Quantum Key Distribution

Spyros Tserkis

Researcher

stserkis@tuc.gr

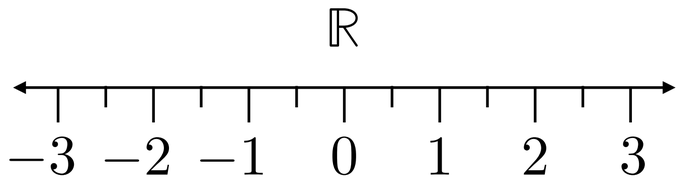
May 20, 2025

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
TECHNICAL UNIVERSITY OF CRETE

Preliminaries

Classical vs Quantum Properties

- A **physical property** is assumed to be a **real-valued scalar**



- A **classical property** can be measured without disturbing another one. Mathematically, this is implied by the **commutativity** of scalar values:

$$a \cdot b = b \cdot a$$

- A **quantum property** when measured does disturb the measurement outcomes of other properties. For that reason we need to represent the quantum properties with a mathematical object that **in general does not satisfy commutativity**, so a matrix:

$$A \cdot B \neq B \cdot A$$

Classical vs Quantum Properties

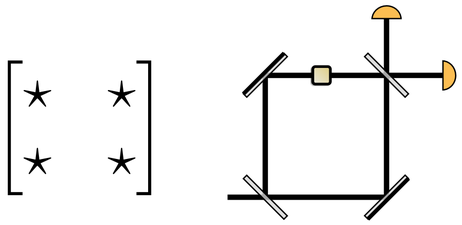
- The **measured values** of quantum properties are the **eigenvalues** of their corresponding matrices, also called observables

- Since physical properties need to be real values, **quantum properties** are represented by **Hermitian matrices** that have real eigenvalues

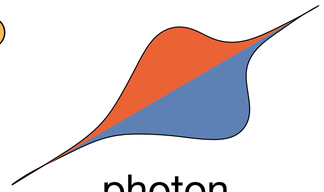
- **Diagonal matrices commute**, so the measured values of classical properties can be represented by the eigenvalues of diagonal matrices

Examples of Quantum Properties

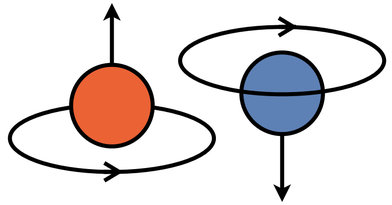
- Property with **two** possible values



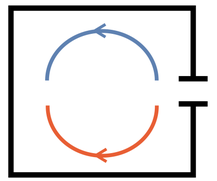
photon detection



photon polarization

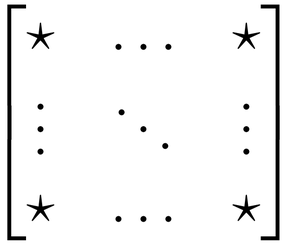


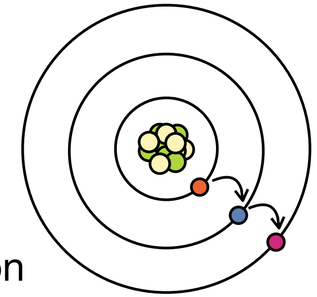
electron spin



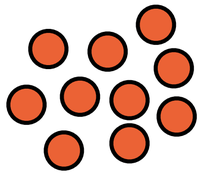
current flow

- Property with **finite** possible values



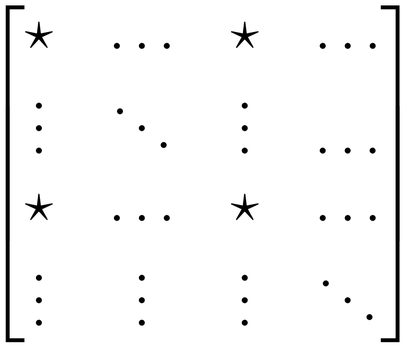


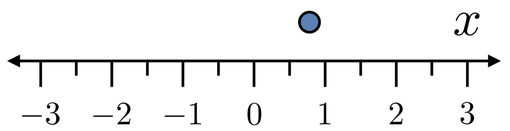
electron excitation



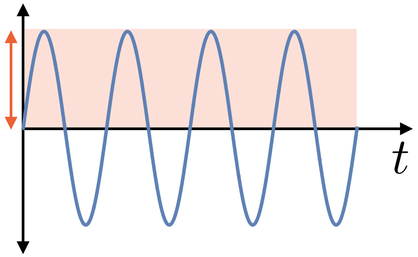
number of particles, e.g., photons

- Property with **infinite** possible values





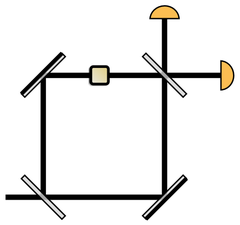
position of a particle



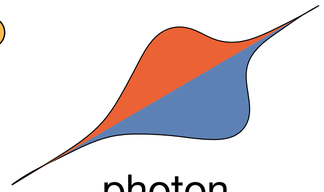
wave amplitude

The Pauli Matrices

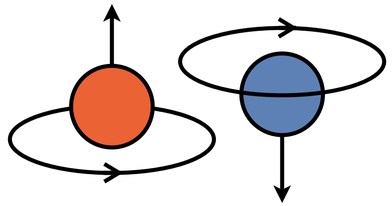
- Property with **two** possible values $\begin{bmatrix} \star & \star \\ \star & \star \end{bmatrix}$



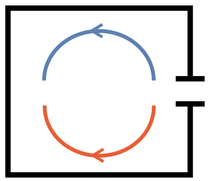
photon detection



photon polarization



electron spin



current flow

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$[X, Y]_- = XY - YX = 2\imath Z$$

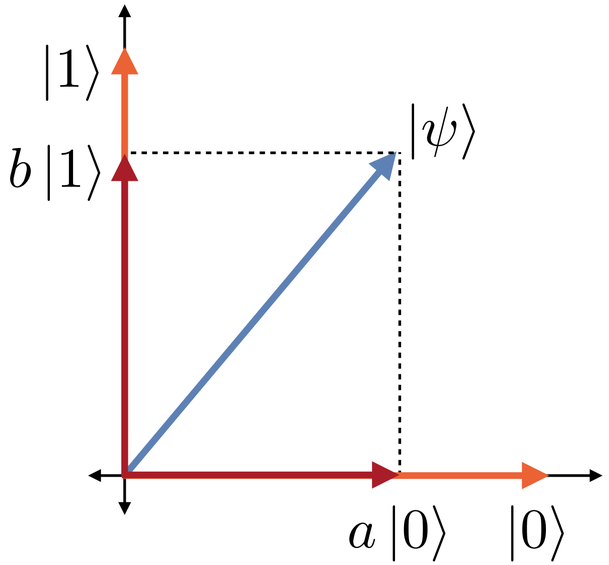
$$[Y, Z]_- = YZ - ZY = 2\imath X$$

$$[Z, X]_- = ZX - XZ = 2\imath Y$$

The Quantum State — Qubit

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \qquad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

When we measure the Pauli matrix Z we can get one of its two eigenvalues: 1 and -1, which correspond to two eigenvectors: $|0\rangle$ and $|1\rangle$



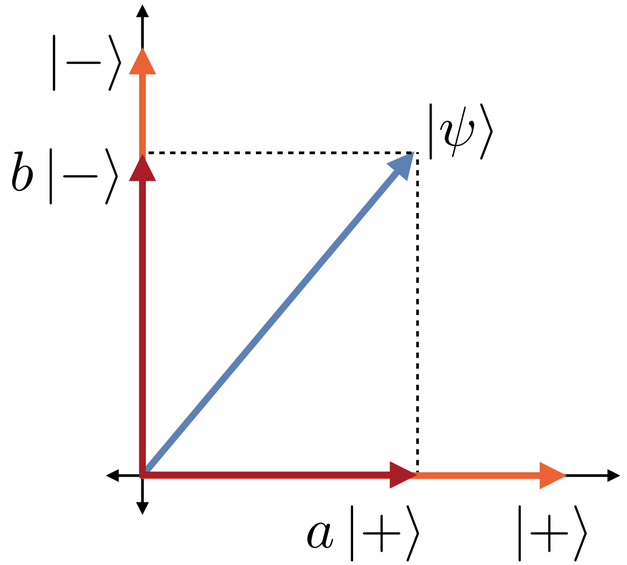
Superposition: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$

$\mathbb{P}(\lambda_0)$ $\mathbb{P}(\lambda_1)$

The Quantum State — Qubit

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} - \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = |+\rangle\langle+| - |-\rangle\langle-| \qquad |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

When we measure the Pauli matrix X we can get one of its two eigenvalues: 1 and -1, which correspond to two eigenvectors: $|+\rangle$ and $|-\rangle$



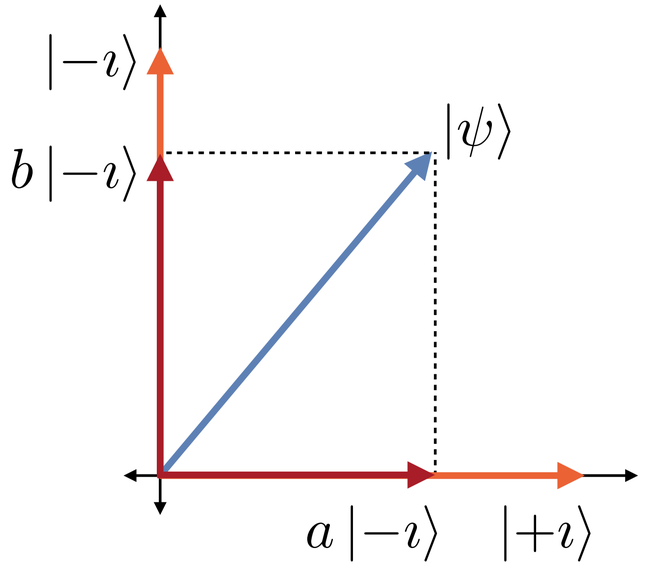
Superposition: $|\psi\rangle = a\,|+\rangle + b\,|-\rangle$

$\mathbb{P}(\lambda_+)$ $\mathbb{P}(\lambda_-)$

The Quantum State — Qubit

$$Y = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & \imath \\ -\imath & 1 \end{bmatrix} - \frac{1}{2}\begin{bmatrix} 1 & -\imath \\ \imath & 1 \end{bmatrix} = |+\imath\rangle\langle+\imath| - |-\imath\rangle\langle-\imath| \qquad |\pm\imath\rangle = \frac{|0\rangle \pm \imath\,|1\rangle}{\sqrt{2}}$$

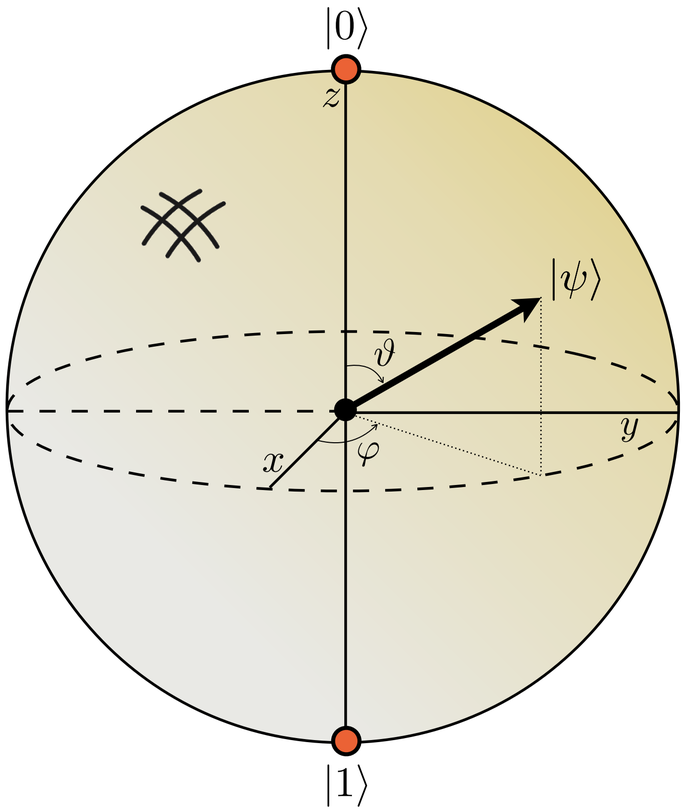
When we measure the Pauli matrix Y we can get one of its two eigenvalues: 1 and -1, which correspond to two eigenvectors: $|+\imath\rangle$ and $|-\imath\rangle$



Superposition: $|\psi\rangle = a\,|+\imath\rangle + b\,|-\imath\rangle$

$\mathbb{P}(\lambda_{+\imath})$ $\mathbb{P}(\lambda_{-\imath})$

Bloch Sphere



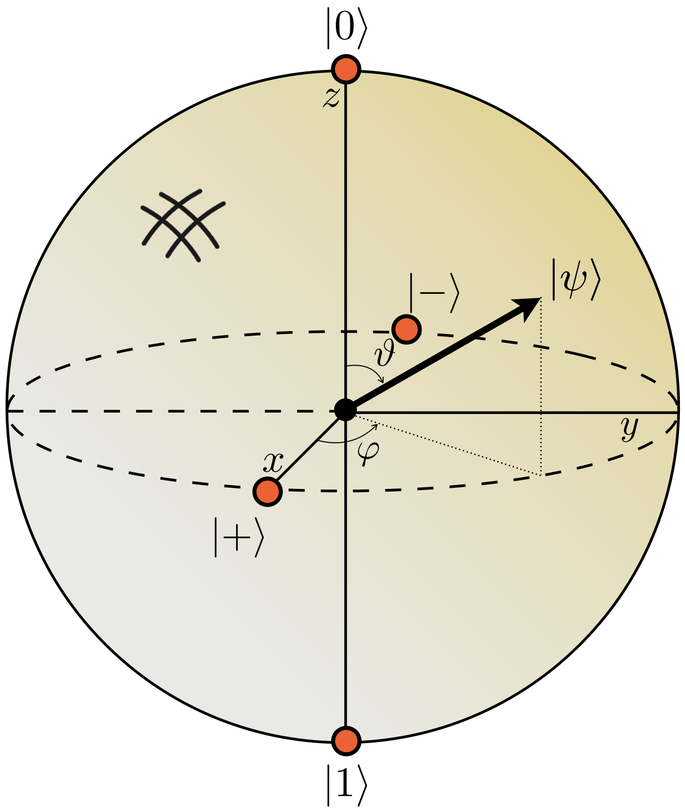
$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

Z basis: $\{|0\rangle, |1\rangle\}$ $\quad \langle 0|1\rangle = 0$

$$|0\rangle : \cos\frac{\theta}{2} = 1 \Leftrightarrow \frac{\theta}{2} = 0 \Leftrightarrow \theta = 0$$

$$|1\rangle : \cos\frac{\theta}{2} = 0 \Leftrightarrow \frac{\theta}{2} = \frac{\pi}{2} \Leftrightarrow \theta = \pi$$

Bloch Sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\imath\varphi}\sin\frac{\theta}{2}|1\rangle$$

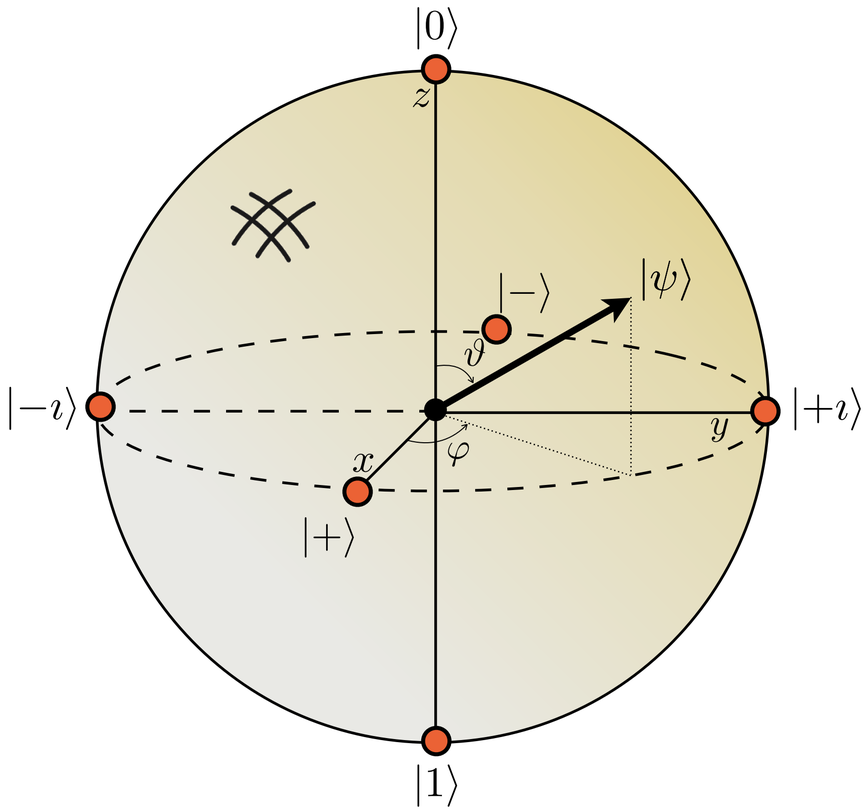
Z basis: $\{|0\rangle, |1\rangle\}$ $\quad \langle 0|1\rangle = 0$

X basis: $\{|+\rangle, |-\rangle\}$ $\quad \langle +|-\rangle = 0$ $\quad |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$

$$|+\rangle : \cos\frac{\theta}{2} = \frac{1}{\sqrt{2}} \Leftrightarrow \frac{\theta}{2} = \frac{\pi}{4} \Leftrightarrow \theta = \frac{\pi}{2}$$

$$e^{\imath\varphi} = 1 \Leftrightarrow \varphi = 0$$

Bloch Sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\imath\varphi}\sin\frac{\theta}{2}|1\rangle$$

Z basis: $\{|0\rangle, |1\rangle\}$ $\quad \langle 0|1\rangle = 0$

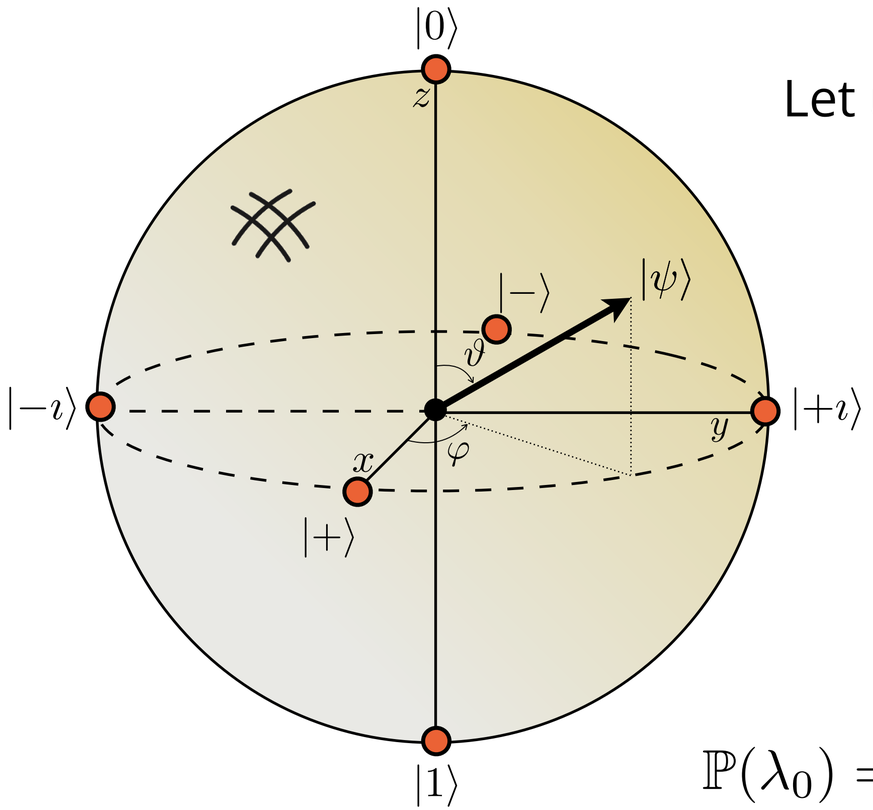
X basis: $\{|+\rangle, |-\rangle\}$ $\quad \langle +|-\rangle = 0$ $\quad |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$

Y basis: $\{|+\imath\rangle, |-\imath\rangle\}$ $\quad \langle +\imath| - \imath\rangle = 0$ $\quad |\pm\imath\rangle = \frac{|0\rangle \pm \imath|1\rangle}{\sqrt{2}}$

$$|+\imath\rangle : \cos\frac{\theta}{2} = \frac{1}{\sqrt{2}} \Leftrightarrow \frac{\theta}{2} = \frac{\pi}{4} \Leftrightarrow \theta = \frac{\pi}{2}$$

$$e^{\imath\varphi} = \imath \Leftrightarrow \varphi = \frac{\pi}{2}$$

Randomness in Measurements



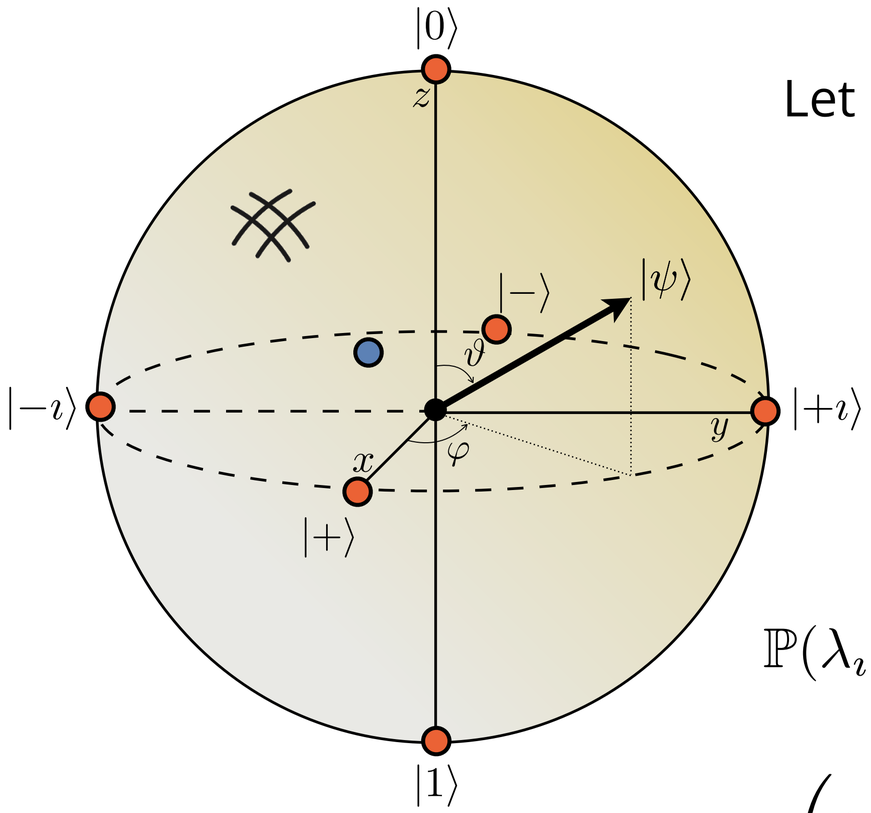
Let us have the state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$

What is the probability of measuring the eigenvalue +1 of the observable Z ?

$$\mathbb{P}(\lambda_0) = \langle\psi| \, \Pi_0 \, |\psi\rangle = \langle +|0\rangle \langle 0|+\rangle = \left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) |0\rangle \langle 0| \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

$$= \left(\frac{\langle 0|0\rangle + \langle 1|0\rangle}{\sqrt{2}}\right) \left(\frac{\langle 0|0\rangle + \langle 0|1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right) \left(\frac{1}{\sqrt{2}}\right) = \frac{1}{2}$$

Randomness in Measurements



Let us have the state $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$

What is the probability of measuring the eigenvalue +1 of the observable Y ?

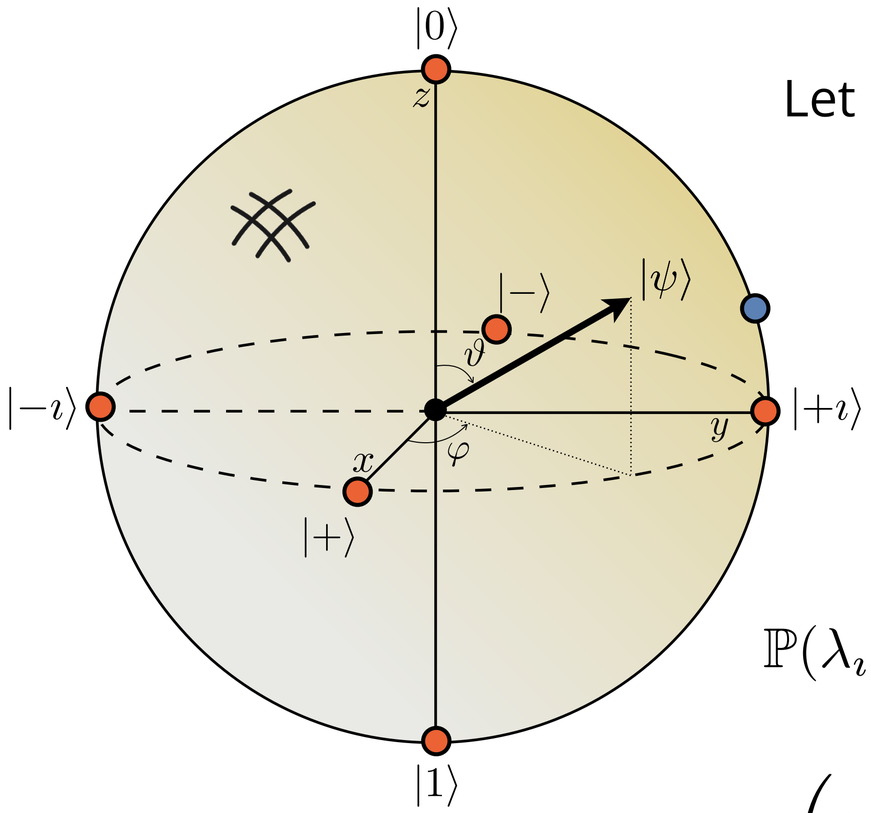
$$\mathbb{P}(\lambda_\imath) = \langle\psi|\, \Pi_\imath\, |\psi\rangle = \left(\frac{\sqrt{3}}{2}\langle 0| + \frac{1}{2}\langle 1|\right) |\imath\rangle\langle\imath| \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$= \left(\frac{\sqrt{3}}{2}\langle 0| + \frac{1}{2}\langle 1|\right) \left(\frac{|0\rangle + \imath|1\rangle}{\sqrt{2}}\right) \left(\frac{\langle 0| - \imath\langle 1|}{\sqrt{2}}\right) \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$= \left(\frac{\sqrt{3}}{2\sqrt{2}} + \frac{\imath}{2\sqrt{2}}\right) \left(\frac{\sqrt{3}}{2\sqrt{2}} - \frac{\imath}{2\sqrt{2}}\right) = \frac{3}{8} + \frac{1}{8} = \frac{1}{2}$$

$$\cos\frac{\theta}{2} = \frac{\sqrt{3}}{2} \Leftrightarrow \frac{\theta}{2} = \frac{\pi}{6} \Leftrightarrow \theta = \frac{\pi}{3}$$

Randomness in Measurements



Let us have the state $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{\imath}{2}|1\rangle$

What is the probability of measuring the eigenvalue +1 of the observable Y ?

$$\mathbb{P}(\lambda_\imath) = \langle\psi| \, \Pi_\imath \, |\psi\rangle = \left(\frac{\sqrt{3}}{2}\langle 0| - \frac{\imath}{2}\langle 1|\right) |\imath\rangle\langle\imath| \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{\imath}{2}|1\rangle\right)$$

$$= \left(\frac{\sqrt{3}}{2}\langle 0| - \frac{\imath}{2}\langle 1|\right) \left(\frac{|0\rangle + \imath|1\rangle}{\sqrt{2}}\right) \left(\frac{\langle 0| - \imath\langle 1|}{\sqrt{2}}\right) \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{\imath}{2}|1\rangle\right)$$

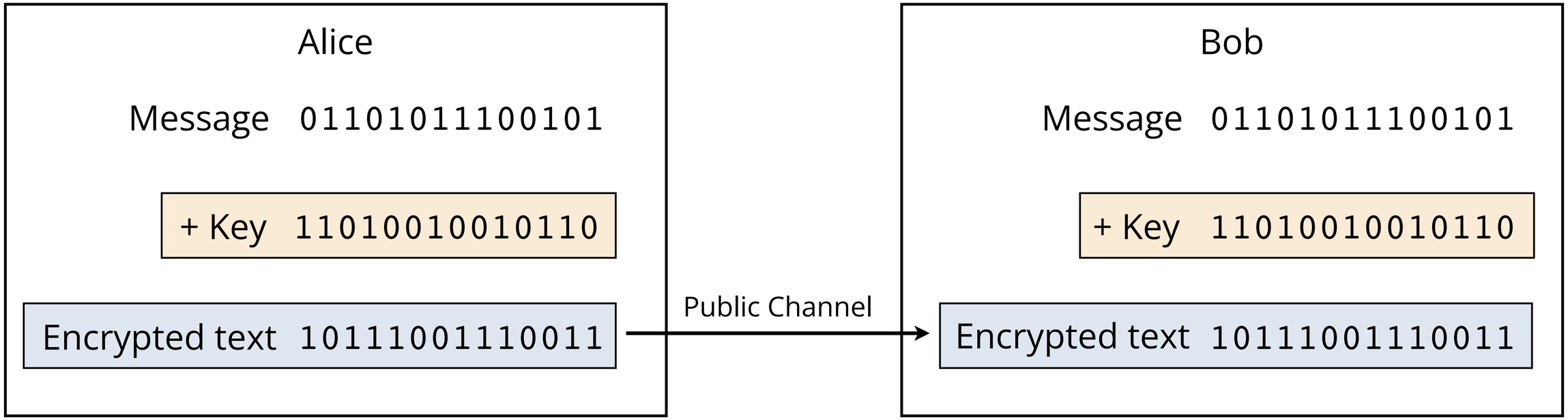
$$= \left(\frac{\sqrt{3}}{2\sqrt{2}} + \frac{1}{2\sqrt{2}}\right) \left(\frac{\sqrt{3}}{2\sqrt{2}} + \frac{1}{2\sqrt{2}}\right) = \frac{3}{8} + \frac{1}{8} + \frac{\sqrt{3}}{4} \approx 0.933$$

$$\cos\frac{\theta}{2} = \frac{\sqrt{3}}{2} \Leftrightarrow \frac{\theta}{2} = \frac{\pi}{6} \Leftrightarrow \theta = \frac{\pi}{3}$$

$$e^{\imath\varphi} = \imath \Leftrightarrow \varphi = \frac{\pi}{2}$$

Protocol BB84

Classical Cryptography



Secure communication if the key is:

- the same size as the message ✓
- used only once ✓
- random ✓
- securely distributed ? Quantum Key Distribution

Alice Randomizes Bits

Alice flips a coin to determine a random bit, 0 or 1.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice’s random bit	0	1	1	0	1	1	1	0	1	0

Alice Randomizes Bases

Alice flips a coin to determine a random basis, Z or X.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice’s random bit	0	1	1	0	1	1	1	0	1	0
Alice’s random base	Z	Z	X	Z	Z	Z	X	Z	X	X

Alice Sends States

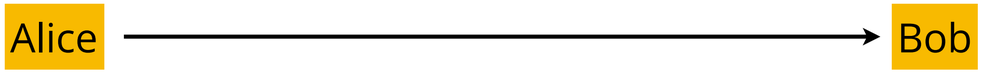
Alice 

Using the mapping:

Bit-Base	Z	X
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$

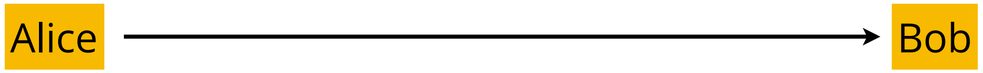
Bob Randomizes Bases



Bob flips a coin to determine a random basis, Z or X.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X

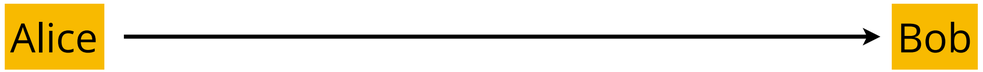
Bob Observes States



Bob's states collapse.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X
Bob observes	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$

Bob Creates a Bit-String

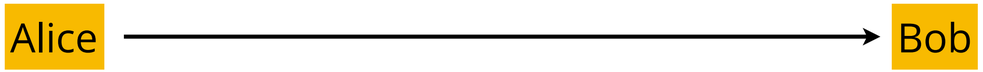


Using the mapping:

Bit-Base	Z	X
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X
Bob observes	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's bits	0	1	1	1	1	0	1	0	1	0

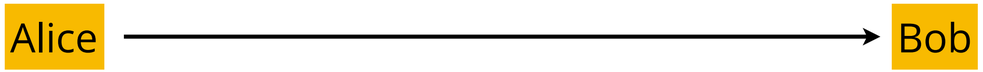
Alice and Bob Communicate



Around half of the bits will be discarded because they measured in different bases.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X
Bob observes	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's bits	0	1	1	1	1	0	1	0	1	0

Alice and Bob Communicate



Around half of the bits will be discarded because they measured in different bases.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's bits		1	1		1			0	1	0

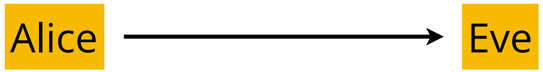
Alice and Bob Create a Secret Key

Alice → Bob

Alice and Bob create an encrypted bit-string.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bob's bits		1	1		1			0	1	0

There is an Eavesdropper at the System



Eve will act as if she was Bob for Alice

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z

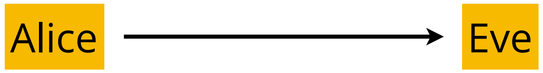
Eve observes states

Alice → Eve

Eve's states collapse.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z
Eve observes/sends	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$

Eve Creates a Bit-String



Using the mapping:

Bit-Base	Z	X
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z
Eve observes/sends	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits	0	0	1	1	1	0	0	0	1	1

Bob Randomized Bases

Bob flips a coin to determine a random basis, Z or X.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z
Eve observes/sends	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits	0	0	1	1	1	0	0	0	1	1
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X

Bob Observes States

Bob's states collapse.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z
Eve observes/sends	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits	0	0	1	1	1	0	0	0	1	1
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X
Bob observes	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$

Bob Creates a Bit-String

Using the mapping:

Bit-Base	Z	X
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z
Eve observes/sends	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits	0	0	1	1	1	0	0	0	1	1
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X
Bob observes	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits	0	0	1	1	1	0	1	1	1	1

Detecting Eavesdropping

Alice and Bob compare bases halving the bit-string.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit	0	1	1	0	1	1	1	0	1	0
Alice's random base	Z	Z	X	Z	Z	Z	X	Z	X	X
Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base	Z	X	X	X	Z	X	Z	X	X	Z
Eve observes/sends	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits	0	0	1	1	1	0	0	0	1	1
Bob's random base	X	Z	X	X	Z	X	Z	Z	X	X
Bob observes	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits	0	0	1	1	1	0	1	1	1	1

Detecting Eavesdropping

Alice and Bob compare bases halving the bit-string.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base		X	X		Z			X	X	Z
Eve observes/sends		$\|+\rangle$	$\|-\rangle$		$\|1\rangle$			$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits		0	1		1			0	1	1
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|0\rangle$	$\|-\rangle$		$\|1\rangle$			$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits		0	1		1			1	1	1

Detecting Eavesdropping

Alice and Bob compare half of the remaining bits to detect Eve's presence.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base		X	X		Z			X	X	Z
Eve observes/sends		$\|+\rangle$	$\|-\rangle$		$\|1\rangle$			$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits		0	1		1			0	1	1
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|0\rangle$	$\|-\rangle$		$\|1\rangle$			$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits		0	1		1			1	1	1

Detecting Eavesdropping

Alice and Bob compare half of the remaining bits to detect Eve's presence.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base		X	X		Z			X	X	Z
Eve observes/sends		$\|+\rangle$	$\|-\rangle$		$\|1\rangle$			$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits		0	1		1			0	1	1
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|0\rangle$	$\|-\rangle$		$\|1\rangle$			$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits		0	1		1			1	1	1

Detecting Eavesdropping

Alice and Bob compare half of the remaining bits to detect Eve's presence.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base		X	X		Z			X	X	Z
Eve observes/sends		$\|+\rangle$	$\|-\rangle$		$\|1\rangle$			$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits		0	1		1			0	1	1
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|0\rangle$	$\|-\rangle$		$\|1\rangle$			$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits		0	1		1			1	1	1

Alice and Bob Create a Secret Key

Alice and Bob create an encrypted bit-string.

Bit index	1	2	3	4	5	6	7	8	9	10
Alice's random bit		1	1		1			0	1	0
Alice's random base		Z	X		Z			Z	X	X
Alice sends		$\|1\rangle$	$\|-\rangle$		$\|1\rangle$			$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Eve's random base		X	X		Z			X	X	Z
Eve observes/sends		$\|+\rangle$	$\|-\rangle$		$\|1\rangle$			$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Eve's bits		0	1		1			0	1	1
Bob's random base		Z	X		Z			Z	X	X
Bob observes		$\|0\rangle$	$\|-\rangle$		$\|1\rangle$			$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob's bits		0	1		1			1	1	1

QKD — Summary

- Quantum cryptography offers advantage in key distribution
- An eavesdropper cannot copy Alice's state due to no-cloning theorem
- Alice and Bob sacrifice half of their bits to align their bases
- Alice and Bob sacrifice half of their remaining bits to detect Eve
- Eve's detection happens probabilistically

Entanglement

Composite Systems — Entanglement

Composite states: $|\psi\rangle^{(1)} = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0 |0\rangle + c_1 |1\rangle$ $\quad$ $|\psi\rangle^{(2)} = \begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = d_0 |0\rangle + d_1 |1\rangle$

$$|\Psi\rangle = |\psi\rangle^{(1)} \otimes |\psi\rangle^{(2)} = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} \otimes \begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = \begin{bmatrix} c_0 \begin{bmatrix} d_0 \\ d_1 \end{bmatrix} \\ c_1 \begin{bmatrix} d_0 \\ d_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} c_0 d_0 \\ c_0 d_1 \\ c_1 d_0 \\ c_1 d_1 \end{bmatrix}$$

Can we always decompose a given vector into a tensor product of vectors?

$$\begin{bmatrix} \star \\ \star \end{bmatrix} \otimes \begin{bmatrix} \star \\ \star \end{bmatrix} \xleftarrow{?} \begin{bmatrix} \star \\ \star \\ \star \\ \star \end{bmatrix}$$

Answer: No!

(Bell state) $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

convention

$$|ij\rangle = |i\rangle \otimes |j\rangle$$

How Do We Detect Entanglement?

Schmidt Decomposition. Any bi-partite state $|\psi\rangle = \sum_{i}^{2}\sum_{j}^{2} c_{ij}\,|i\rangle \otimes |j\rangle$ with $c_{ij} \in \mathbb{C}$ and $\{|i\rangle\}, \{|j\rangle\}$ being orthonormal bases, can be re-written as

$$|\psi\rangle = \sum_{k}^{2} s_k\,|e_k\rangle \otimes |h_k\rangle$$

with real coefficients $s_i \in \mathbb{R}$ and orthonormal bases $\{|e_i\rangle\}, \{|h_i\rangle\}$

A quantum state is entangled if and only if there are two non-zero Schmidt coefficients.

Schmidt Decomposition — Proof

$$|\psi\rangle = \sum_i^2 \sum_j^2 c_{ij} \, |i\rangle \otimes |j\rangle \; = \sum_i^2 \sum_j^2 \sum_k^2 \overbrace{u_{ik} \cdot s_k \cdot v_{jk}^*}^{\substack{\text{singular} \\ \text{value} \\ \text{decomposition}}} \, |i\rangle \otimes |j\rangle$$

$$C = \begin{bmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{bmatrix}$$

$$= \overbrace{\begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}}^{U} \cdot \overbrace{\begin{bmatrix} s_0 & 0 \\ 0 & s_1 \end{bmatrix}}^{S} \cdot \overbrace{\begin{bmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{bmatrix}^\dagger}^{V^\dagger}$$

eigenvectors of $CC^\dagger$

eigenvectors of $C^\dagger C$

square root of the eigenvalues of $CC^\dagger$ or $C^\dagger C$

$$= \sum_k^2 s_k \overbrace{\left[\sum_i^2 u_{ik} \, |i\rangle \right]}^{|e_k\rangle} \otimes \overbrace{\left[\sum_j^2 v_{jk}^* \, |j\rangle \right]}^{|h_k\rangle}$$

$$= \sum_k^2 s_k \, |e_k\rangle \otimes |h_k\rangle$$

Schmidt Decomposition — Examples

$$|\psi\rangle = |1\rangle \otimes |1\rangle$$

$$= \boxed{0} \cdot |0\rangle \otimes |0\rangle + \boxed{1} \cdot |1\rangle \otimes |1\rangle$$

$$|\psi\rangle = \frac{1}{2}|0\rangle \otimes |0\rangle - \frac{1}{2}|0\rangle \otimes |1\rangle - \frac{1}{2}|1\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |1\rangle$$

$$= \boxed{0} \cdot |+\rangle \otimes |+\rangle + \boxed{1} \cdot |-\rangle \otimes |-\rangle$$

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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|\psi\rangle = \frac{1+\sqrt{6}}{2\sqrt{6}}|0\rangle \otimes |0\rangle + \frac{1-\sqrt{6}}{2\sqrt{6}}|0\rangle \otimes |1\rangle + \frac{\sqrt{2}-\sqrt{3}}{2\sqrt{6}}|1\rangle \otimes |0\rangle + \frac{\sqrt{2}+\sqrt{3}}{2\sqrt{6}}|1\rangle \otimes |1\rangle$$

$$= \boxed{\frac{1}{2}} \cdot |e_0\rangle \otimes |h_0\rangle + \boxed{\frac{\sqrt{3}}{2}} \cdot |e_1\rangle \otimes |h_1\rangle$$

$$|e_0\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle \qquad |h_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|e_1\rangle = \frac{\sqrt{2}}{\sqrt{3}}|0\rangle - \frac{1}{\sqrt{3}}|1\rangle \qquad |h_1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Entanglement in Different Bases

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle)$$

$$= \frac{1}{\sqrt{2}}(|i\rangle \otimes |i\rangle + |-i\rangle \otimes |-i\rangle)$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|i\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} \qquad |-i\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}$$