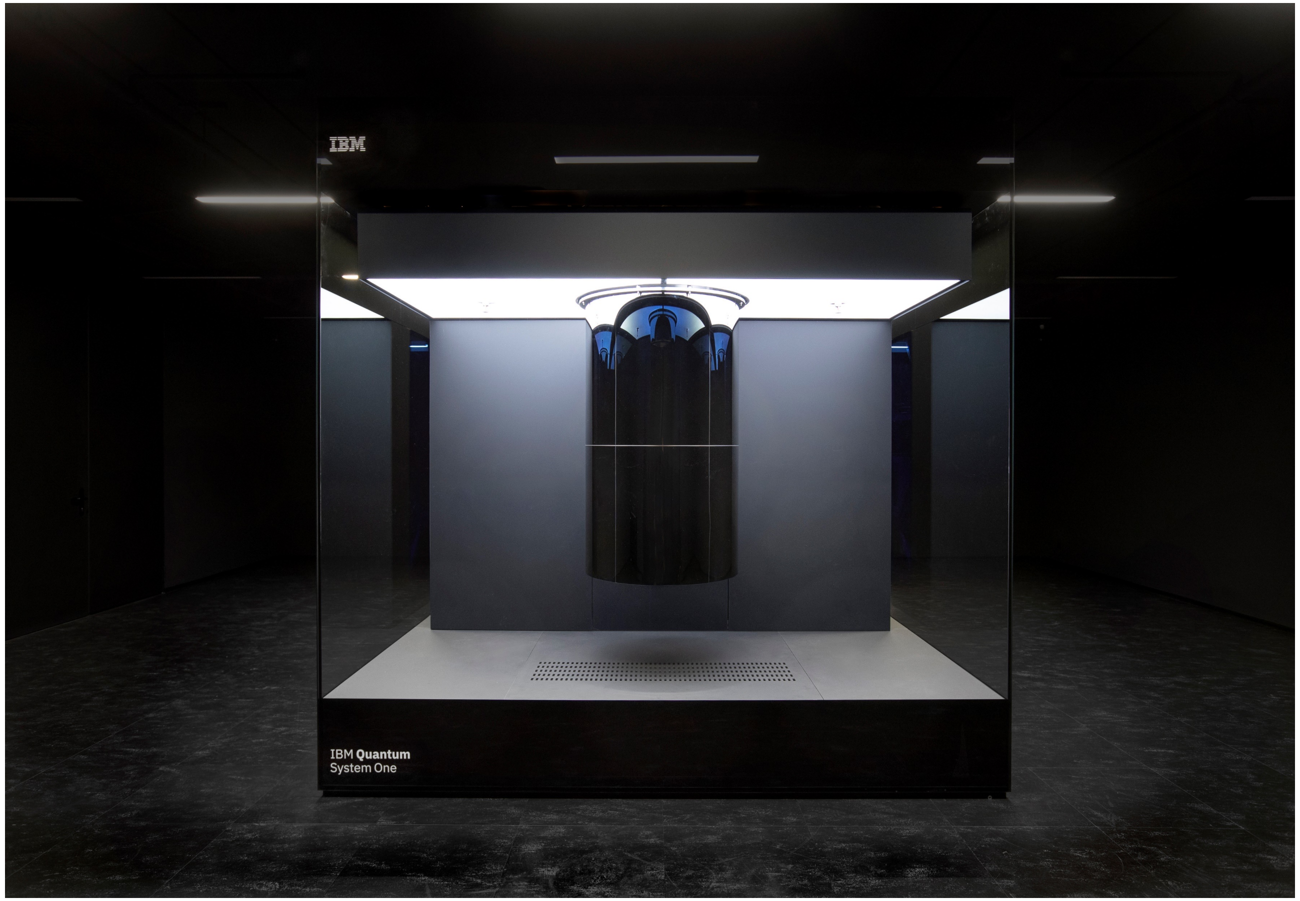
量子计算
Quantum Computing

武亦文 5.5

什么是量子计算?
What is Quantum Computing?

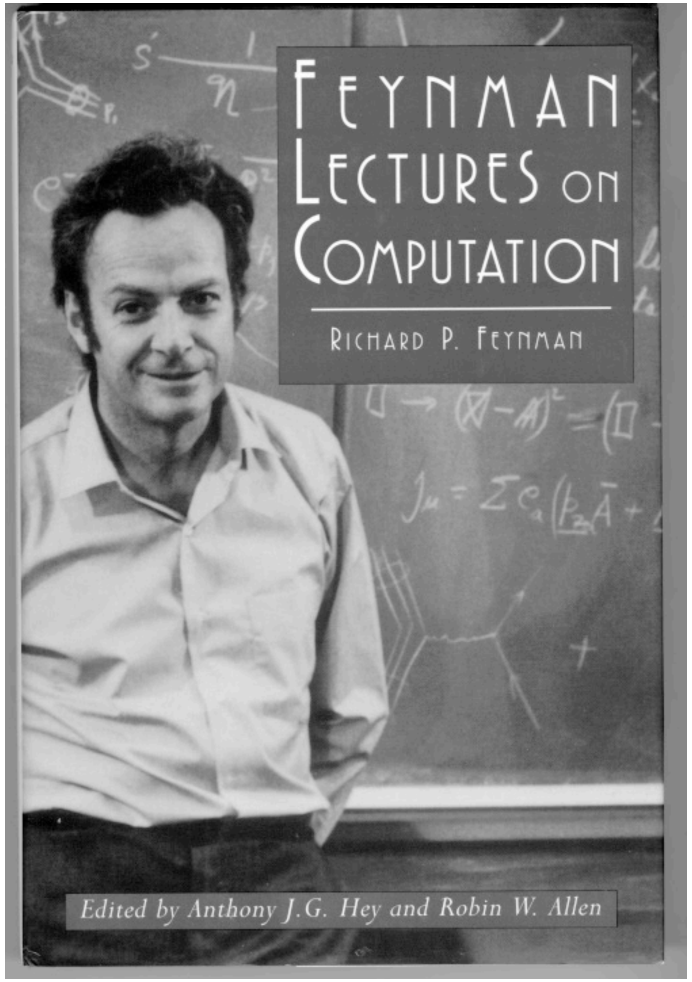
From WIKI

Quantum computing is a type of computation that harnesses the collective properties of quantum states, such as **superposition**, **interference**, and **entanglement**, to perform calculations.



IBM Quantum System One (20qbits)

为什么要量子计算?
Why Quantum Computing?



"**Nature isn't classical**, dammit, and if you want to make a simulation of Nature, **you'd better make it quantum mechanical**, and by golly it's a wonderful problem because it doesn't look so easy."

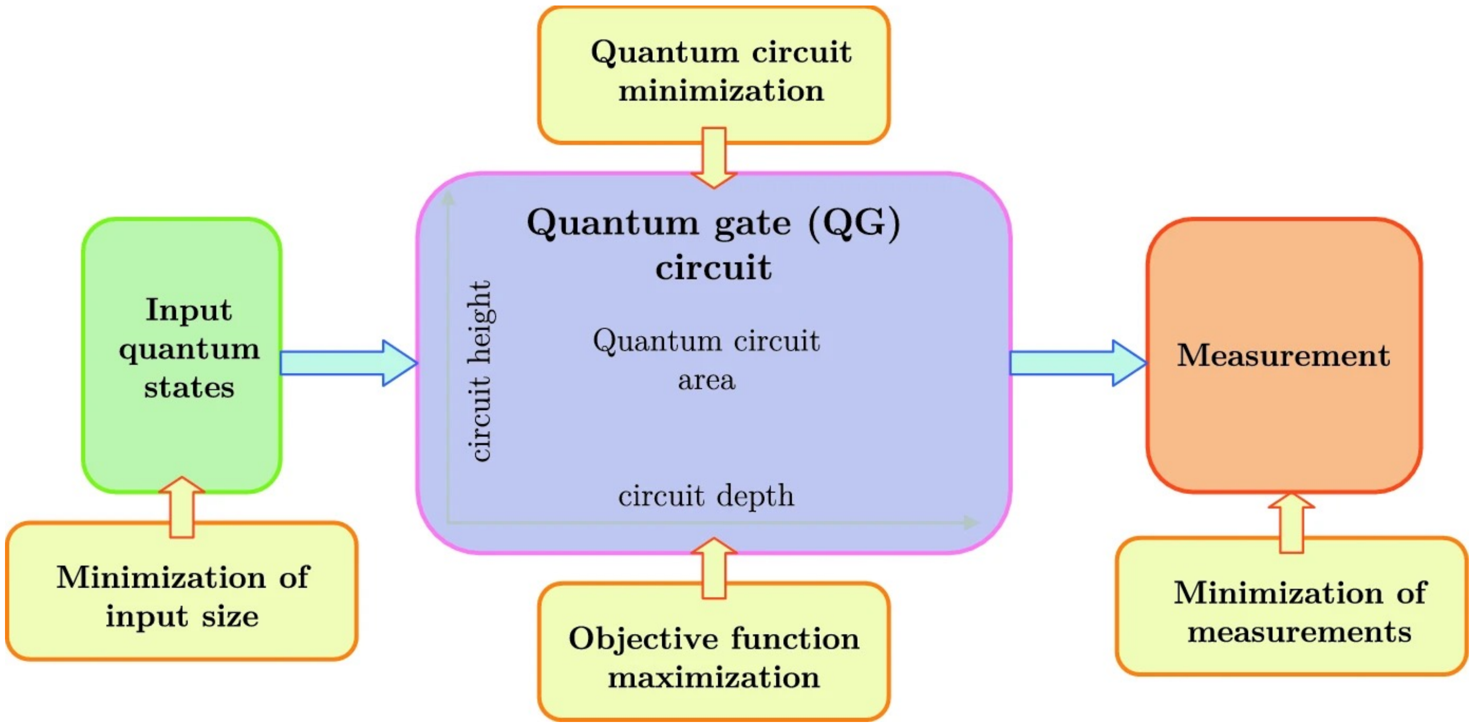
R. P. Feynman, 1981

量子计算机
Quantum Computer

The devices that perform quantum computations are known as **quantum computers**.

There are several types of quantum computers, including the **quantum circuit model**, quantum Turing machine, adiabatic quantum computer, one-way quantum computer, and various quantum cellular automata.

The most widely used model is the quantum circuit, based on the quantum bit, or **“qubit”.**



量子计算
Quantum computing

软件
software

硬件
hardware

量子算法
Quantum algorithm

大数因子分解
比经典算法复杂度低

难点：实际硬件不精确
需要纠错

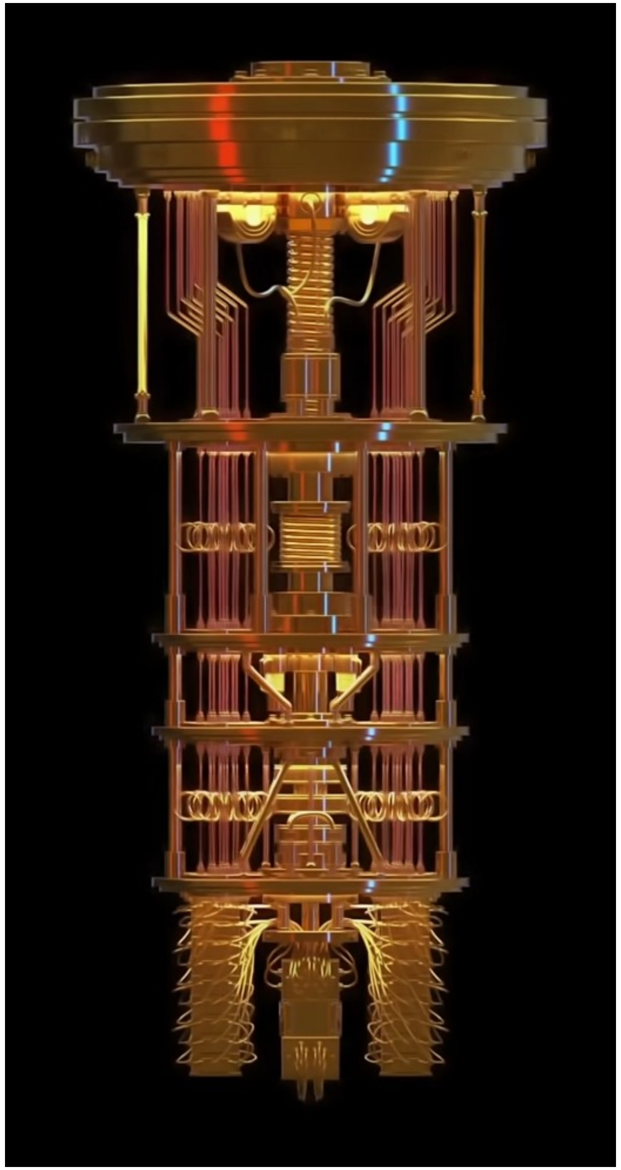
量子电路
Quantum circuit

量子门
对量子比特进行操作

难点：让量子比特相互作用
并且不跟环境作用

量子比特
Qubit

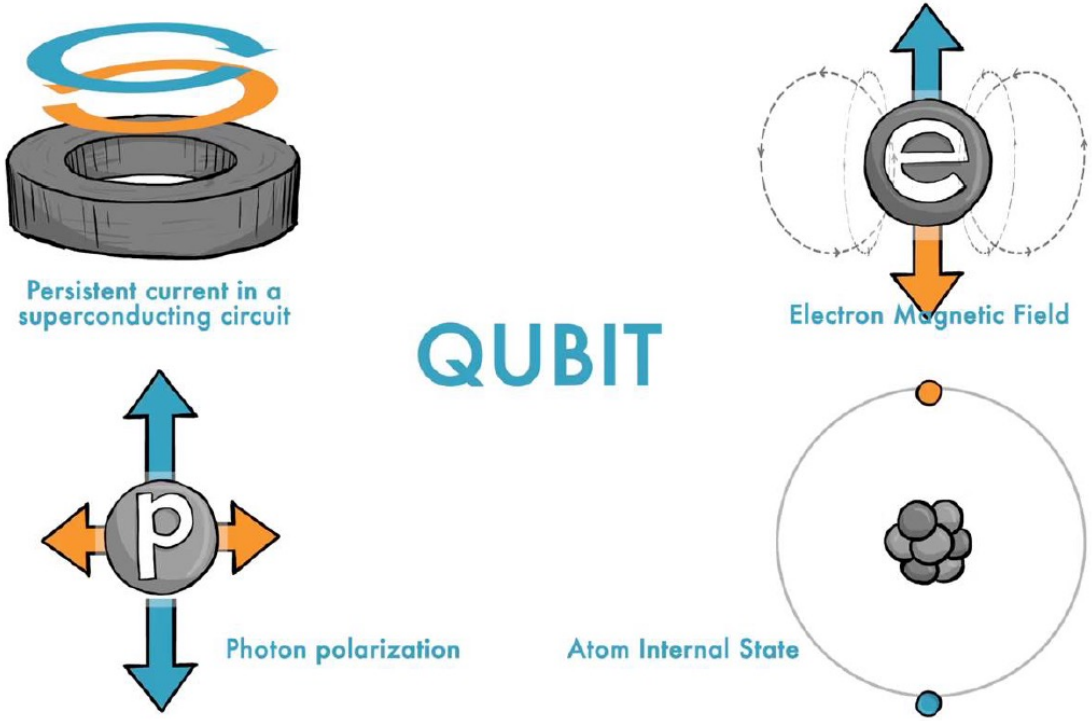
制备，存储
测量，传输



IBM 2021 （127qbit）

量子比特的制备
Qubit

0和1用量子态来实现



量子比特的测量
Measurement

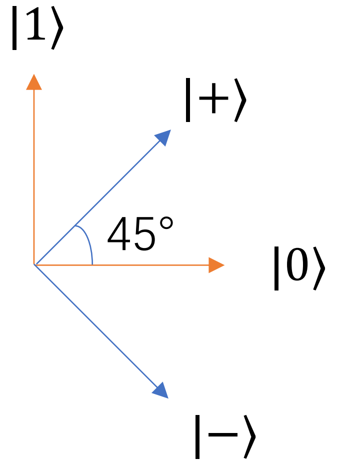
力学量 / 算符 / 矩阵 —测量结果→ 本征值 —对应→ 本征态 / 波函数 / 向量 —叠加→ 量子态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

量子态 —测量后塌缩→ 本征态

力学量 $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	本征值 1, -1 本征态 $\|0\rangle$, $\|1\rangle$	$\rightarrow$ 称为用 $\{\|0\rangle, \|1\rangle\}$ 基测量
力学量 $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	本征值 1, -1 本征态 $\|+\rangle$, $\|-\rangle$	$\rightarrow$ 称为用 $\{\|+\rangle, \|-\rangle\}$ 基测量

态叠加原理带来的特性——信息安全

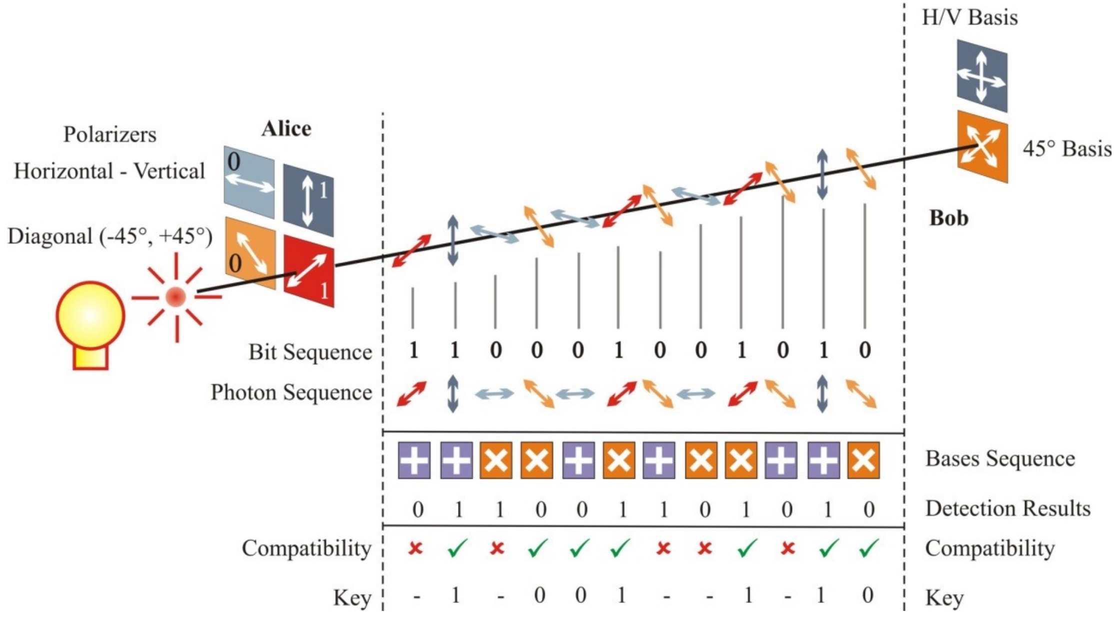
superposition principle



$$|+\rangle = 1/\sqrt{2}\,(|0\rangle + \beta|1\rangle)$$

$$|-\rangle = 1/\sqrt{2}\,(|0\rangle - \beta|1\rangle)$$

量子密钥分发 BB84协议



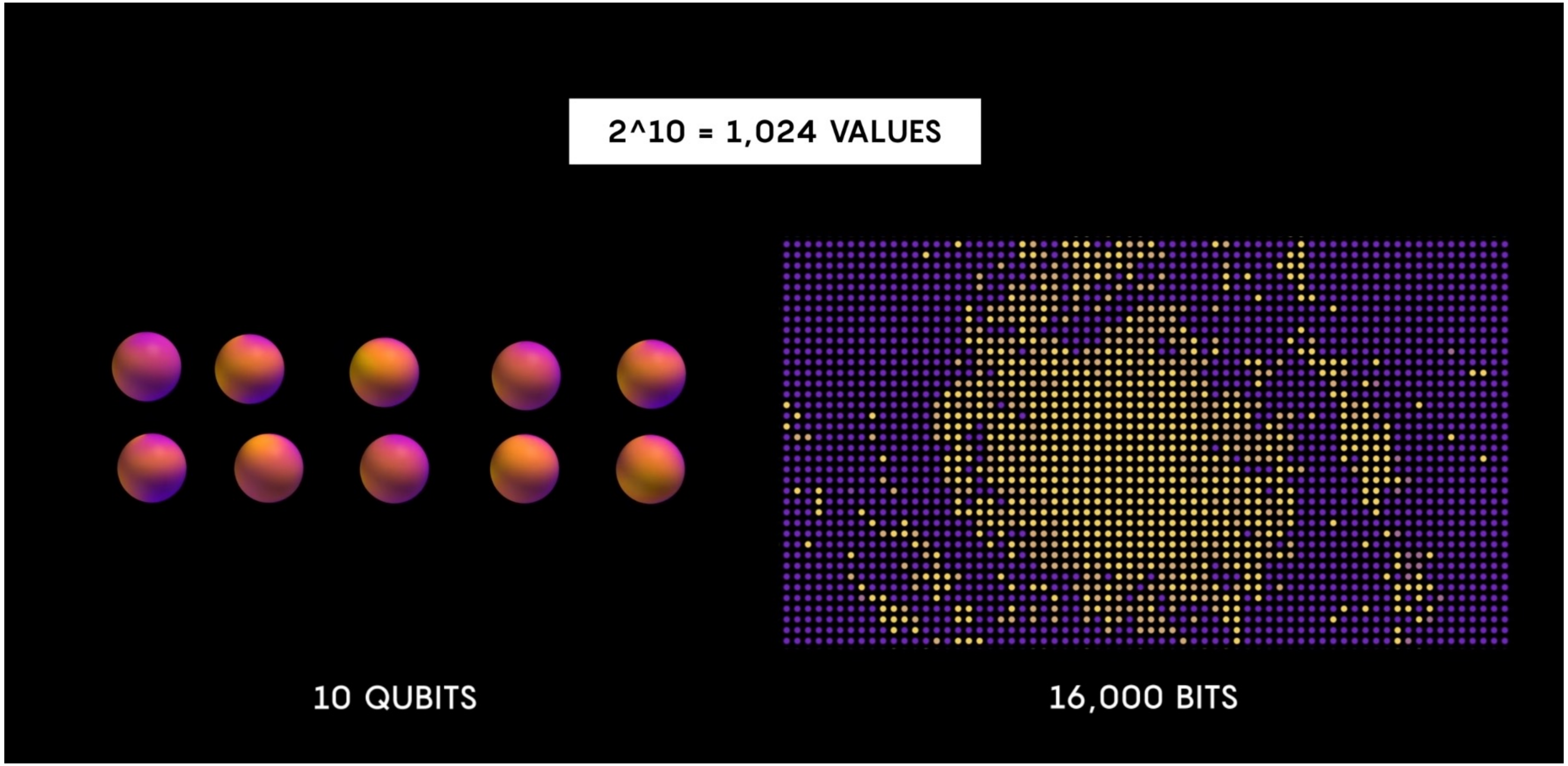
对未知态的测量会改变其量子态

每次窃听被发现的概率=25%

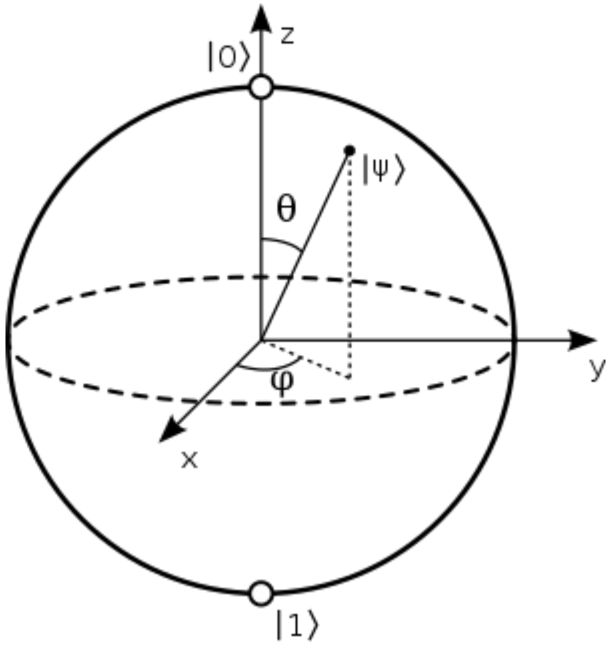
无窃听——误码率=0%
有窃听——误码率>0%

态叠加原理带来的特性——数据存储
superposition principle

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



量子比特的表示——Bloch Sphere Representation



Single qubit states that are not entangled and lack global phase can be represented as **points on the surface of the Bloch sphere**, written as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

量子逻辑门
Quantum logic gate

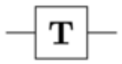
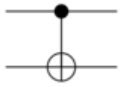
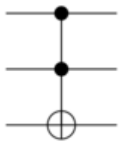
Quantum logic gates are represented by **unitary matrices**.

Identity gate $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$ $I \coloneqq \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ $I|0\rangle = |0\rangle$ $I|1\rangle = |1\rangle$

NOT gate $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$ $X \coloneqq \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ $X|0\rangle = |1\rangle$ $X|1\rangle = |0\rangle$

CNOT gate $|00\rangle := \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ $|01\rangle := \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$ $|10\rangle := \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$ $|11\rangle := \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$ $CNOT \coloneqq \begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{pmatrix}$

$CNOT|00\rangle = |00\rangle$
$CNOT|01\rangle = |01\rangle$
$CNOT|10\rangle = |11\rangle$
$CNOT|11\rangle = |10\rangle$

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$