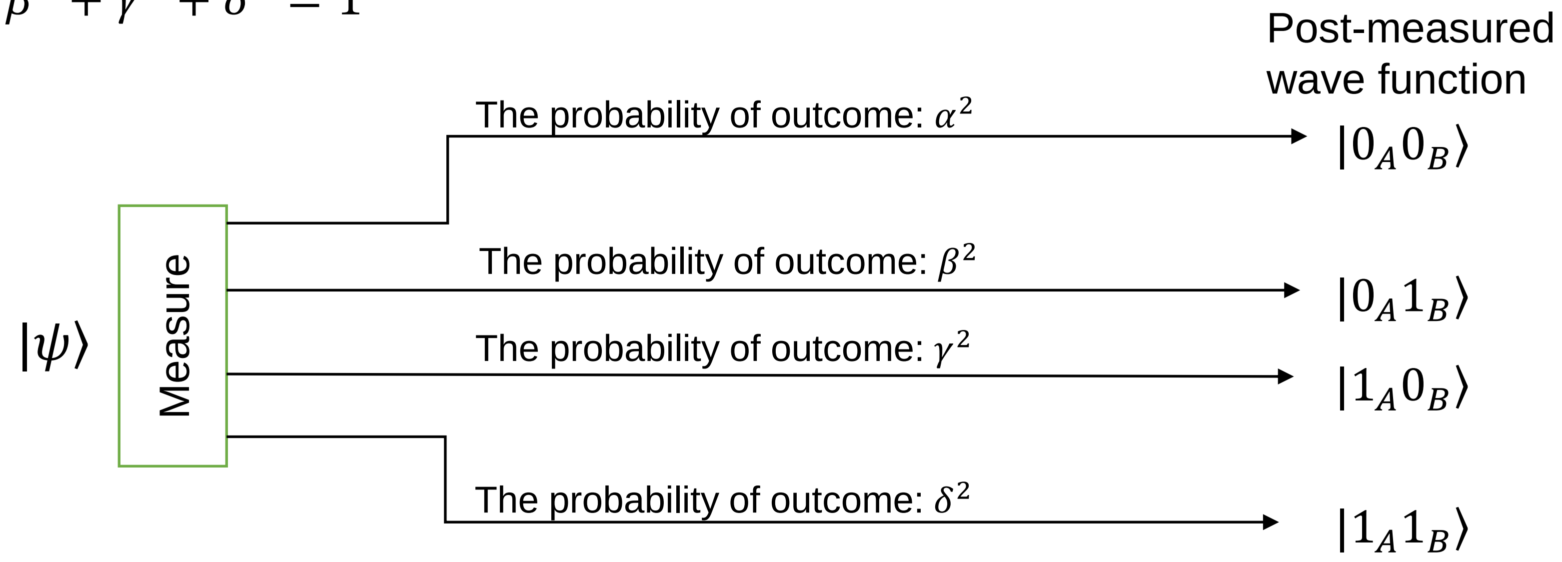
Qubit A
$|0_A\rangle$, $|1_A\rangle$

Qubit B
$|0_B\rangle$, $|1_B\rangle$

- The wave function of the system is the superposition of four states $|0_A 0_B\rangle, |0_A 1_B\rangle, |1_A 0_B\rangle, |1_A 1_B\rangle$

$$|\psi\rangle = \alpha|0_A 0_B\rangle + \beta|0_A 1_B\rangle + \gamma|1_A 0_B\rangle + \delta|1_A 1_B\rangle$$

where $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$



Non-entangled (Separable) System

- Consider a two qubit system
- The wave function of the system

$$|\psi\rangle = \alpha|0_A 0_B\rangle + \beta|0_A 1_B\rangle + \gamma|1_A 0_B\rangle + \delta|1_A 1_B\rangle \ (\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1)$$

- This system is *non-entangled* if the wave function of this system can be written as the product of two wave functions of two independent quantum system

$$|\psi\rangle = \alpha|0_A 0_B\rangle + \beta|0_A 1_B\rangle + \gamma|1_A 0_B\rangle + \delta|1_A 1_B\rangle = \underbrace{(a|0_A\rangle + b|1_A\rangle)}_{\text{System A}}\underbrace{(c|0_B\rangle + d|1_B\rangle)}_{\text{System B}}$$

$$= \mathrm{ac}|0_A 0_B\rangle + \mathrm{ad}|0_A 1_B\rangle + \mathrm{bc}|1_A 0_B\rangle + \mathrm{bd}|1_A 1_B\rangle$$

where $\mathrm{a}^2 + \mathrm{b}^2 = 1, \mathrm{c}^2 + \mathrm{d}^2 = 1$

In other words, we can find 4 number a, b, c, d so that

$$\begin{array}{c} \alpha = ac \\ \beta = ad \\ \gamma = bc \\ \delta = bd \end{array} \quad \text{and} \quad \begin{array}{c} \mathrm{a}^2 + \mathrm{b}^2 = 1, \mathrm{c}^2 + \mathrm{d}^2 = 1 \\ (\mathrm{a}^2 + \mathrm{b}^2)(\mathrm{c}^2 + \mathrm{d}^2) = 1 \end{array}$$

Non-entangled (Separable) System (2)

- Property:
  - Two qubits in the non-entangled system can be measured independently
    - Before or after the first qubit is measured, the probability of the second qubit's measurement is unchanged
  - Explain:

From the condition $(\mathrm{a}^2 + \mathrm{b}^2)(\mathrm{c}^2 + \mathrm{d}^2)$ =1 we have $a^2 + b^2 = \frac{1}{c^2+d^2}$

The wave function of the non-entangled system

$$|\psi\rangle = (a|0_A\rangle + b|1_A\rangle)(c|0_B\rangle + d|1_B\rangle) = \mathrm{ac}|0_A 0_B\rangle + \mathrm{ad}|0_A 1_B\rangle + \mathrm{bc}|1_A 0_B\rangle + \mathrm{bd}|1_A 1_B\rangle$$

- Before qubit A is measured
  - The probability that we can measure $|0_B\rangle$ = $a^2c^2 + \mathrm{b}^2c^2 = c^2(a^2 + b^2) = \frac{c^2}{c^2+d^2}$
- After qubit A is measured (assume $|0_A\rangle$ is the result of the measurement)
  - The wave function of the system is $|\psi\rangle_{new} = \frac{\mathrm{ac}|0_A 0_B\rangle + \mathrm{ad}|0_A 1_B\rangle}{\sqrt{a^2c^2+a^2d^2}}$
  - The probability that we can measure $|0_B\rangle$ = $\left(\frac{ac}{\sqrt{a^2c^2+a^2d^2}}\right)^2 = \frac{a^2c^2}{a^2c^2+a^2d^2} = \frac{c^2}{c^2+d^2}$

Entangled System

- The two qubit system is *entangled* if we cannot find 4 number a, b, c, d so that

$$\begin{aligned} \alpha &= ac \\ \beta &= ad \\ \gamma &= bc \\ \delta &= bd \end{aligned} \quad \text{and} \quad \begin{aligned} \mathrm{a}^2 + \mathrm{b}^2 = 1, \mathrm{c}^2 + \mathrm{d}^2 = 1 \\ (\mathrm{a}^2 + \mathrm{b}^2)(\mathrm{c}^2 + \mathrm{d}^2) = 1 \end{aligned}$$

Or $|\psi\rangle = \alpha|0_A 0_B\rangle + \beta|0_A 1_B\rangle + \gamma|1_A 0_B\rangle + \delta|1_A 1_B\rangle \neq (a|0_A\rangle + b|1_A\rangle)(c|0_B\rangle + d|1_B\rangle)$ with all a, b, c, d

- There are 4 special cases of entangled system (Bell states):

$$\frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \left(\alpha = \frac{1}{\sqrt{2}}, \beta = 0, \gamma = 0, \delta = \frac{1}{\sqrt{2}}\right)$$

$$\frac{|0_A 0_B\rangle - |1_A 1_B\rangle}{\sqrt{2}} \left(\alpha = \frac{1}{\sqrt{2}}, \beta = 0, \gamma = 0, \delta = \frac{-1}{\sqrt{2}}\right)$$

$$\frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}} \left(\alpha = 0, \beta = \frac{1}{\sqrt{2}}, \gamma = \frac{1}{\sqrt{2}}, \delta = 0\right)$$

$$\frac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}} \left(\alpha = 0, \beta = \frac{1}{\sqrt{2}}, \gamma = \frac{-1}{\sqrt{2}}, \delta = 0\right)$$

Entangled System (2)

- Property:
  - When we measure one qubit in the entangled system, the probability distribution of the other qubit is disclosed
    - In the entangled system with Bell states, when we measure one qubit, we can determine the state of the other qubit with certainty
- Example:
  - Consider an entangled system $|\psi\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}|0_A 1_B\rangle + \frac{1}{\sqrt{2}}|1_A 0_B\rangle$
  - When we measure the qubit A
    - The state if $|0_A\rangle$ is measured

$$|\psi\rangle_{new} = |0_A 1_B\rangle = |0_A\rangle|1_B\rangle$$

$\rightarrow$ The state of the qubit B is $|1_B\rangle$

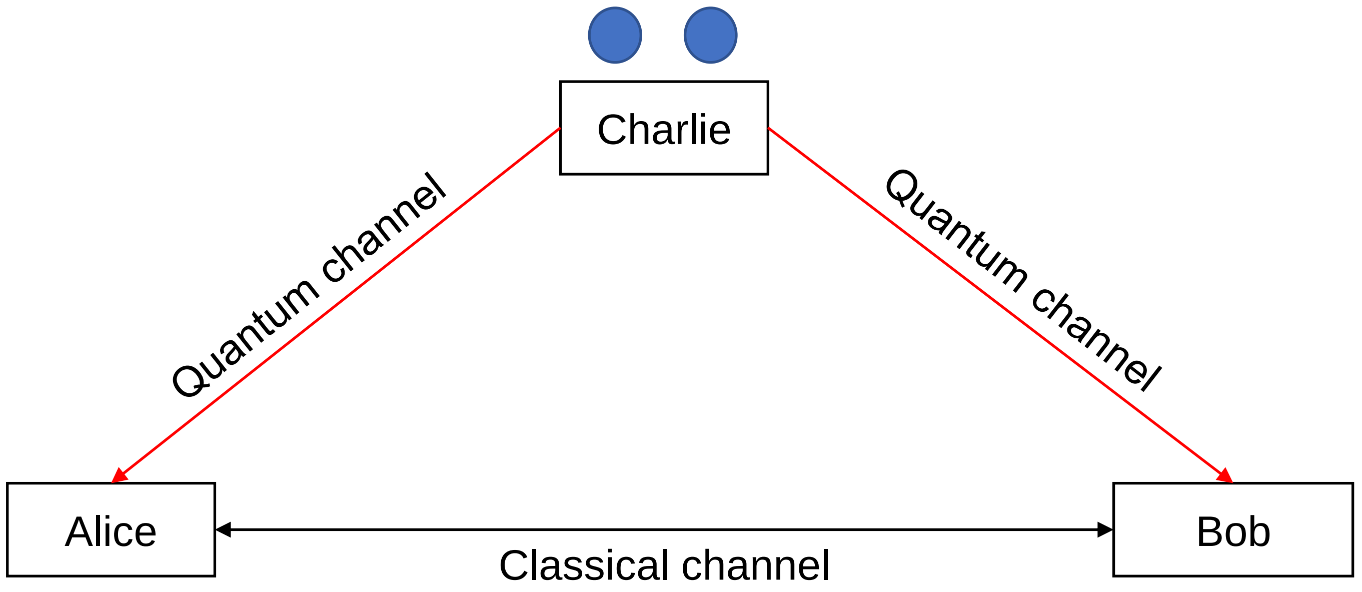
- The state if $|1_A\rangle$ is measured

$$|\psi\rangle_{new} = |1_A 0_B\rangle = |1_A\rangle|0_B\rangle$$

$\rightarrow$ The state of the qubit B is $|0_B\rangle$

BBM92 Protocol

$$|\psi\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}}$$



Basic setting of the BBM92 protocol (Alice, Bob: legitimate parties, Charlie: entangled photon pair source)

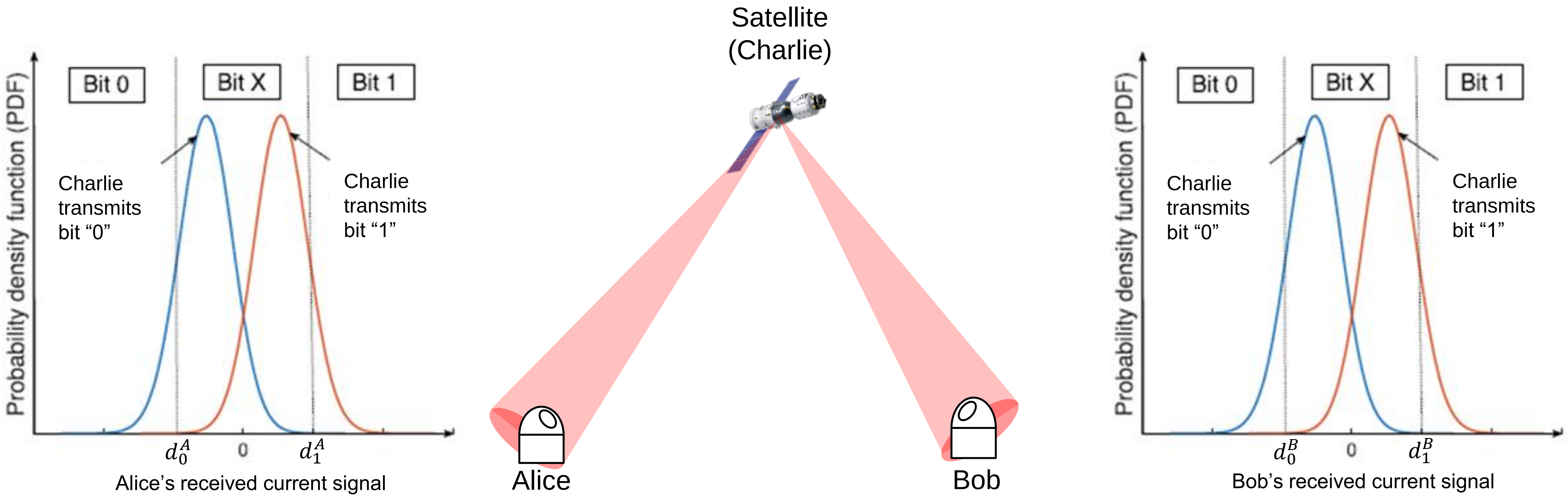
BBM92 Protocol: Example

Charlie		Alice				Bob				Sifted key
Time	Entangled photon pairs state	Time	Basis	Measured state	Bit	Time	Basis	Measured state	Bit (inverted)	
t_0	$1/\sqrt{2}(\|01\rangle + \|10\rangle)$	t_0	$\oplus$	$0°$	0	t_0	$\oplus$	$90°$	0	0
t_1	$1/\sqrt{2}(\|01\rangle + \|10\rangle)$	t_1	$\oplus$	$0°$	–	t_1	$\otimes$	$45°$	–	*discarded*
t_2	$1/\sqrt{2}(\|01\rangle + \|10\rangle)$	t_2	$\otimes$	$45°$	1	t_2	$\otimes$	$-45°$	1	1
t_3	$1/\sqrt{2}(\|01\rangle + \|10\rangle)$	t_3	$\otimes$	$-45°$	–	t_3	$\oplus$	$90°$	–	*discarded*

Thank you for your listening

BBM92 Protocol with Dual-threshold/Direct Detection

- We propose a new design concept for satellite CV-QKD for the entanglement-based scheme based on the BBM92 protocol with DT/DD receiver
- Motivation: To achieve QKD function with simple configuration and overcome the challenging issue of CV-QKD



Example

Satellite (Charlie)			Alice			Bob			Sifted key
Time	Bit	Signal	Time	Threshold	Bit	Time	Threshold	Bit	
t_0	0	i_0	t_0	d_0^A	0	t_0	d_0^B	X	*discarded*
t_2	1	i_1	t_2	d_1^A	X	t_2	d_1^B	X	*discarded*
t_3	0	i_0	t_3	d_0^A	0	t_3	d_0^B	0	0
t_4	1	i_1	t_4	d_1^A	1	t_4	d_1^B	1	1
t_5	0	i_0	t_5	d_0^A	X	t_5	d_0^B	0	*discarded*

BBM92 Protocol (2)

- Alice and Bob convert remaining results by assigning them for bit “0” and bit “1” to form *sifted key* as follows:

Bit 0	Bit 1
$(0°)$	$(90°)$
$(-45°)$	$(45°)$

- The photon pairs are (anti-correlated) entangled, Bob needs to invert his detected bits so that he and Alice could get an identical bit string

- **Step 4:** Alice and Bob perform post-processing procedures including *information reconciliation* and *privacy amplification* over classical channel to correct transmission errors and produce the *final secret key*