Quantum Computing

Chao Liang

School of Computer Science
Wuhan University

Review: Lecture 7

1. Deutsch's algorithm
   - Deutsch's orcal problems
   - Four operations and quantum gates
   - Deutsch's algorithm
   - Discussion
2. Deutsch-Jozsa algorithm
   - Hadamard matrix and Kronecker product
   - N-bit Deutsch oracle problem
   - Deutsch-Jozsa algorithm

Lecture 8: Quantum Cryptography

1

Classic cryptography
- Basic concepts
- Symmetric cryptography
- Asymmetric cryptography

2

Quantum key exchange
- The BB84 protocol
- The B92 protocol
- The EPR protocol

3

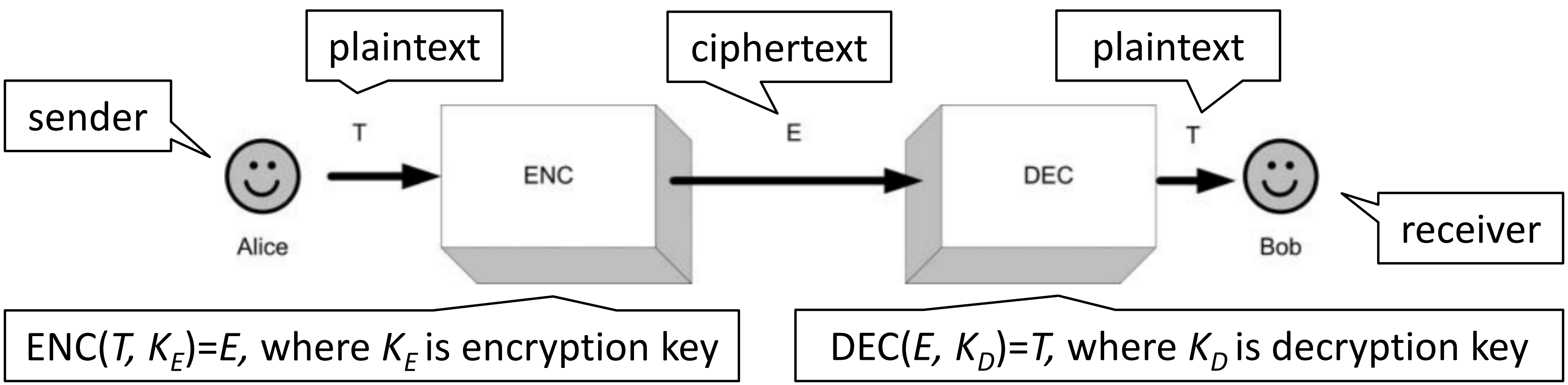
Quantum teleportation
- Definition
- Bell basis and its quantum circuit
- Quantum teleportation protocol
- 超光速通讯不可行

4

Superdense Coding
- Objective
- Inverse Bell circuit
- Superdense coding protocol

1. Classic cryptography

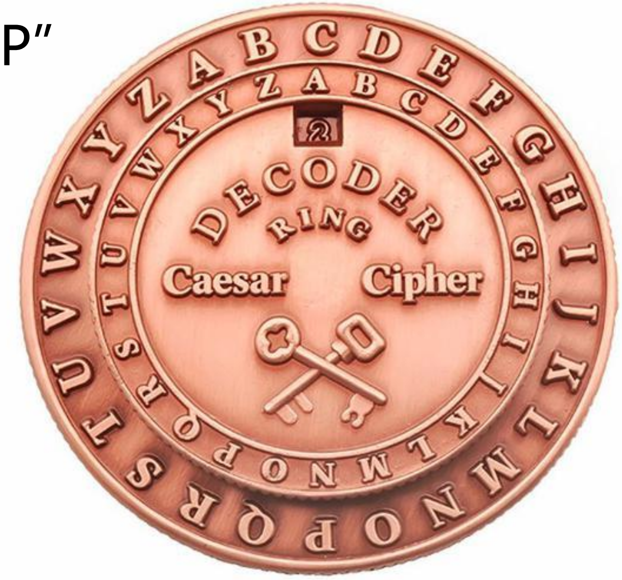
- Definition: Cryptography
  - Cryptography is the art of concealing messages.



DEC(ENC(T, K_E), K_D)=T *means that as long as we use the right keys, we can always retrieve the original message intactly without any loss of information*

1. Classic cryptography

- Examples
  - Caesar's protocol
    - ENC =DEC =shift(-, -)
    - E.g., shift(“MOM,” 3) = “PRP”
  - Weakness
    - high statistical correlation



Source: http://www.veryhuo.com/a/view/205069.html

1. Classic cryptography

- Examples
  - One-Time-Pad protocol (一次性密码本)
    - Share the key *K*

$K_E = K_D = K$

$ENC(T,K) = DEC(T,K) = T \oplus K$

$$
\begin{aligned}
DEC(ENC(T, K), K) &= DEC(T \oplus K, K) \\
&= (T \oplus K) \oplus K \\
&= T \oplus (K \oplus K) \\
&= T
\end{aligned}
$$

One-Time-Pad Protocol

Original message T		0	1	1	0	1	1
Encryption key K	⊕	1	1	1	0	1	0
Encrypted message E		1	0	0	0	0	1
Public channel		⇓	⇓	⇓	⇓	⇓	⇓
Received message E		1	0	0	0	0	1
Decryption key K	⊕	1	1	1	0	1	0
Decrypted message T		0	1	1	0	1	1

补充材料：OTP优缺点

- 优点
  - 绝对无法破解
- 缺点
  - 密钥太长
  - 无法重用密钥（存在信息泄露的风险）
  - 密钥的配送
  - 密钥的保存

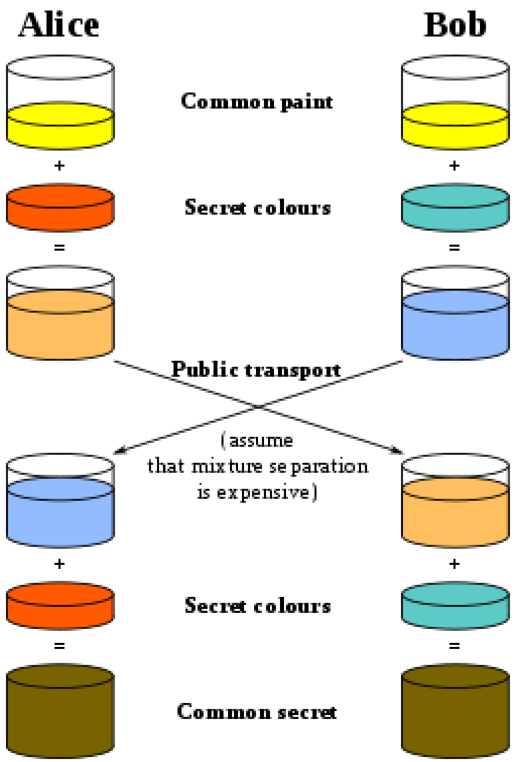
1. Classic cryptography

- Examples
  - One-Time-Pad protocol's issues
    - One time only (see Exercise 9.1.4)
      - $E_1 \oplus E_2 = (T_1 \oplus K) \oplus (T_2 \oplus K)$

        $= T_1 \oplus K \oplus K \oplus T_2$

        $= T_1 \oplus T_2$
    - Diffie-Hellman Key distribution
      - Core idea: One-way function
      - E.g., modular exponentiation:

        $g^x \bmod p$



Reference： Crash Course Computer Science 33 Cryptography, https://www.bilibili.com/video/BV1EW411u7th?p=33

补充材料：D-H 密钥交换

- **Diffie-Hellman Key Exchange**
  - Alice 选择数 a，Bob选择数 b（两人不互知）
  - 两人通过p 和 g 从各自的数字里分别算出 A 和 B，并且交换 A 和 B（注意不是交换 a 和 b）
  - Alice 就可以用 B 和 a 算出 s（秘钥），而 Bob 用 A 和 b 可以算出同样的秘钥 s
  - Eve 知道 A 和 B，但不知道 a 和 b，所以算不出 s

Reference：Diffie-Hellman Key Exchange：互联网通信背后的历史虚无主义革命，https://zhuanlan.zhihu.com/p/113072558

补充材料：D-H 密钥交换

- **Diffie-Hellman Key Exchange**

Alice		Bob		Eve	
Known	**Unknown**	**Known**	**Unknown**	**Known**	**Unknown**
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$\mathbf{a = 6}$	$\mathbf{b}$	$\mathbf{b = 15}$	$\mathbf{a}$		$\mathbf{a}, \mathbf{b}$
$A = 5^{a} \bmod 23$		$B = 5^{b} \bmod 23$			
$A = 5^{6} \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$\mathbf{B = 19}$		$\mathbf{A = 8}$		$A = 8, B = 19$	
$s = B^{a} \bmod 23$		$s = A^{b} \bmod 23$			
$s = 19^{6} \bmod 23 = \mathbf{2}$		$s = 8^{15} \bmod 23 = \mathbf{2}$			$\mathbf{s}$

Reference： Diffie-Hellman Key Exchange：
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

补充材料：D-H 密钥交换

■ Diffie-Hellman Key Exchange

- 上述做法是安全的，因为：
  - Eve 不能通过 A 和 p, g 算出 a
  - Eve 也不能通过 B 和 p, g 算出 b

$$A = g^a \mod p$$

$$B = g^b \mod p$$

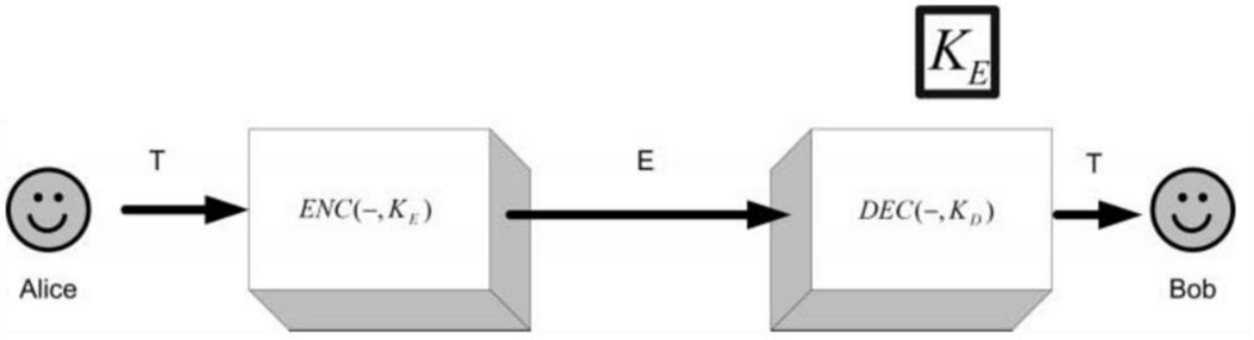
trapdoor function

如果 A, g, a 都是整数，具体地说，变成 0 到 p 之间的整数（实际操作中，通常 p 很大，比 g, a, b 都要大很多）之后，这个问题就变得很难解了。

Reference：Diffie-Hellman Key Exchange：互联网通信背后的历史虚无主义革命, https://zhuanlan.zhihu.com/p/113072558

1. Classic cryptography

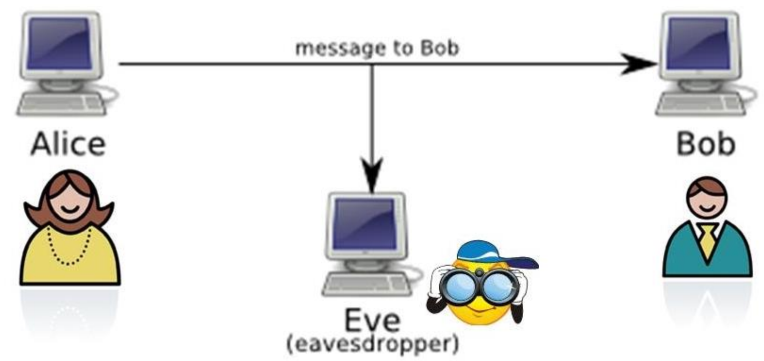
- Private-key cryptography
  - $K_E \leftarrow\rightarrow K_D$, hence K_E and K_D are both kept secret
- Public-key cryptography
  - $K_E \rightarrow K_D$ is extremely hard (trapdoor function)
  - Only K_D is kept secret, K_E is open to the public



1. Classic cryptography

- Public-key cryptography
  - Plus side
    - No key distribution problem
  - Minus sides
    - Slower than private-key cryptography
    - Temporary fact that $K_E \rightarrow K_D$ is extremely hard
      (三十年河东，三十年河西，未来也许不难)

1. Classic cryptography



- Typical issues
  - Success communication
  - Intrusion detection
    - Alice and Bob would like to determine whether Eve is, in fact, eavesdropping
  - Authentication (身份验证，认证)
    - We would like to ensure that nobody is impersonating Alice and sending false messages

参考文献:《为什么计算机科学如密码学喜欢用 Alice 和 Bob 举栗子? 》
https://www.zhihu.com/question/63306763

2. Quantum Key Ex

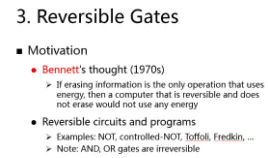
2. Observables and measuring

- Classic physics
  - the act of measuring would leave the system in whatever state it already was, at least in principle
  - the result of a measurement on a well-defined state is predictable, i.e., if we know the state with absolute certainty, we can anticipate the value of the observable on that state
- Quantum physics
  - systems do get perturbed and modified as a result of measuring them
  - only the probability of observing specific values can be calculated: measurement is inherently a nondeterministic process

- Motivation
  - Classic world
    - Eve can make copies of arbitrary portions of the encrypted bit stream
    - Eve can listen without affecting the bitstream
  - Quantum world (Alice sends qubits)
    - Eve cannot make perfect copies of the qubit stream (because of the no-cloning theorem)
    - The very act of measuring the qubit stream alters it

2. Quant

Lecture 1



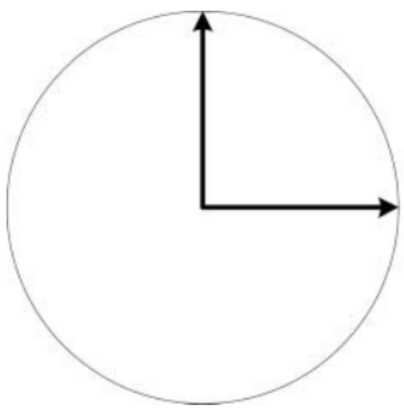
Lecture 6

Charles H. Bennett

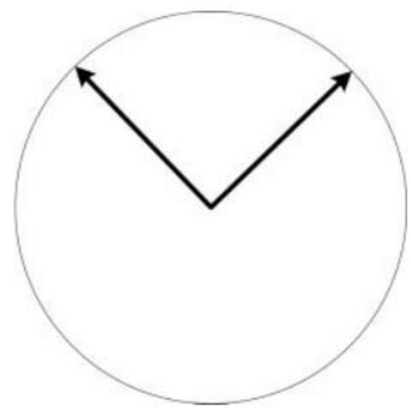
- BB84 protocol (Bennett and Brassard, 1984)
  - Preliminaries (预备1/4)
    - Alice sends Bob a key via a quantum channel (like one-time-pad protocol)
    - Her key is a sequence of random (classic) bits, perhaps, by tossing a coin
    - Alice sends a qubit each time she generates a new bit of her key

2. Quantum Key Exchange

- BB84 protocol
  - Preliminaries (预备2/4)
    - ➢ + and X bases

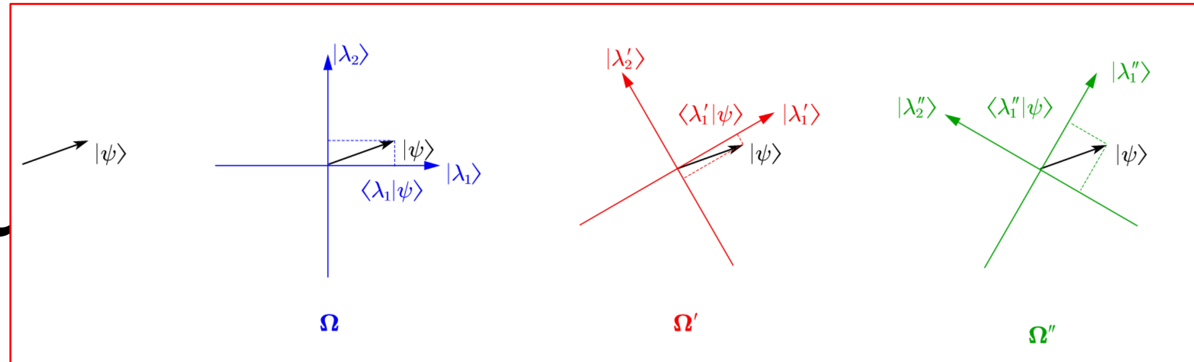


$+ = \{|\rightarrow\rangle, |\uparrow\rangle\} = \{[1,0]^T, [0,1]^T\}$



$X = \{|\nwarrow\rangle, |\nearrow\rangle\} = \left\{\frac{1}{\sqrt{2}}[-1,1]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$

2. Quantu



同一个向量在不同基下对应不同的线性组合

- BB84 protocol
  - Preliminaries (预备3/4)
    - Cross representation under 'plus' and 'times' bases
      (交叉表示，将一个基向量在另外一组基下进行表示)

$$+ = \{|\rightarrow\rangle, |\uparrow\rangle\} = \{[1,0]^T, [0,1]^T\} \qquad X = \{|\nwarrow\rangle, |\nearrow\rangle\} = \left\{\frac{1}{\sqrt{2}}[-1,1]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$$

$|\nwarrow\rangle$ with respect to $+$ will be $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$.

$|\nearrow\rangle$ with respect to $+$, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$.

$|\uparrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

$|\rightarrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

2. Quantum Key Exchange

- BB84 protocol
  - Preliminaries (预备4/4)
    - Map table between bit and qubit

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

  - Meaning
    - Sender: from bit (0/1) to qubit (arrows)
    - Receiver: from qubit (arrows) to bit (0/1)

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

um Key Exchange

- BB84 protocol
  - Step 1 (Alice)
    - Randomly determines classical bits to send
    - Randomly determines the bases to send bits
    - sends the bits in their appropriate basis

Step 1: Alice sends *n* random bits in random bases

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

um Key Exchange

- BB84 protocol
  - Step 2 (Bob)
    - Randomly determines the bases to receive qubits
    - measures the qubit in those random bases

Step 2: Bob receives *n* random bits in random measurements

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob's bits	0	1	1	1	1	0	1	0	1	0	1	0

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

um

Step 1: Alice sends *n* random bits in random bases												
Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

$|\nwarrow\rangle$ with respect to + will be $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$.

$|\nearrow\rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$.

$|\uparrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

$|\rightarrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

- BB84 protocol
  - Step 2 (Bob)
    - Randomly determines the bases to receive bits
    - measures the qubit in those random bases

Step 2: Bob receives *n* random bits in random measurements												
Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob's bits	0		1	1	1	0	1	0	1	0	1	0

跨基观测，随机结果（50%的正确概率）

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

um

Step 1: Alice sends *n* random bits in random bases

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

- BB84 protocol
  - Step 2 (Bob)
    - Randomly determine the bases to receive bits
    - measure the qubit in those random bases

Step 2: Bob receives *n* random bits in random measurements

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob's bits	0	1	[illegible]	1	1	0	1	0	1	0	1	0

一致基观测，确定性结果（100%的正确概率）

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

um

Step 1: Alice sends *n* random bits in random bases

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

- BB84 protocol
  - Step 2 (Bob)
    - Randomly determine the bases to receive bits
    - measure the qubit in those random bases

Step 2: Bob receives *n* random bits in random measurements

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob's bits	0		1	1	1	0	1	0	1	0	1	0

一致基观测，确定性结果（100%的正确概率）

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

um

Step 1: Alice sends *n* random bits in random bases												
Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

$|\nwarrow\rangle$ with respect to + will be $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$.

$|\nearrow\rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$.

$|\uparrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

$|\rightarrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

- BB84 protocol
  - Step 2 (Bob)
    - Randomly determine the bases to receive bits
    - measure the qubit in those random bases

Step 2: Bob receives *n* random bits in random measurements												
Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob's bits	0	1	[illegible]	1	1	0	1	0	1	0	1	0

跨基观测，随机结果（50%的正确概率）

2. Quantum Key Exchange

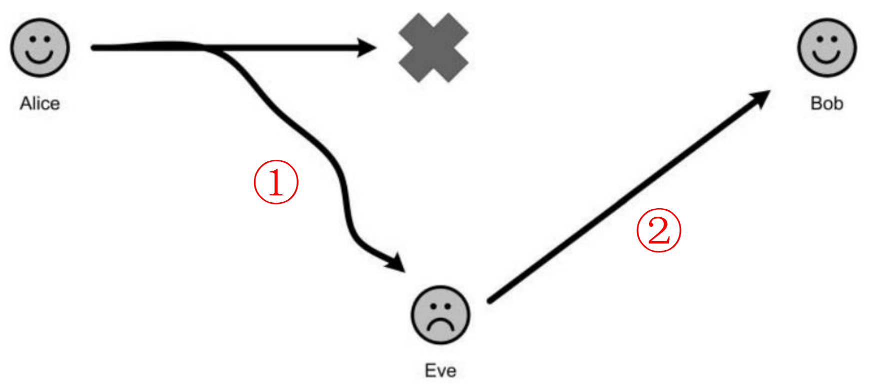
- BB84 protocol
  - Step 2 (Bob): without eavesdropping
    - consistent bases: 100% correct
    - Inconsistent bases: 50% correct

$|\nwarrow\rangle$ with respect to $+$ will be $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$.
$|\nearrow\rangle$ with respect to $+$, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$.
$|\uparrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$.
$|\rightarrow\rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$.

    - Expected correct rate (ECR): $\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4}=75\%$

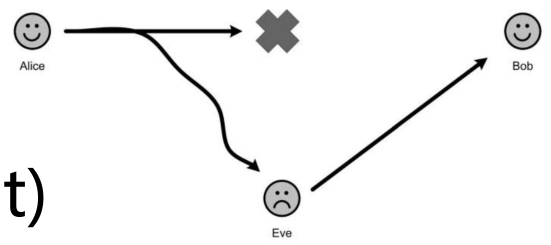
2. Quantum Key Exchange

- BB84 protocol
  - Step 2 (Bob): with eavesdropping



  - What Eve does?
    - Eve reads the information that Alice transmits
    - Eve sends that information onward to Bob

2. Quantum Key Exchange



- BB84 protocol
  - ECR = P(Bob receives correct bit)
  - Solution I
    - Case 1: Eve √ and Bob √
    - Case 2: Eve × but Bob √

Case 2: Eve gets incorrect bits

Bob uses the same base as Eve (definitely wrong)

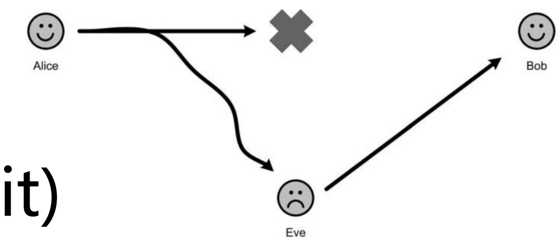
$$\boxed{\frac{3}{4}\times\frac{3}{4}}+\boxed{\frac{1}{4}}\times\left(\boxed{\frac{1}{2}\times 0}+\boxed{\frac{1}{2}\times\frac{1}{2}}\right)=\frac{10}{16}=62.5\%$$

Case 1: Eve gets correct bits and Bob too

Bob uses different base as Eve

2. Quantum Key Exchange

- BB84 protocol
  - ECR = P(Bob receives correct bit)

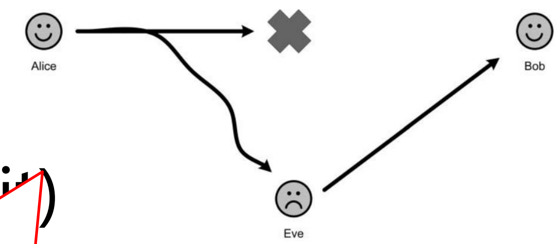


  - Solution II

Eve		Bob		Probability
Receiving basis (consistent to Alice)	Sending bit (qubit) (consistent to Alice)	Receiving basis (consistent to Eve)	Receiving bit (consistent to Alice)	
P(√) = 1/2	P(√) = 1	P(√) = 1/2	P(√) = 1	$\frac{1}{2}\cdot 1\cdot\left[\frac{1}{2}\cdot 1+\frac{1}{2}\cdot\frac{1}{2}\right]=\frac{6}{16}$
		P(×) = 1/2	P(√) = 1/2	
P(×) = 1/2	P(√) = 1/2	P(√) = 1/2	P(√) = 1	$\frac{1}{2}\cdot\frac{1}{2}\cdot\left[\frac{1}{2}\cdot 1+\frac{1}{2}\cdot\frac{1}{2}\right]=\frac{3}{16}$
		P(×) = 1/2	P(√) = 1/2	
	P(×) = 1/2	P(√) = 1/2	P(√) = 0	$\frac{1}{2}\cdot\frac{1}{2}\cdot\left[\frac{1}{2}\cdot 0+\frac{1}{2}\cdot\frac{1}{2}\right]=\frac{1}{16}$
		P(×) = 1/2	P(√) = 1/2	

2. Quantum Key Exchange

- BB84 protocol
  - ECR = P(Bob receives correct bit)
  - Solution II



Ev			
Receiving basis (corr			
P(√)			$\left[\frac{1}{2}\cdot 1+\frac{1}{2}\cdot\frac{1}{2}\right]=\frac{6}{16}$
			$\frac{1}{2}\cdot\left[\frac{1}{2}\cdot 1+\frac{1}{2}\cdot\frac{1}{2}\right]=\frac{3}{16}$
P(×)		0	$\frac{1}{2}\cdot\frac{1}{2}\cdot\left[\frac{1}{2}\cdot 0+\frac{1}{2}\cdot\frac{1}{2}\right]=\frac{1}{16}$
		P(√) /2	

$$\because \frac{6}{16}+\frac{3}{16}+\frac{1}{16}=\frac{10}{16}<\frac{12}{16}=0.75$$

∴ 一旦有人窃听ECR会降低

2. Quantum Key Exchange

- BB84 protocol
  - Step 3 (Alice and Bob)
    - publicly compare which basis they used at each step
    - scratch out corresponding bits under different bases

Step 3: Alice and Bob publicly compare bases used

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Public channel	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Which agree?		✓	✓		✓			✓	✓	✓	✓	✓
Shared secret keys		1	1		1			0	1	0	1	0

On average this subsequence is of length n

2. Quantum Key Exchange

- BB84 protocol
  - Step 4 (Alice and Bob)
    - Bob randomly chooses half of the n/2 bits
    - publicly compares them with Alice

Step 4: Alice and Bob publicly compare half of the remaining bits

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Shared secret keys		1	1		1			0	1	0	1	0
Randomly chosen to compare			✓						✓	✓		✓
Public channel			⇕						⇕	⇕		⇕
Shared secret keys		1	1		1			0	1	0	1	0
Which agree?			✓						✓	✓		✓
Unrevealed secret keys:		1			1			0			1	

2. Quantum Key Exchange

- BB84 protocol
  - Step 4 (Alice and Bob)
    - Bob randomly chooses half of the n/2 bits
    - publicly compares them with Alice
      - If $\mathrm{ECR} \leqslant 1 - \epsilon$, Eve is listening, scratch the whole sequence
      - Otherwise, scratch out the revealed test subsequence and keep the remains as unrevealed secret private key

2. Quantum Key Exchange

- B92 protocol (Bennett, 1992)
  - Motivation
    - two different bases are redundant for Alice
    - But Bob still needs two bases
  - Main idea
    - Alice uses only one non-orthogonal basis

$$\{|\rightarrow\rangle \mid \nearrow\rangle\} = \left\{[1,0]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$$

2. Quantum Key Exchange

- B92 protocol
  - Step 1 (Alice)
    - randomly determine classical bits to send
    - send the bits in the appropriate polarization

Step 1: Alice sends *n* random bits in the ∠ basis

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's qubits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

2. Quantum Key Exchange

- B92 protocol
  - Step 2 (Bob)
    - randomly determines the bases to receive bits
    - measures the qubit in those random bases

- If Bob uses the $+$ basis and observes a $|\uparrow\rangle$, then he knows that Alice must have sent a $|\nearrow\rangle = |1\rangle$ because if Alice had sent a $|\rightarrow\rangle$, Bob would have received a $|\rightarrow\rangle$.
- If Bob uses the $+$ basis and observes a $|\rightarrow\rangle$, then it is not clear to him which qubit Alice sent. She could have sent a $|\rightarrow\rangle$ but she could also have sent a $|\nearrow\rangle$ that collapsed to a $|\rightarrow\rangle$. Because Bob is in doubt, he will omit this bit.
- If Bob uses the X basis and observes a $|\nwarrow\rangle$, then he knows that Alice must have sent a $|\rightarrow\rangle = |0\rangle$ because if Alice had sent a $|\nearrow\rangle$, Bob would have received a $|\nearrow\rangle$.
- If Bob uses the X basis and observes a $|\nearrow\rangle$, then it is not clear to him which qubit Alice sent. She could have sent a $|\nearrow\rangle$ but she could also have sent a $|\rightarrow\rangle$ that collapsed to a $|\nearrow\rangle$. Because Bob is in doubt, he will omit this bit.

2. Quantum K

- If Bob uses the + basis and observes a $|\uparrow\rangle$, then he knows that Alice must have sent a $|\nearrow\rangle = |1\rangle$ because if Alice had sent a $|\rightarrow\rangle$, Bob would have received a $|\rightarrow\rangle$.
- If Bob uses the + basis and observes a $|\rightarrow\rangle$, then it is not clear to him which qubit Alice sent. She could have sent a $|\rightarrow\rangle$ but she could also have sent a $|\nearrow\rangle$ that collapsed to a $|\rightarrow\rangle$. Because Bob is in doubt, he will omit this bit.
- If Bob uses the X basis and observes a $|\nwarrow\rangle$, then he knows that Alice must have sent a $|\rightarrow\rangle = |0\rangle$ because if Alice had sent a $|\nearrow\rangle$, Bob would have received a $|\nearrow\rangle$.
- If Bob uses the X basis and observes a $|\nearrow\rangle$, then it is not clear to him which qubit Alice sent. She could have sent a $|\nearrow\rangle$ but she could also have sent a $|\rightarrow\rangle$ that collapsed to a $|\nearrow\rangle$. Because Bob is in doubt, he will omit this bit.

- B92 protocol
  - Step 2 (Bob)
    - randomly determines the bases to receive bits
    - measures the qubit in those random bases

Step 2: Bob receives *n* random bits in a random basis

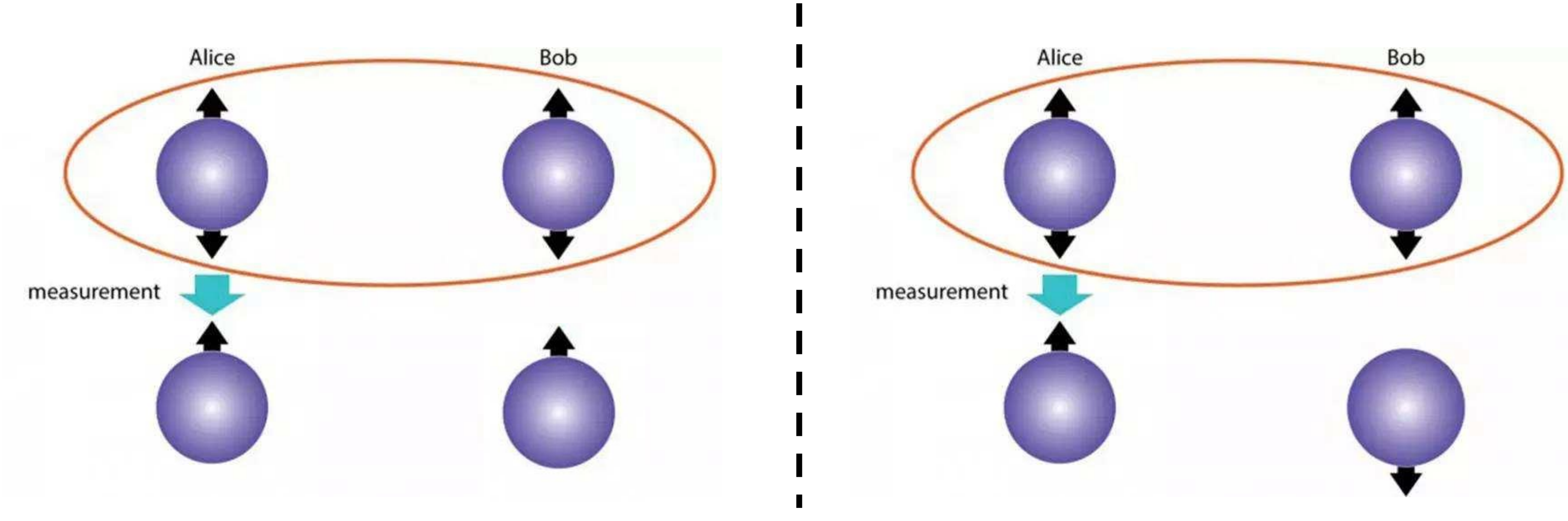
Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
Bob's random bases	X	+	X	X	+	X	+	+	X	+	X	+
Bob's observations	↖	→	↗	↖	↑	↖	→	→	↗	↑	↗	→
Bob's bits	0	?	?	0	1	0	?	?	?	1	?	?

2. Quantum Key Exchange

- B92 protocol
  - Step 3 (Alice and Bob)
    - Bob publicly tells Alice which bits were uncertain
    - they both omit uncertain bits
  - Step 4 (optional for intrusion detection)
    - Bob randomly chooses half of the n/2 bits
    - publicly compares them with Alice

2. Quantum Key Exchange

- EPR protocol (Ekert, 1991)
  - Idea: entangled state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ or $\frac{|01\rangle + |10\rangle}{\sqrt{2}}$
    - Prepare a sequence of entangled pairs of qubits



2. Quantum Key Exchange

- EPR protocol (Ekert, 1991)
  - Aims
    - Intrusion detection
    - Quantum decoherence detection
  - Idea
    - Measure a qubit in two bases:

      X and + bases

      (same vocabulary of BB84)

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

2. Quantum Key Exchange

- EPR protocol (Ekert, 1991)
  - Step 1 (Alice and Bob)
    - Both sides are each assigned one of each of the pairs of a sequence of entangled qubits

State / Basis	+	X
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

2. Quantum Key Exc

- EPR protocol with intrusion detection
  - Step 2 (Alice and Bob)
    - separately choose a random sequence of bases
    - measure their qubits in their chosen basis

Step 2: Alice and Bob measure in each of their random bases

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	X	X	+	+	X	+	X	+	+	X	+	X
Alice's observations	↗	↖	→	↑	↗	→	↖	→	→	↗	→	↗
Bob's random bases	X	+	+	X	X	+	+	+	+	X	X	+
Bob's observations	↗	→	→	↗	↗	→	↑	→	→	↗	↖	→

2. Quantum Key Exchange

■ EPR protocol with intrusion detection

- Step 3 (Alice and Bob)
  - ➢ publicly compare what bases were used
  - ➢ keep only those bits measured in the same basis

Step 3: Alice and Bob publicly compare their bases

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	X	X	+	+	X	+	X	+	+	X	+	X
Public channel	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Bob's random bases	X	+	+	X	X	+	+	+	+	X	X	+
Which agree?	✓		✓		✓	✓		✓	✓	✓		

2. Quantum Key Exchange

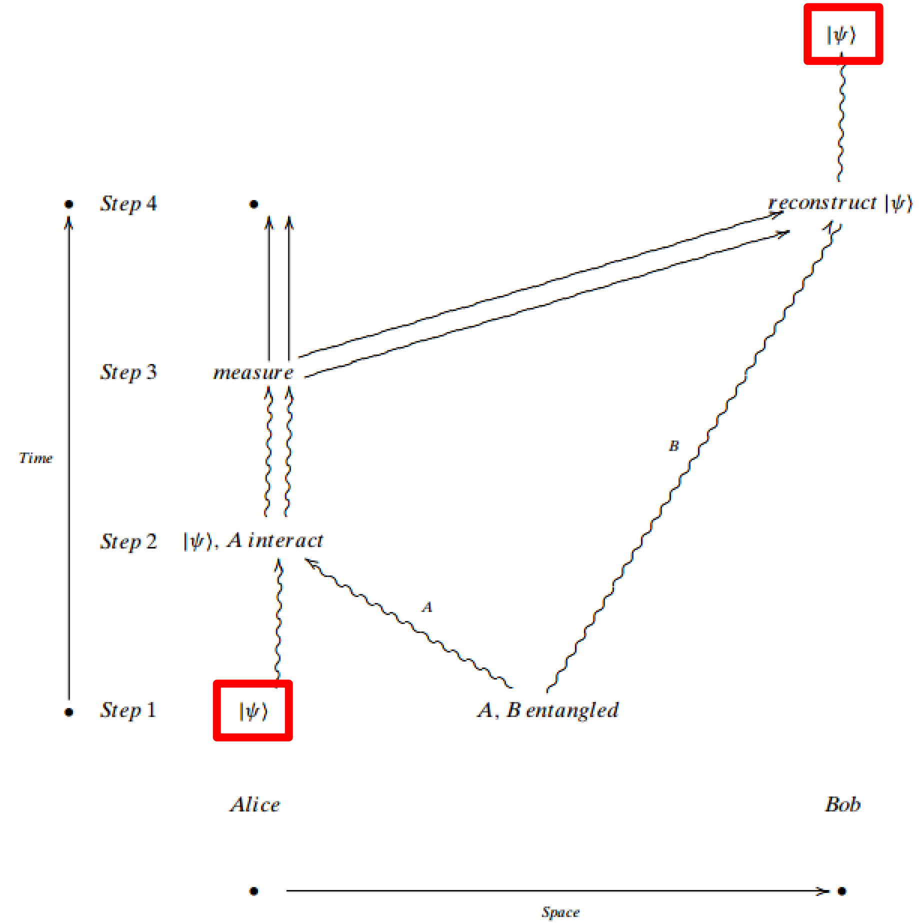
- EPR protocol with intrusion detection
  - Step 4 (optional for intrusion or disentangled detection)
    - Bob randomly chooses half of the $n/2$ bits
    - publicly compares them with Alice
  - Remark
    - In Ekert's original protocol, qubits are measured in three different bases
    - Bell's inequality is used to detect decoherence

3. Quantum Teleportation

- Definition: Quantum teleportation（远距离传输，量子隐形传态）
  - Quantum teleportation is the process by which the state of an arbitrary qubit is transferred from one location to another
- Note (no-cloning theorem)
  - Move is possible, copy is impossible

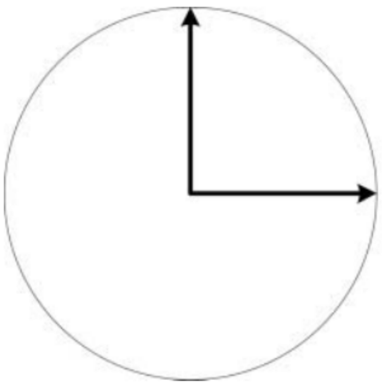
3. Quantum Teleportation

- Definition
  - Alice has $|\psi\rangle$
  - Bob is far from Alice
  - Transmit $|\psi\rangle$ from Alice to Bob

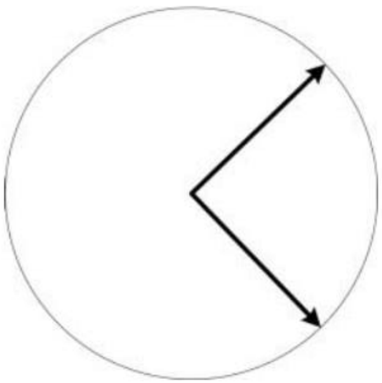


3. Quantum Teleportation

- Preliminary
  - Canonical basis
    - $\{|0\rangle, |1\rangle\}$



  - Non-canonical basis
    - $\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$



3. Quantum Teleportation

- Preliminary
  - Canonical basis for a single qubit
    - $\{\,|0\rangle,\ |1\rangle\,\}$
  - Non-canonical basis (Bell basis) for single qubit
    - $\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$

Φ φ	φεῖ	Phi	/ˈfaɪ/
Χ χ	χεῖ	Chi	/ˈkaɪ/
Ψ ψ	ψεῖ	Psi	/ˈsaɪ/ , /ˈpsaɪ/

3. Quantum Teleportation

- Preliminary
  - Canonical basis for two qubits
    - $\{|0_A 0_B\rangle, |0_A 1_B\rangle, |1_A 0_B\rangle, |1_A 1_B\rangle\}$
  - Non-canonical basis (Bell basis) for two qubits
    - entangled states
      - $|\Psi^+\rangle = \dfrac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}}$ and $|\Psi^-\rangle = \dfrac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}}$
      - $|\Phi^+\rangle = \dfrac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$ and $|\Phi^-\rangle = \dfrac{|0_A 0_B\rangle - |1_A 1_B\rangle}{\sqrt{2}}$

Φ φ	φεῖ	Phi	/ˈfaɪ/
Χ χ	χεῖ	Chi	/ˈkaɪ/
Ψ ψ	ψεῖ	Psi	/ˈsaɪ/ , /ˈpsaɪ/

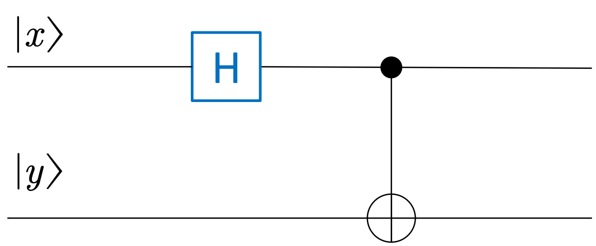
3. Quantum Teleportation

- Preliminary
  - Bell circuit: Derivation of Bell basis
    - Two-dimensional case

$$\mathrm{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{and} \quad \mathrm{H}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

    - Four-dimensional case

Why?



Example: $|00\rangle \mapsto |\Phi^+\rangle$

$$\mathrm{CNOT} \cdot (\mathrm{H}|0\rangle \otimes |0\rangle) = \mathrm{CNOT} \cdot \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right)$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle$$

$$|00\rangle \mapsto |\Phi^+\rangle, \quad |10\rangle \mapsto |\Phi^-\rangle, \quad |01\rangle \mapsto |\Psi^+\rangle, \quad |11\rangle \mapsto |\Psi^-\rangle$$

Φ φ	φεῖ	Phi	/ˈfaɪ/
Χ χ	χεῖ	Chi	/ˈkaɪ/
Ψ ψ	ψεῖ	Psi	/ˈsaɪ/ , /ˈpsaɪ/

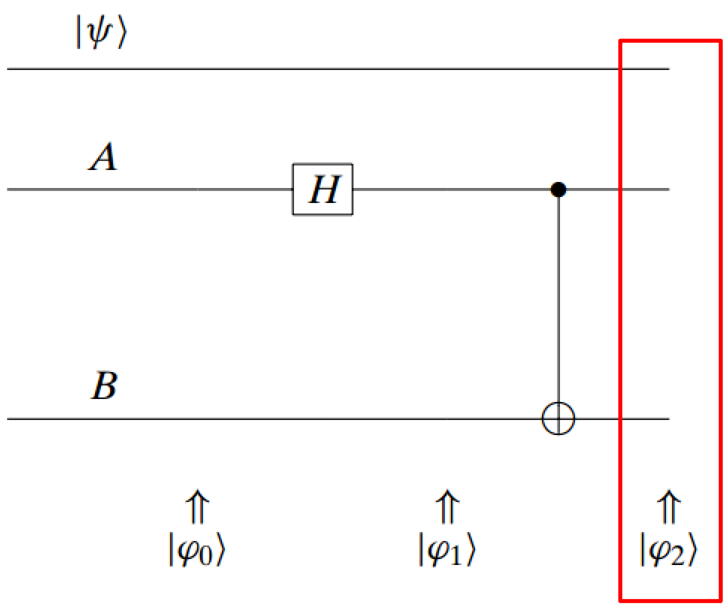
3. Quantum Teleportation

- Step 0
  - Alice has a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Φ φ	φεῖ	Phi	/ˈfaɪ/
Χ χ	χεῖ	Chi	/ˈkaɪ/
Ψ ψ	ψεῖ	Psi	/ˈsaɪ/ , /ˈpsaɪ/

3. Quantum Teleportation

- Step 1：制备两个纠缠的量子比特A和B
  - two entangled qubits are formed as $|\Phi^+\rangle$.
  - one is given to Alice and one is given to Bob



$$|\varphi_0\rangle = |\psi\rangle \otimes |0_A\rangle \otimes |0_B\rangle = |\psi\rangle \otimes |0_A 0_B\rangle,$$

$$|\varphi_1\rangle = |\psi\rangle \otimes \frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}} \otimes |0_B\rangle,$$

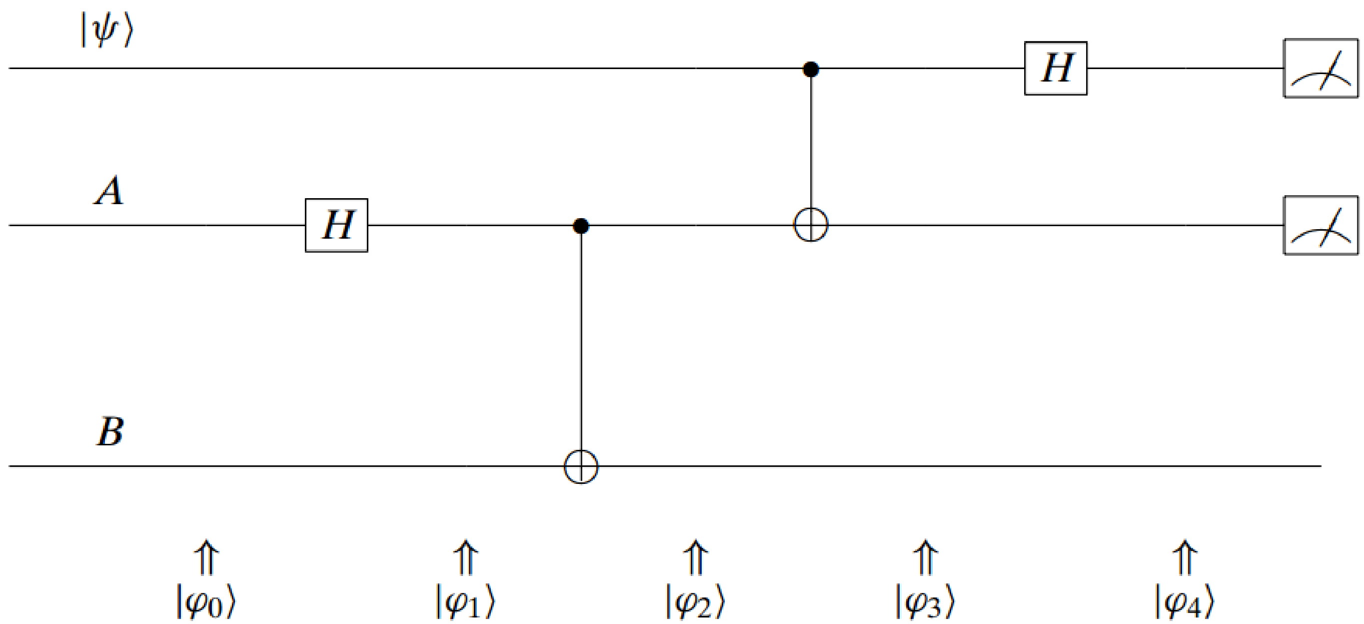
$$|\varphi_2\rangle = |\psi\rangle \otimes |\Phi^+\rangle = |\psi\rangle \otimes \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$

$$= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$

$$= \frac{\alpha|0\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta|1\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle)}{\sqrt{2}}.$$

3. Quantum Teleportation

- Step 2：用目标量子比特对A进行控制
  - Alice lets her $|\psi\rangle$ interact with her entangled qubit



3. Quantum Teleportation

- Step 2
  - Alice lets her $|\psi\rangle$ interact with her entangled qubit

$$|\varphi_2\rangle = \frac{\alpha|0\rangle(|0_A0_B\rangle + |1_A1_B\rangle) + \beta|1\rangle(|0_A0_B\rangle + |1_A1_B\rangle)}{\sqrt{2}}.$$

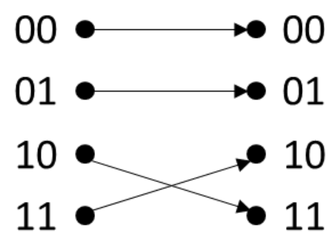
$$|\varphi_3\rangle = \frac{\alpha|0\rangle(|0_A0_B\rangle + |1_A1_B\rangle) + \beta|1\rangle(|1_A0_B\rangle + |0_A1_B\rangle)}{\sqrt{2}},$$

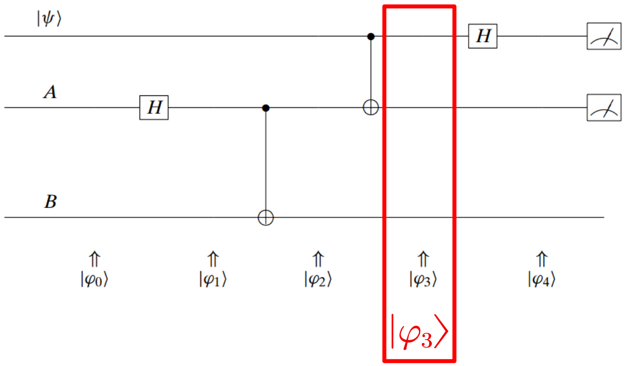
$$\begin{aligned}|\varphi_4\rangle &= \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|0_A0_B\rangle + |1_A1_B\rangle) + \beta(|0\rangle - |1\rangle)(|1_A0_B\rangle + |0_A1_B\rangle))\\ &= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)).\end{aligned}$$

$$\begin{aligned}|\varphi_4\rangle = \frac{1}{2}(&|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle)\\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)).\end{aligned}$$

3. Qua

$$|x,\ y\rangle \mapsto |x,\ x \oplus y\rangle$$





- Step 2
  - Alice lets her $|\psi\rangle$ interact with her entangled qubit.

$$|\varphi_2\rangle = \frac{\alpha|0\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta|1\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle)}{\sqrt{2}}.$$

$$|\varphi_3\rangle = \frac{\alpha|0\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta|1\rangle(|1_A 0_B\rangle + |0_A 1_B\rangle)}{\sqrt{2}},$$

$$|\varphi_4\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta(|0\rangle - |1\rangle)(|1_A 0_B\rangle + |0_A 1_B\rangle))$$

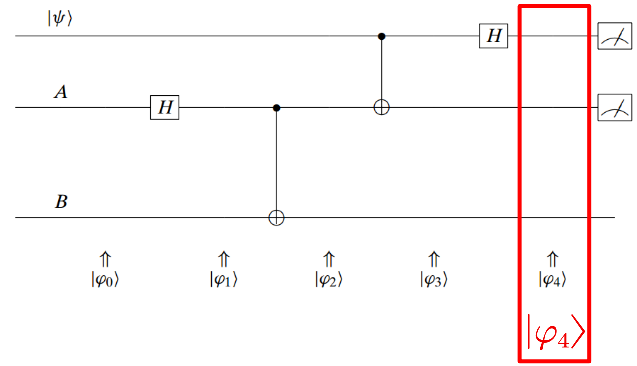
$$= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)).$$

$$|\varphi_4\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle)$$
$$+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)).$$

3. Qua

$$\mathbf{H}|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\mathbf{H}|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$



- Step 2
  - Alice lets her $|\psi\rangle$ interact with her entangled qubit.

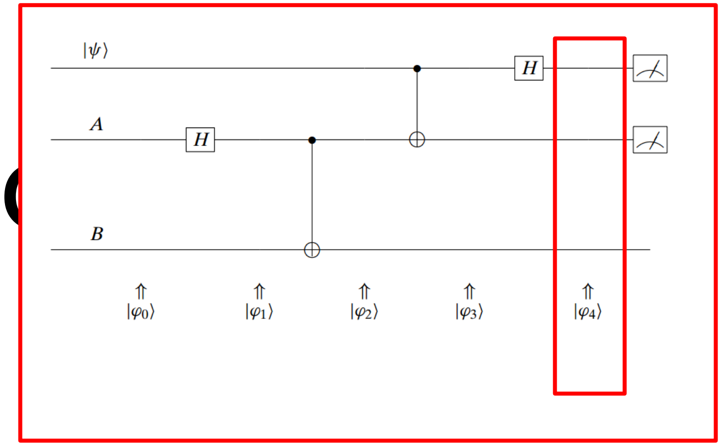
$$|\varphi_2\rangle = \frac{\alpha|0\rangle(|0_A0_B\rangle + |1_A1_B\rangle) + \beta|1\rangle(|0_A0_B\rangle + |1_A1_B\rangle)}{\sqrt{2}}.$$

$$|\varphi_3\rangle = \frac{\alpha|0\rangle(|0_A0_B\rangle + |1_A1_B\rangle) + \beta|1\rangle(|1_A0_B\rangle + |0_A1_B\rangle)}{\sqrt{2}},$$

$$\begin{aligned} |\varphi_4\rangle &= \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|0_A0_B\rangle + |1_A1_B\rangle) + \beta(|0\rangle - |1\rangle)(|1_A0_B\rangle + |0_A1_B\rangle)) \\ &= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)). \end{aligned}$$

$$\begin{aligned} |\varphi_4\rangle = &\frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) \\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)). \end{aligned}$$

3. Quantum Telep



- Step 2
  - Alice lets her $|\psi\rangle$ interact with her entangled qubit.

$$|\varphi_2\rangle = \frac{\alpha|0\rangle(|0_A0_B\rangle + |1_A1_B\rangle) + \beta|1\rangle(|0_A0_B\rangle + |1_A1_B\rangle)}{\sqrt{2}}.$$

$$|\varphi_3\rangle = \frac{\alpha|0\rangle(|0_A0_B\rangle + |1_A1_B\rangle) + \beta|1\rangle(|1_A0_B\rangle + |0_A1_B\rangle)}{\sqrt{2}},$$

$$|\varphi_4\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|0_A0_B\rangle + |1_A1_B\rangle) + \beta(|0\rangle - |1\rangle)(|1_A0_B\rangle + |0_A1_B\rangle))$$
$$= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)).$$

$$|\varphi_4\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle)$$
$$+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)).$$

The first two qubits is now in a superposition of four possible states

3. Quantum Teleportation

$$|\varphi_4\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)).$$

- Step 3：Alice进行观测
  - Alice measures her two qubits
  - Alice determines to which of the four possible states the system collapses
- Two problems
  - Alice knows this state but Bob does not
  - Bob may not have the desired state after Alice's measurement

3. Quantum Teleportation

- Step 4：Bob根据Alice观测结果进行相应变换
  - Alice sends copies of her two bits (not qubits) to Bob
  - Bob uses that information to achieve the desired state

- Example

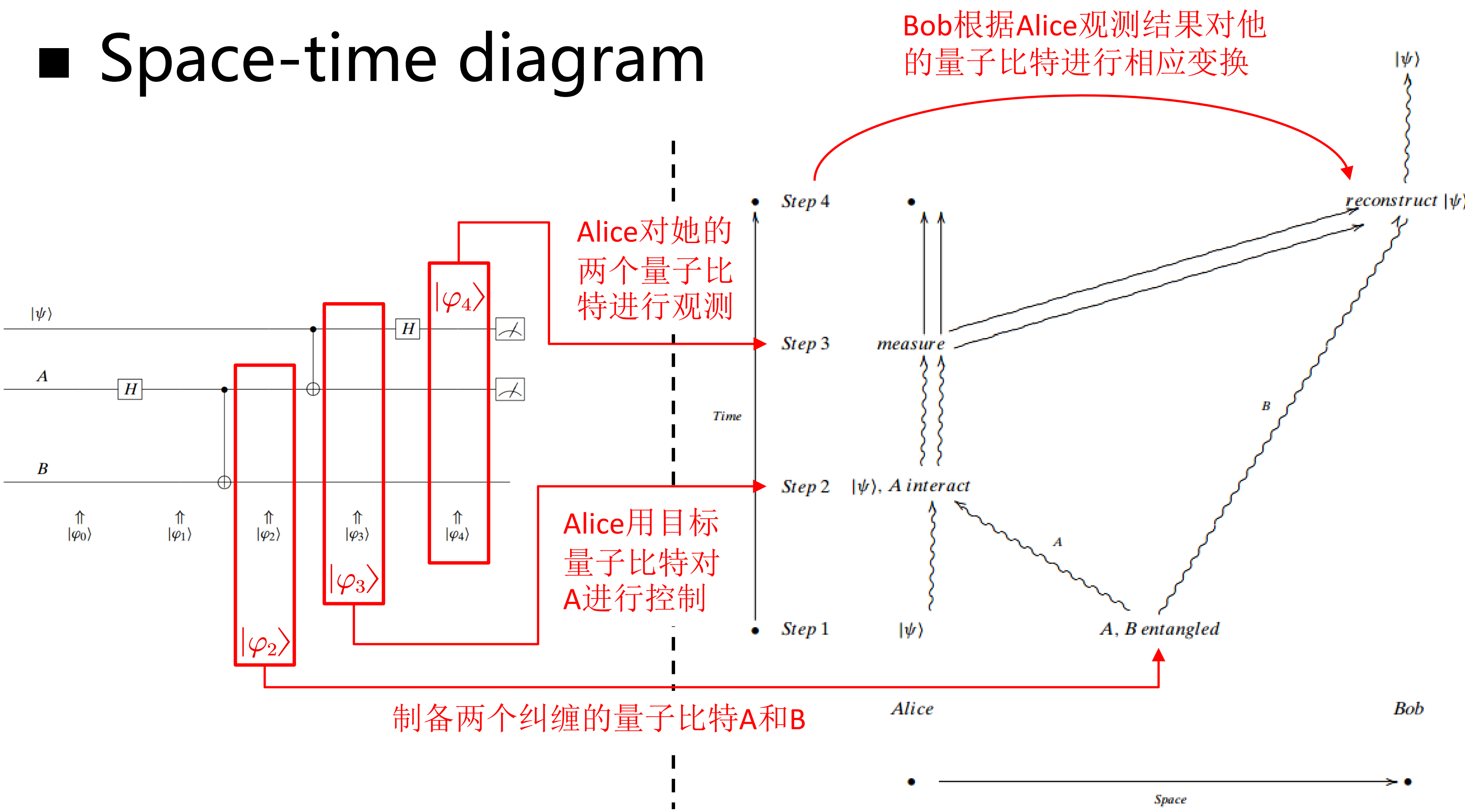
$$|\varphi_4\rangle = \frac{1}{2}\big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)\big).$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

Bob's reconstruction matrices				
Bits received	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
Matrix to apply	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
Pauli变换	I 门	X 门	Z 门	Y 门

3. Quantum Teleportation

- Space-time diagram



补充材料

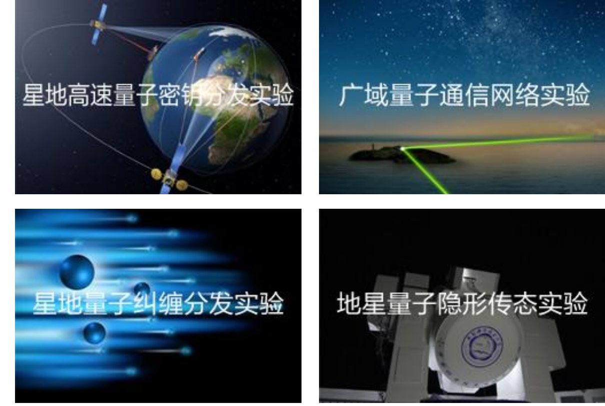
- 墨子号

空间的光子对话，视频来源：https://www.bilibili.com/video/BV1FC4y1h779

3. Quantum Teleportation

- Remarks
  - After teleportation, Alice has only two classic bits
  - Entanglement acts at a super-light speed, but communication does not (见后续页补充材料)
  - Information teleported from Alice to Bob via qubit is infinite (无穷维小数，所以信息是无限的), but it is useless to Bob once he make the measurement (qubit will collapse to a classic bit)
  - no particle has been moved at all, only the state

补充材料

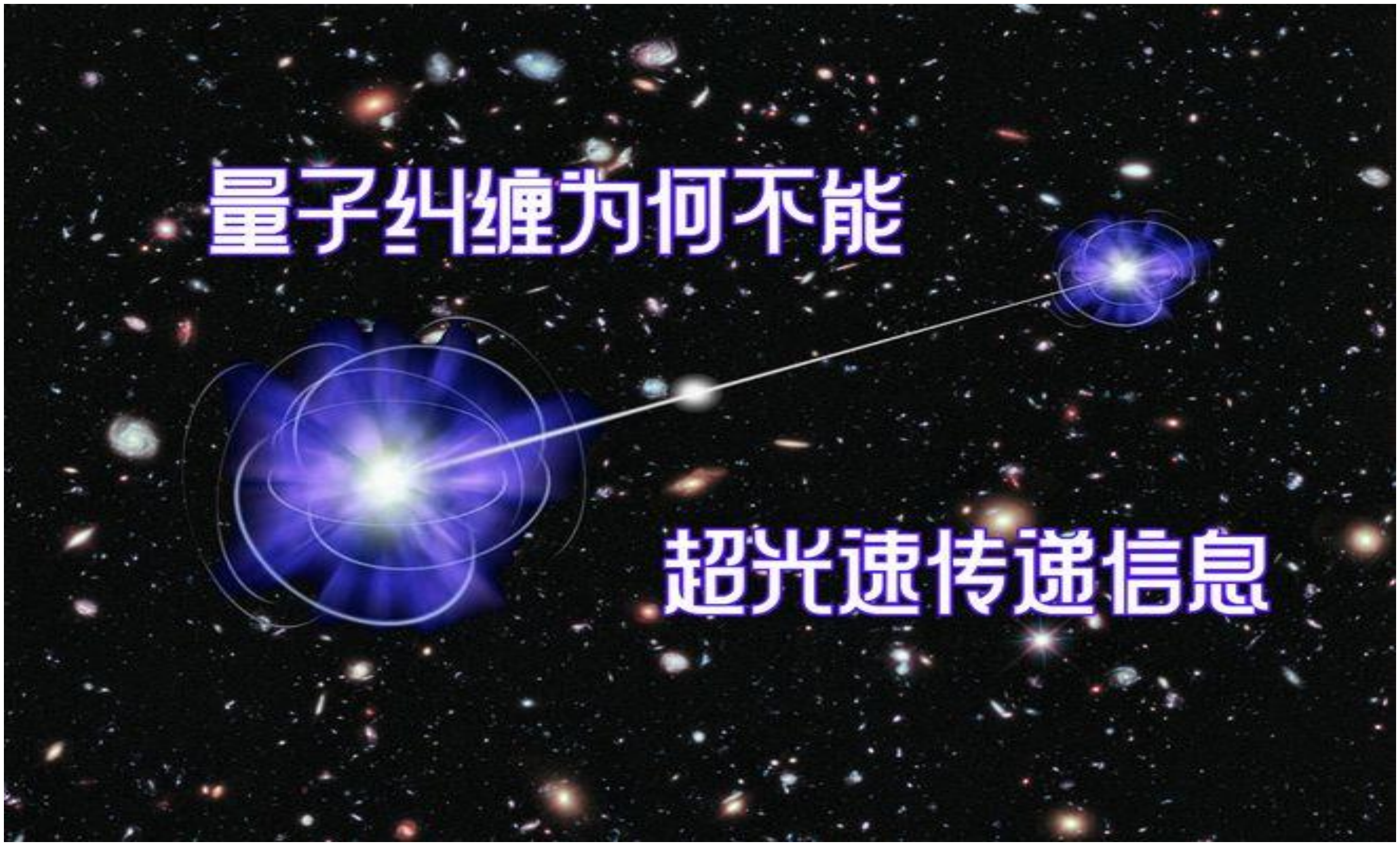


■ 墨子号

- 世界首颗量子科学实验卫星，潘建伟院士，2016年
- 目的：建立卫星与地面远距离量子科学实验平台
  - ➢ 空间大尺度量子科学实验
- 有效载荷

载荷名称	目标/用途
量子纠缠发射机QET	将卫星上产生的量子密钥通过激光分发到地面上。
量子密钥通信机QKC	对星地量子密钥分发进行验证，进行星地量子通讯。
量子纠缠源QEPS	产生纠缠光子对。
量子实验控制与处理机QCP	通过量子纠缠和隐形传态实验对量子理论的完备性进行验证。

补充材料：超光速通讯不可行



图片来源：https://www.163.com/dy/article/H4CTB8RC05327GVA.html

补充材料：超光速通讯不可行

- 硬币的两面

知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

- 将两枚硬币分别放入两个盒子

知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

- 用 A 方法打开两个盒子，一正一反

或者

知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

- 用 B 方法打开两个盒子，同正或同反

或者

知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

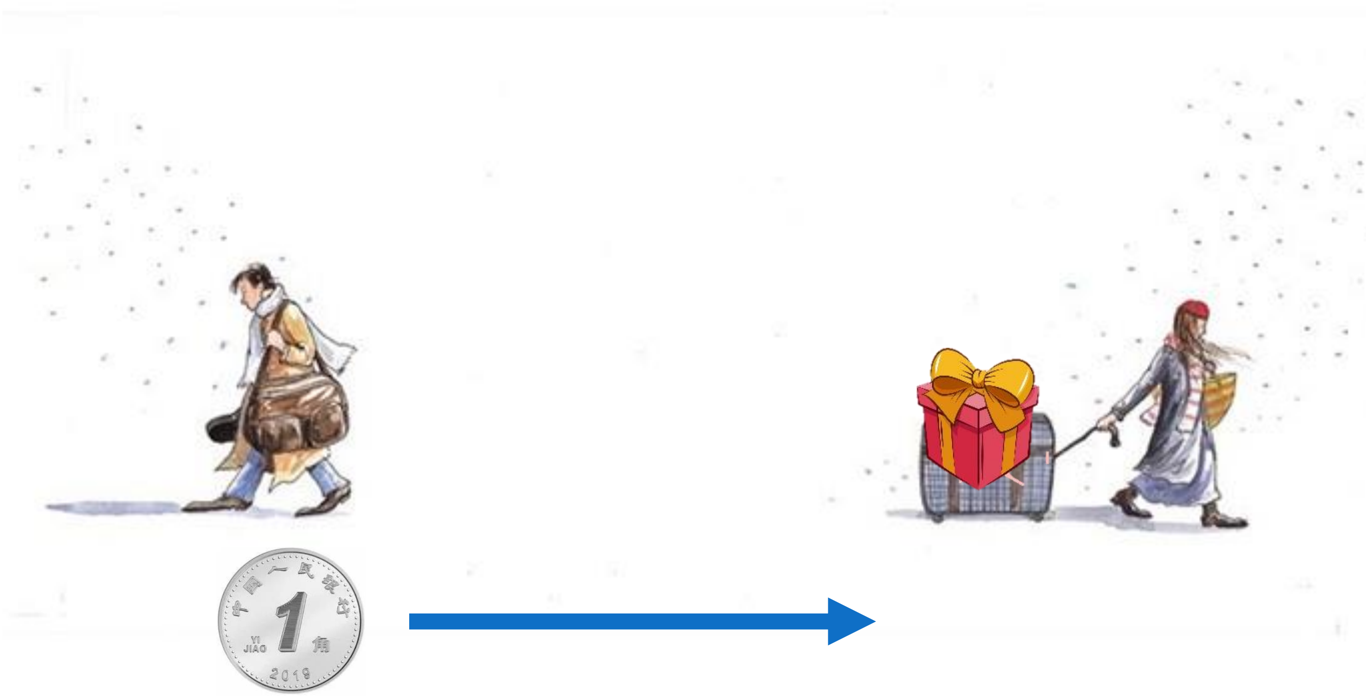
补充材料：超光速通讯不可行

- 甲乙两人分别带着两个盒子去往两处，他们各自可以自由决定用何种方式（A或B）打开盒子
- 打开盒子的方式就是双方要传递的信息

知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

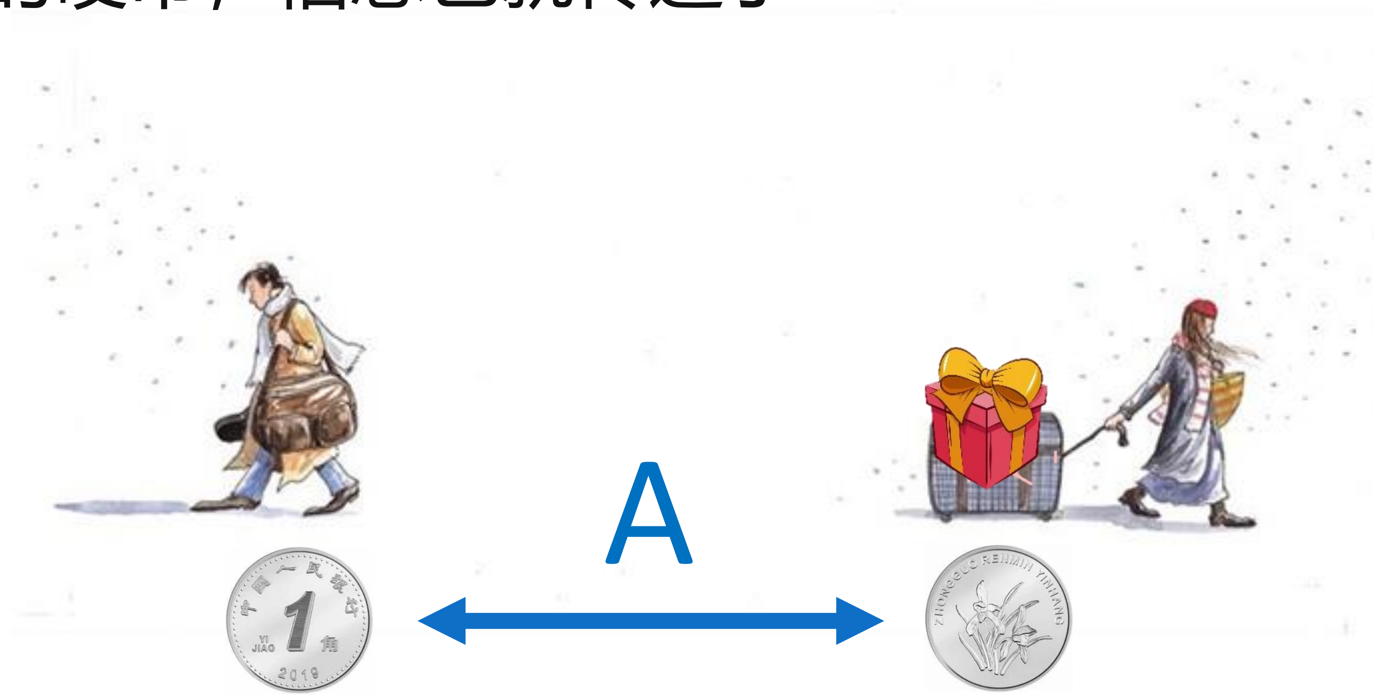
- 甲打开盒子，然后打电话告诉乙自己硬币的正反



知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

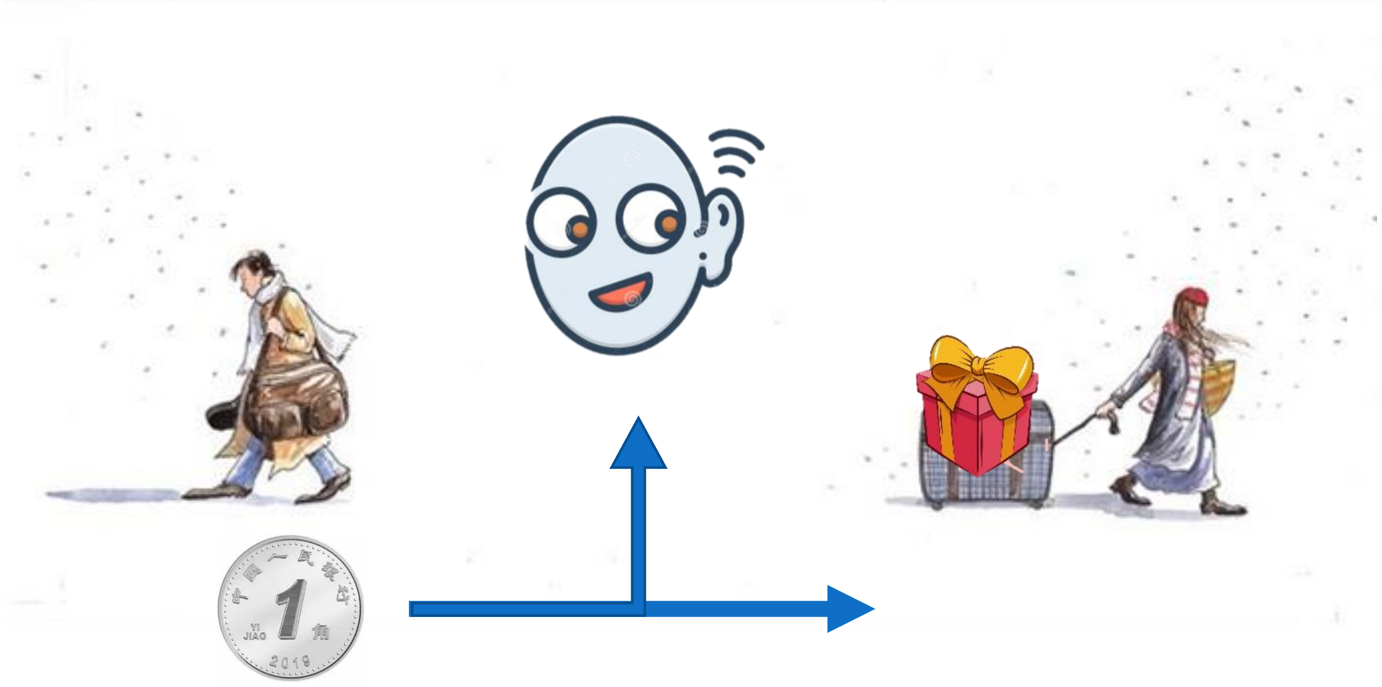
- 乙看一眼自己的硬币，就知道甲用哪种方法打开的硬币，信息也就传递了



知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

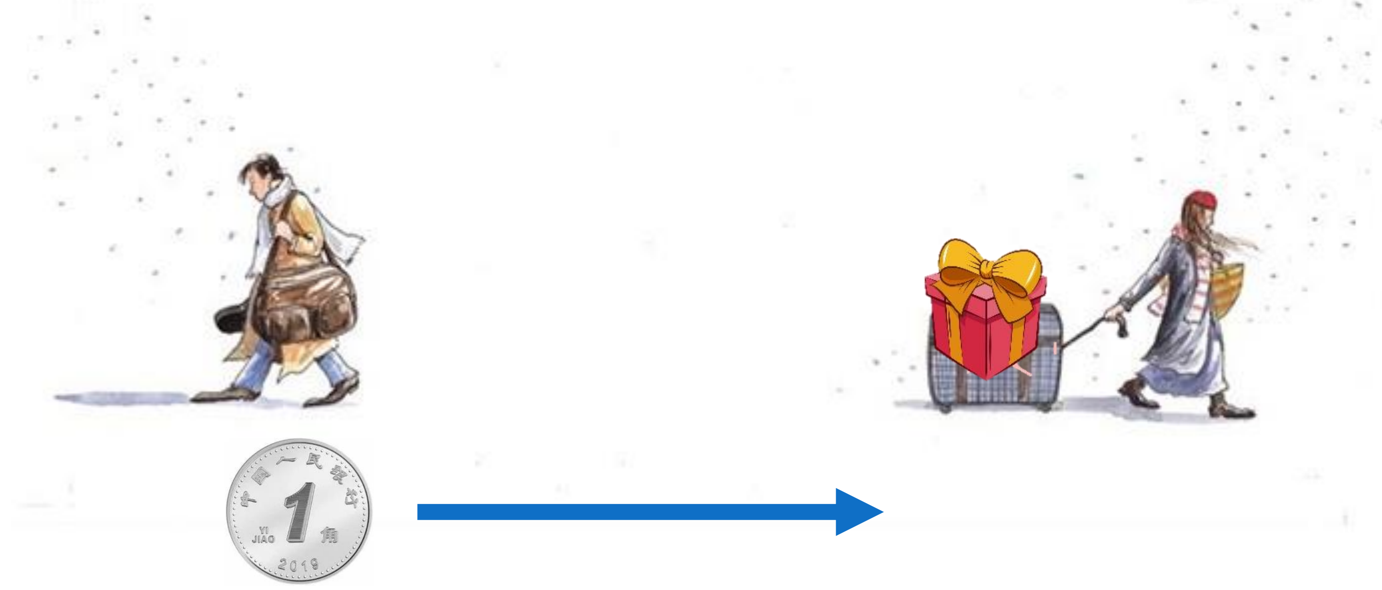
- 哪怕别人窃听了电话，也没法知道信息内容，所以量子通信是一种安全的信息加密方法



知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

- 信息传播的速度不会超过打电话的速度，在没有接到电话时，乙光凭自己的硬币无法得知任何信息。所以量子通讯并非超光速通讯的手段。



知乎，为什么量子通信不能超光速传递信息？
https://www.zhihu.com/question/34773362

补充材料：超光速通讯不可行

- 纠缠电子
  - 给定一对纠缠电子，将其分别给Alice和Bob

$$\frac{1}{2}|a_0\rangle|b_0\rangle+\frac{1}{2}|a_0\rangle|b_1\rangle+\frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle+0|a_1\rangle|b_1\rangle$$

  - 两人如果同时测量，则根据概率幅知：
    - 00的概率为1/4
    - 01的概率为1/4
    - 10的概率为1/2
    - 11的概率为0

来源于：《人人可懂的量子计算》，**Chris Bernhardt**著，邱道文等译，机械工业出版社，**2020**年

补充材料：超光速通讯不可行

- 假设Alice进行测量，Bob没有测量

$$\frac{1}{2}|a_0\rangle|b_0\rangle+\frac{1}{2}|a_0\rangle|b_1\rangle+\frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle+0|a_1\rangle|b_1\rangle$$

$$=|a_0\rangle\left(\frac{1}{2}|b_0\rangle+\frac{1}{2}|b_1\rangle\right)+|a_1\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle+0|b_1\rangle\right)$$

$$=\frac{1}{\sqrt{2}}|a_0\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\right)+\frac{1}{\sqrt{2}}|a_1\rangle(1|b_0\rangle+0|b_1\rangle)$$ % 括号内为量子比特

  - 括号内项不同，所以状态是纠缠的
  - a粒子的状态振幅表明，Alice观测到0的概率为1/2，观测到1的概率为1/2
  - 如果Alice观测到0，则b粒子状态为 $\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle$；如果Alice观测到1，则b粒子状态为 $|b_0\rangle$

来源于：《人人可懂的量子计算》，**Chris Bernhardt**著，邱道文等译，机械工业出版社，**2020**年

补充材料：超光速通讯不可行

- 假设Bob进行测量，Alice没有测量

$$\frac{1}{2}|a_0\rangle|b_0\rangle+\frac{1}{2}|a_0\rangle|b_1\rangle+\frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle+0|a_1\rangle|b_1\rangle$$

$$=\left(\frac{1}{2}|a_0\rangle+\frac{1}{\sqrt{2}}|a_1\rangle\right)|b_0\rangle+\left(\frac{1}{2}|a_0\rangle+0|a_1\rangle\right)|b_1\rangle$$

$$=\left(\frac{1}{\sqrt{3}}|a_0\rangle+\frac{\sqrt{2}}{\sqrt{3}}|a_1\rangle\right)\frac{\sqrt{3}}{2}|b_0\rangle+(1|a_0\rangle+0|a_1\rangle)\frac{1}{2}|b_1\rangle$$ % 括号内为量子比特

  - 括号内项不同，所以状态是纠缠的
  - b粒子的状态振幅表明，Bob观测到0的概率为3/4，观测到1的概率为1/4
  - 如果Bob观测到0，则a粒子状态为$\frac{1}{\sqrt{3}}|a_0\rangle+\frac{\sqrt{2}}{\sqrt{3}}|a_1\rangle$；如果Bob观测到1，则a粒子状态为$|a_0\rangle$

来源于：《人人可懂的量子计算》，**Chris Bernhardt著，邱道文等译，机械工业出版社，2020年**

补充材料：超光速通讯不可行

- 假设Alice先于Bob进行测量
  - Alice观测到0的概率为1/2，观测到1的概率为1/2
- 假设Bob先于Alice进行测量
  - Alice观测到0的概率为 $\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$
    - Bob观测先到0，Alice后观测到0的概率为 $\frac{3}{4}\times\left(\frac{1}{\sqrt{3}}\right)^2=\frac{1}{4}$
    - Bob观测先到1，Alice后观测到0的概率为 $\frac{1}{4}\times 1=\frac{1}{4}$
  - Alice观测到1的概率为 $\frac{1}{2}+0=\frac{1}{2}$
    - Bob观测先到0，Alice后观测到1的概率为 $\frac{3}{4}\times\left(\frac{\sqrt{2}}{\sqrt{3}}\right)^2=\frac{1}{2}$
    - Bob观测先到1，Alice后观测到1的概率为 $\frac{1}{4}\times 0=0$

来源于：《人人可懂的量子计算》，**Chris Bernhardt**著，邱道文等译，机械工业出版社，**2020**年

补充材料：超光速通讯不可行

- 假设Alice先于Bob进行测量
  - Alice观测到0的概率为1/2，观测到1的概率为1/2
- 假设Bob先于Alice进行测量
  - Alice观测到0的概率为1/2，观测到1的概率为1/2

> 全一致。因此，Alice 无法从她的测量结果中判断出它们是在 Bob 测量之前还是之后。所有纠缠态都是这样的。如果 Alice 和 Bob 无法通过他们的测量结果判断谁先测量，那么其中一个人肯定无法向另一个发送任何信息。

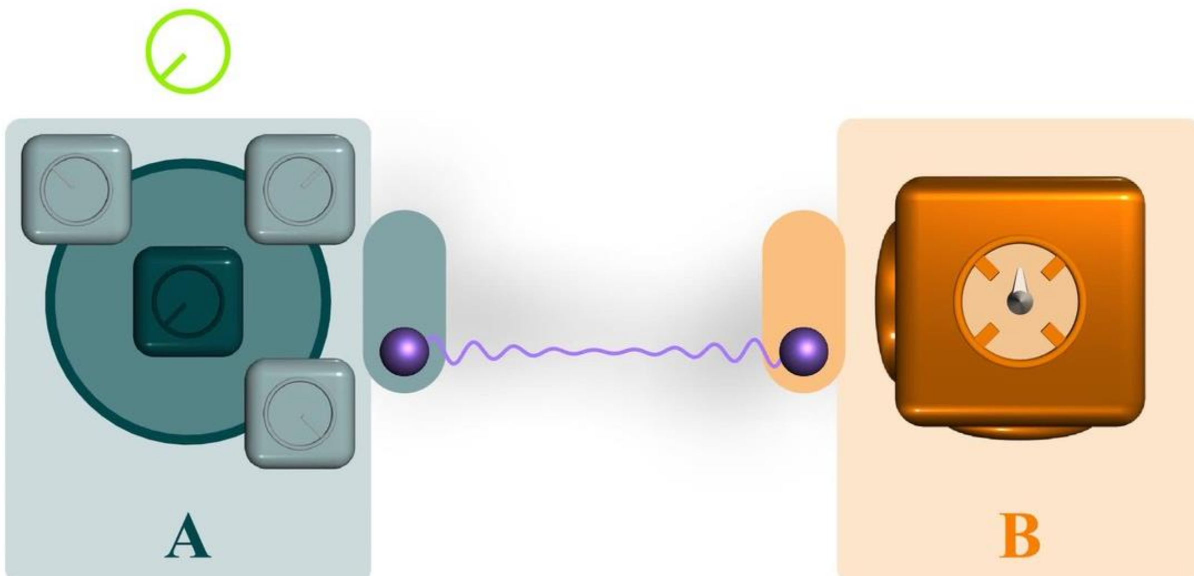
来源于：《人人可懂的量子计算》，**Chris Bernhardt著，邱道文等译，机械工业出版社，2020年**

补充材料：超光速通讯不可行

- 传信息的条件是你要能操纵测量结果，但量子纠缠不能，一操作就不纠缠了
- 实际上测量后，原纠缠对里的粒子A就无法决定粒子B的状态了，无论在测量后对粒子A进行任何操作，都不会改变粒子B的状态

4. Superdense Coding

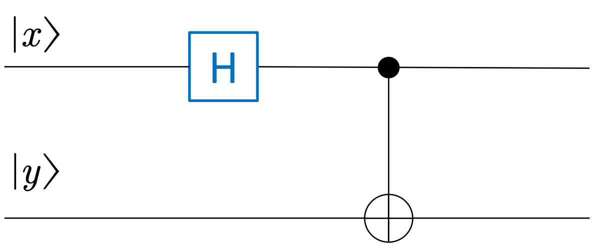
- Objective
  - Communicate a two-bit message via a qubit



Source: https://en.wikipedia.org/wiki/Superdense_coding

4. Superdense Coding

- Preliminary
  - Bell circuit and Bell basis



Example: $|00\rangle \mapsto |\Phi^+\rangle$

$$\text{CNOT} \cdot (H|0\rangle \otimes |0\rangle) = \text{CNOT} \cdot \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right)$$

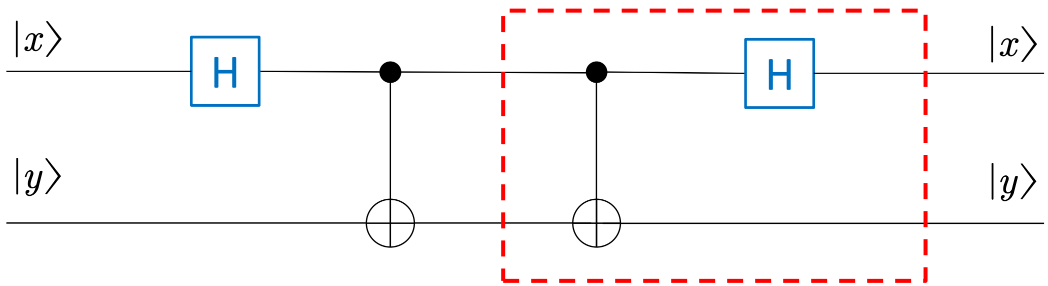
$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle$$

$$|0_A 0_B\rangle \mapsto |\Phi^+\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \quad \text{and} \quad |1_A 0_B\rangle \mapsto |\Phi^-\rangle = \frac{|0_A 0_B\rangle - |1_A 1_B\rangle}{\sqrt{2}}$$

$$|0_A 1_B\rangle \mapsto |\Psi^+\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}} \quad \text{and} \quad |1_A 1_B\rangle \mapsto |\Psi^-\rangle = \frac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}}$$

4. Superdense Coding

- Preliminary
  - Inverse Bell circuit

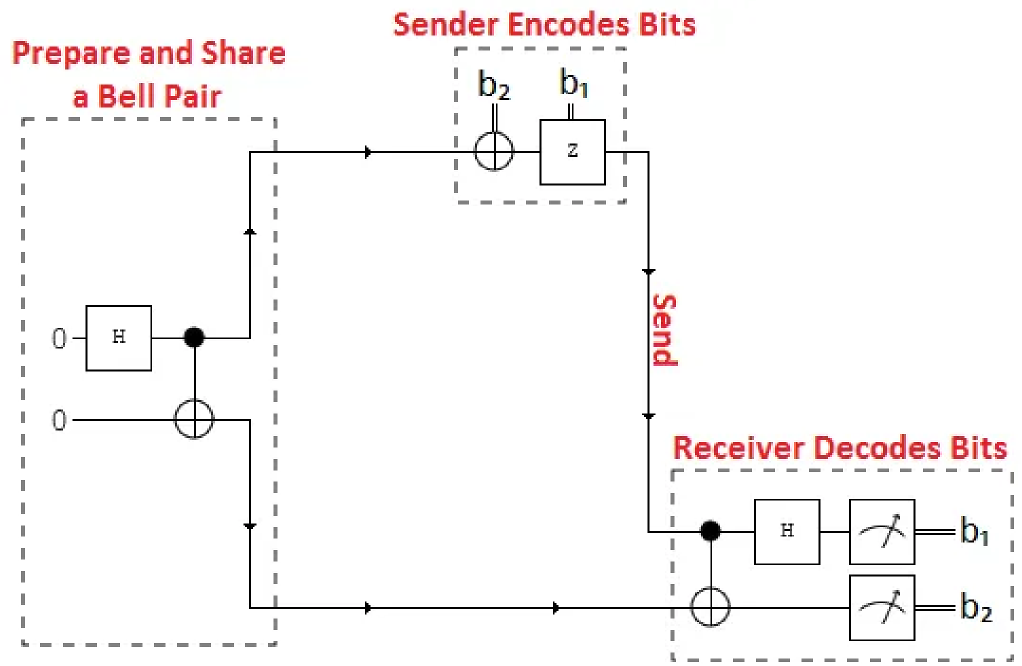


$$|\Phi^+\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \mapsto |0_A 0_B\rangle \quad \text{and} \quad |\Phi^-\rangle = \frac{|0_A 0_B\rangle - |1_A 1_B\rangle}{\sqrt{2}} \mapsto |1_A 0_B\rangle$$

$$|\Psi^+\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}} \mapsto |0_A 1_B\rangle \quad \text{and} \quad |\Psi^-\rangle = \frac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}} \mapsto |1_A 1_B\rangle$$

4. Superdense Coding

- The protocol
  - preparation, sharing, encoding, sending, and decoding

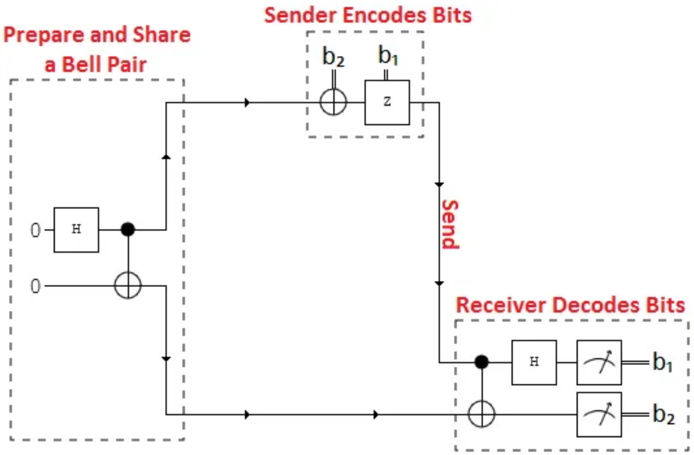


Source: https://en.wikipedia.org/wiki/Superdense_coding

4. Superdense Coding

- Step 1: Preparation
  - The protocol starts with the preparation of an entangled state, which is later shared between Alice and Bob

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

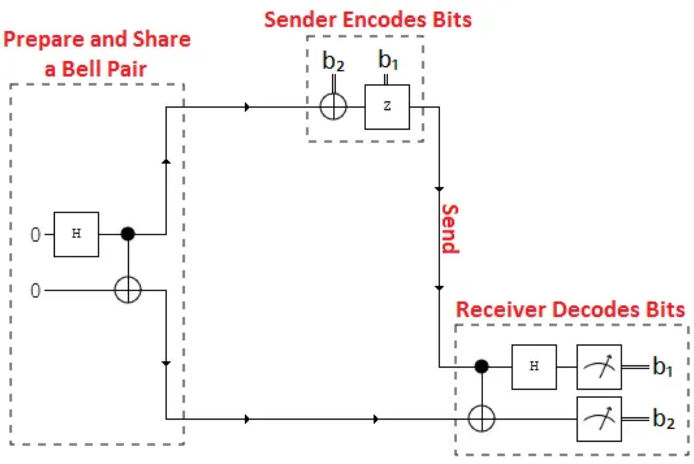


Source: https://en.wikipedia.org/wiki/Superdense_coding

4. Superdense Coding

- Step 2: Sharing
  - The qubit denoted by subscript A is sent to Alice and the qubit denoted by subscript B is sent to Bob

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

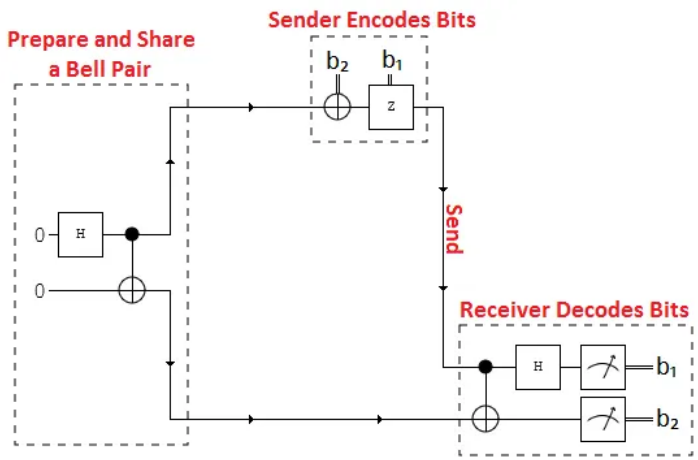


Source: https://en.wikipedia.org/wiki/Superdense_coding

4. Superdense Coding

- Step 3: Encoding
  - Alice can transform the entangled state $|\Phi^+\rangle$ into any of the four Bell states (including, of course $|\Phi^+\rangle$)

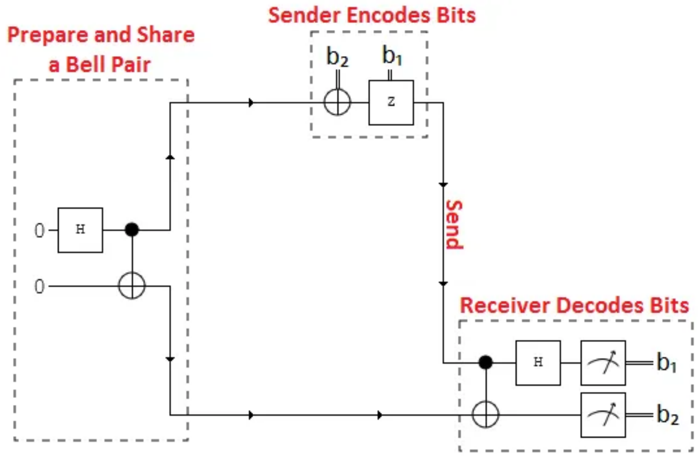
Intended Message	Applied Gate	Resulting State ($\cdot\sqrt{2}$)
00	I	$\|00\rangle + \|11\rangle$
10	X	$\|01\rangle + \|10\rangle$
01	Z	$\|00\rangle - \|11\rangle$
11	ZX	$-\|01\rangle + \|10\rangle$



Source: https://medium.com/geekculture/understanding-superdense-coding-c10b42adecca

4. Superdense Coding

- Step 4: Sending
  - Alice send her entangled qubit to Bob using a quantum network through some conventional physical medium

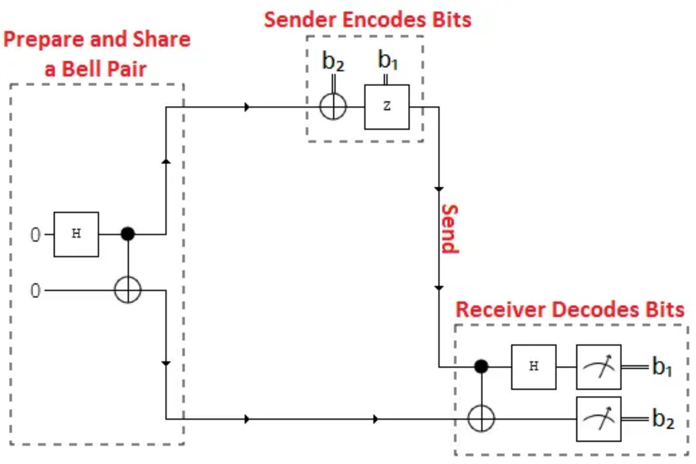


Source: https://en.wikipedia.org/wiki/Superdense_coding

4. Superdense Coding

- Step 5: Decoding
  - Bob applies the inverse Bell circuit to decode the two qubits

Bob Receives:	After CNOT-gate:	After H-gate:
$\|00\rangle + \|11\rangle$	$\|00\rangle + \|01\rangle$	$\|00\rangle$
$\|01\rangle + \|10\rangle$	$\|11\rangle + \|10\rangle$	$\|10\rangle$
$\|00\rangle - \|11\rangle$	$\|00\rangle - \|01\rangle$	$\|01\rangle$
$-\|01\rangle + \|10\rangle$	$-\|11\rangle + \|10\rangle$	$\|11\rangle$



Source: https://medium.com/geekculture/understanding-superdense-coding-c10b42adecca

4. Superdense Coding

- Discussion
  - Secure quantum communication
    - without access to Bob's qubit, Eve is unable to get any information from Alice's qubit
    - an attempt to measure either qubit would collapse the state of that qubit and alert Bob and Alice

Source: https://en.wikipedia.org/wiki/Superdense_coding

补充材料

- 量子隐形传态 vs. 超密编码

量子通讯	中间媒介 （Alice -> Bob）	传递对象 （Bob）
量子隐形传态	（2个）经典比特	（1个）量子比特
超密编码	（1个）量子比特	（2个）经典比特

Conclusion

- Classic cryptography
  - private-key cryptography
  - Key exchange
- Quantum key exchange（量子保密通讯）
  - BB84 protocol
  - B92 protocol
  - EPR protocol
- Quantum teleportation（量子隐形传态）
  - Canonical and non-canonical bases
  - The protocol: entanglement, interaction, measurement, reconstruction
- Superdense coding （超密编码）
  - Inverse bell circuit
  - The protocol: entanglement, sharing, encoding, sending, decoding