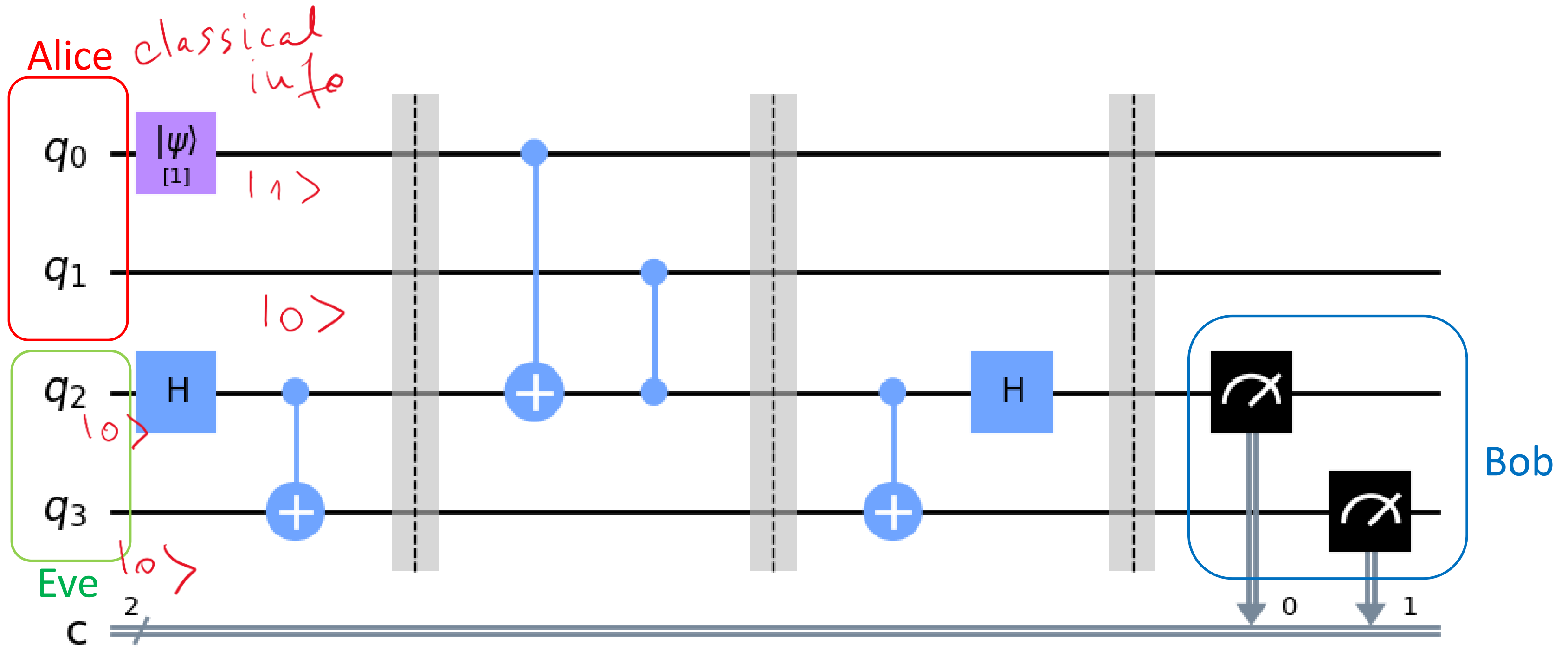
Embracing the quantum future: fundamental training for UPT students

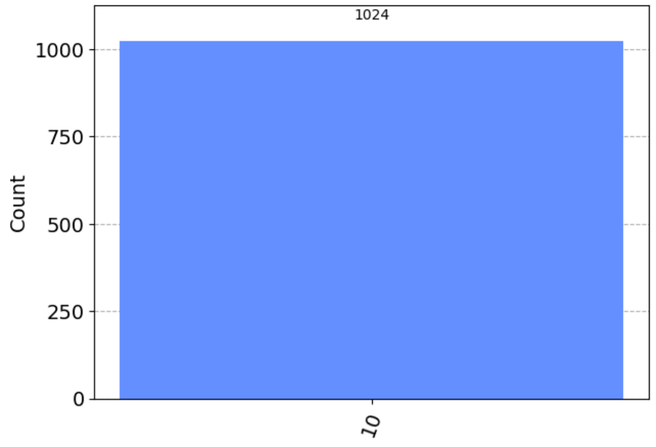
Entanglement, Teleportation and Quantum Cryptography

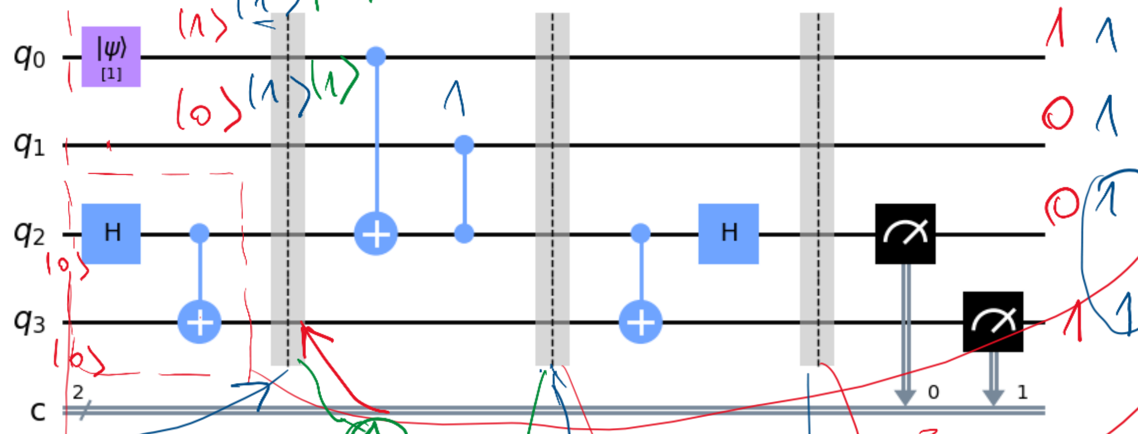
Mihai Udrescu (UPT)

Superdense coding

- A qubit potentially has infinite information (i.e., analog amplitudes)
- How much information can we send with a qubit?







$$\frac{1}{\sqrt{2}}(|11000\rangle + |11010\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|11000\rangle + |11011\rangle)$$

$$\frac{1}{\sqrt{2}}(|11010\rangle + |11001\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|11010\rangle + |11001\rangle)$$

$$\frac{1}{\sqrt{2}}(|11011\rangle + |11001\rangle) \longmapsto \frac{1}{2}(|11001\rangle - \cancel{|11011\rangle} + |11001\rangle + \cancel{|11011\rangle}) = |11001\rangle$$

$\to |11000\rangle$

$H\,|0\rangle \longmapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$H: |1\rangle \longmapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$|10\rangle \to |01\rangle$

$|11\rangle \to |11\rangle$

$$\frac{1}{\sqrt{2}}(|1100\rangle + |1111\rangle)$$

$$\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{array}\right] \quad \begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |10\rangle \\ |11\rangle \to -|11\rangle \end{array}$$

$$\to \frac{1}{\sqrt{2}}(|1110\rangle + |1101\rangle) \to \frac{1}{\sqrt{2}}(|1101\rangle - |1110\rangle)$$

$$\frac{1}{\sqrt{2}}(|1101\rangle + |1111\rangle) \to \frac{1}{2}(\cancel{|1101\rangle} + |1111\rangle + \cancel{|1101\rangle} + |1111\rangle) =$$

$= |1111\rangle$

$|01\rangle \to |10\rangle$

△ $\frac{1}{\sqrt{2}}(|0100\rangle + |0111\rangle)$

□ $\frac{1}{\sqrt{2}}(|0100\rangle - |0111\rangle)$

$$\frac{1}{\sqrt{2}}(|0100\rangle - |0110\rangle) \longrightarrow \frac{1}{2}(\cancel{|0100\rangle} + |0110\rangle + |0110\rangle - \cancel{|0100\rangle})$$

$= |0110\rangle$

Qubit teleportation protocol

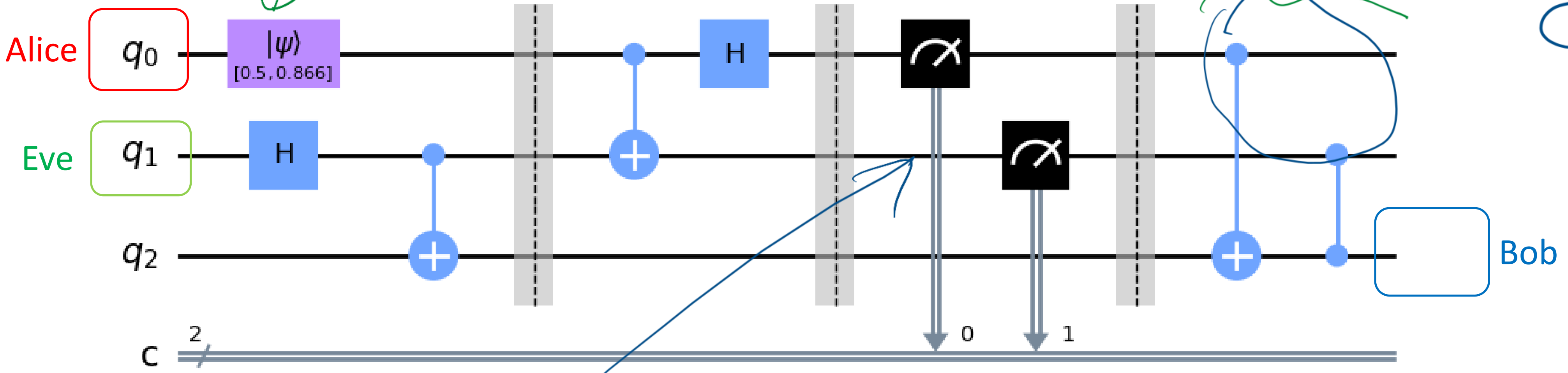
- Is qubit teleportation instantaneous?

$$\frac{1}{4} + \frac{3}{4} = \frac{4}{4}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$\left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \quad \alpha|0\rangle + \beta|1\rangle$$

? Recovery

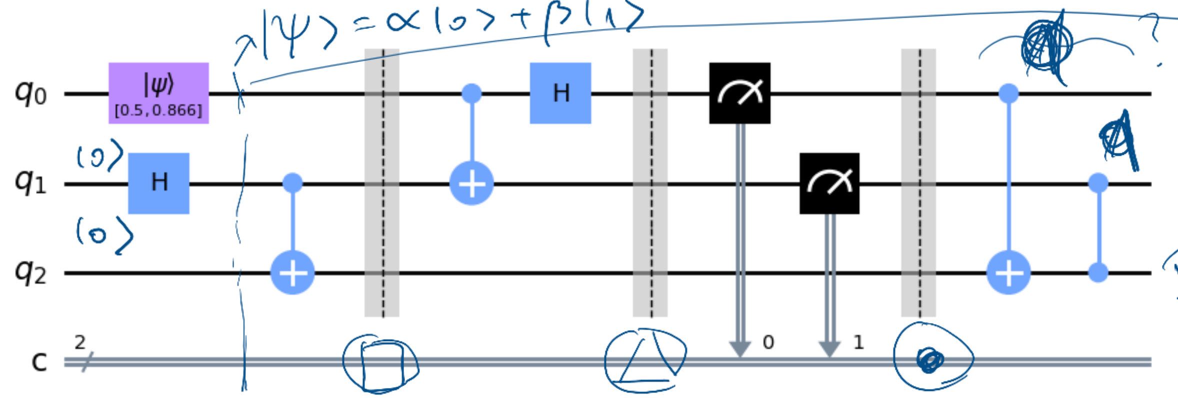


00 → $|\psi\rangle$ teleported without error

01 → $|\psi\rangle$ teleported negated

10 → $|\psi\rangle$ teleported w/ phase shift

11 → $|\psi\rangle$ teleported negated and phase sh



Bob

$$|\psi\rangle \otimes |00\rangle = \alpha|000\rangle + \beta|100\rangle$$

$$H: |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H: |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|010\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|110\rangle \longmapsto \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

$$\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle \longmapsto \frac{\alpha}{2}|000\rangle + \frac{\alpha}{2}|100\rangle + \frac{\alpha}{2}|011\rangle + \frac{\alpha}{2}|111\rangle + \frac{\beta}{2}|010\rangle - \frac{\beta}{2}|110\rangle + \frac{\beta}{2}|001\rangle - \frac{\beta}{2}|101\rangle =$$

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

measurement

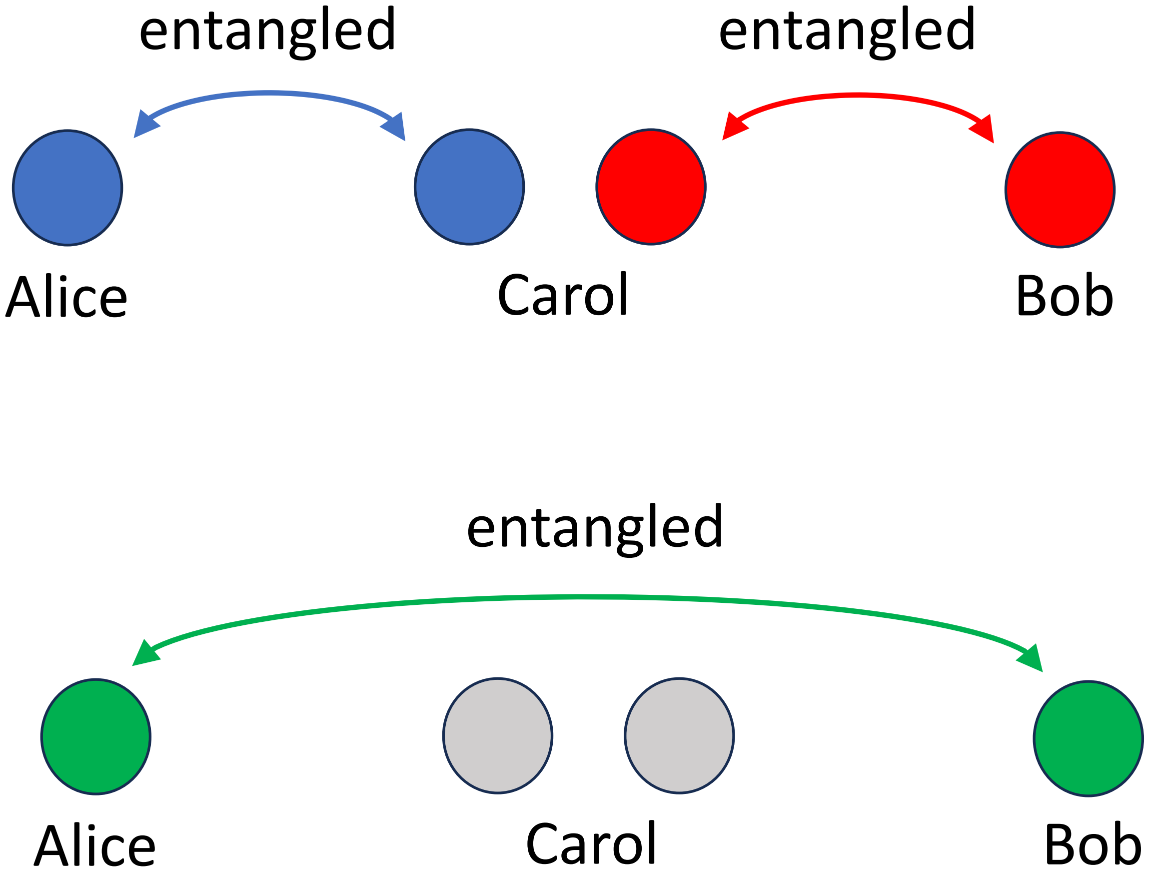
$|00\rangle$ post measurement Bob: $|\psi\rangle$

$|01\rangle \longmapsto \alpha|1\rangle + \beta|0\rangle$

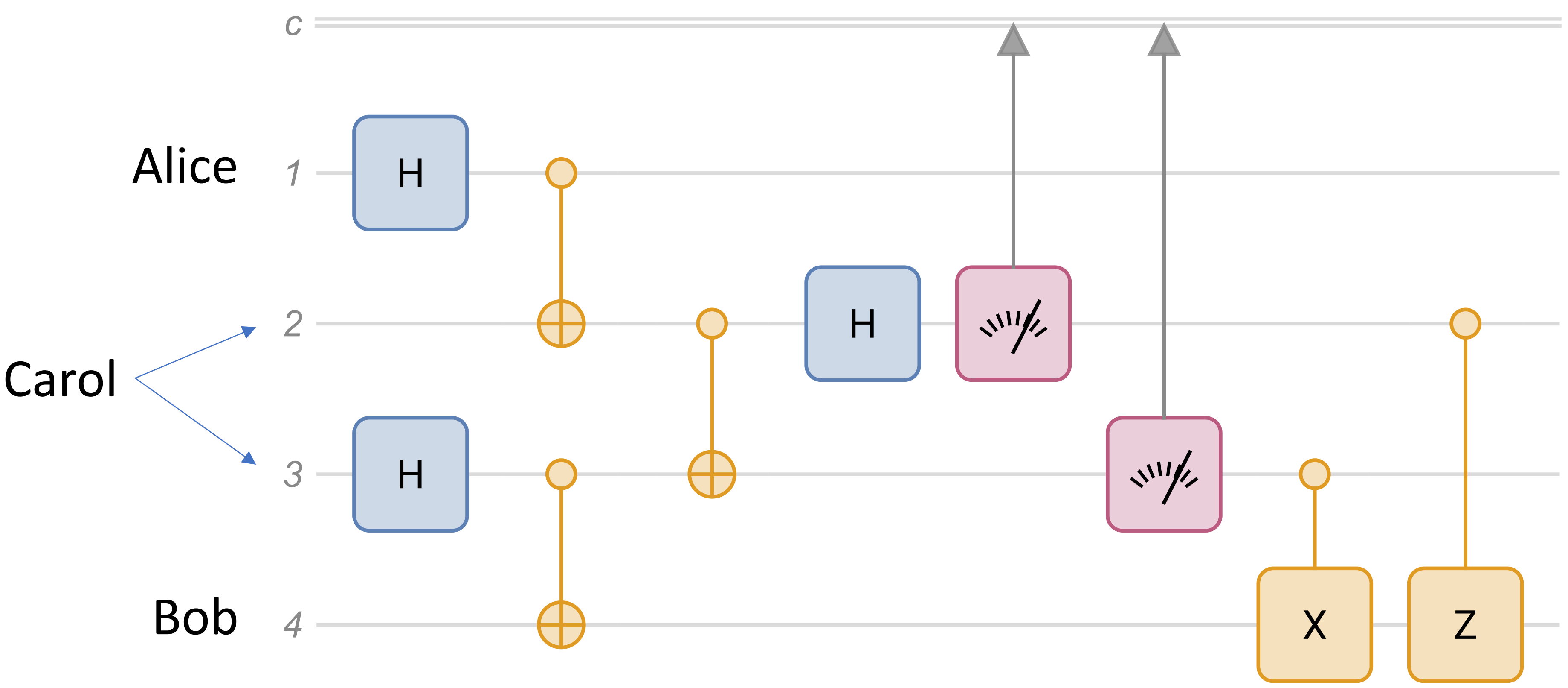
$|10\rangle \longmapsto \alpha|0\rangle - \beta|1\rangle$

$|11\rangle \longmapsto \alpha|1\rangle - \beta|0\rangle$

Entanglement distribution & swapping

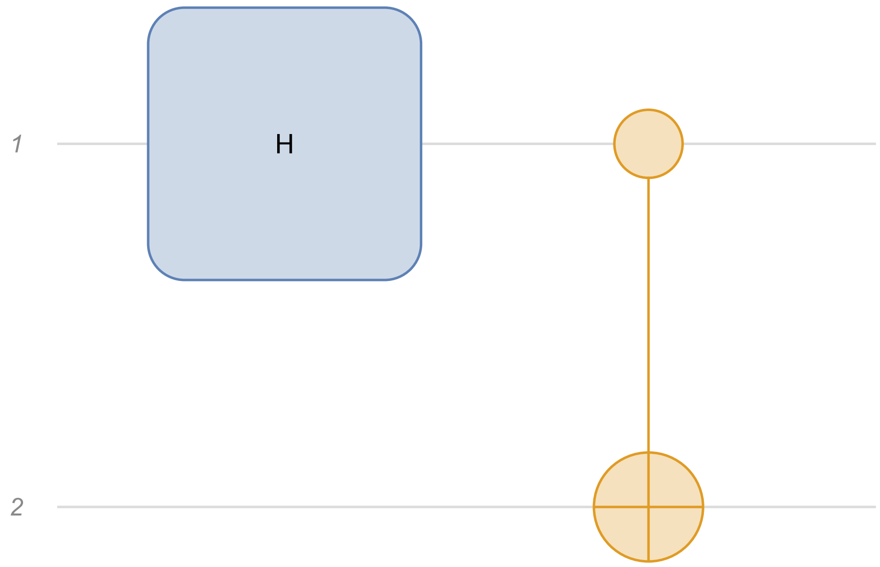


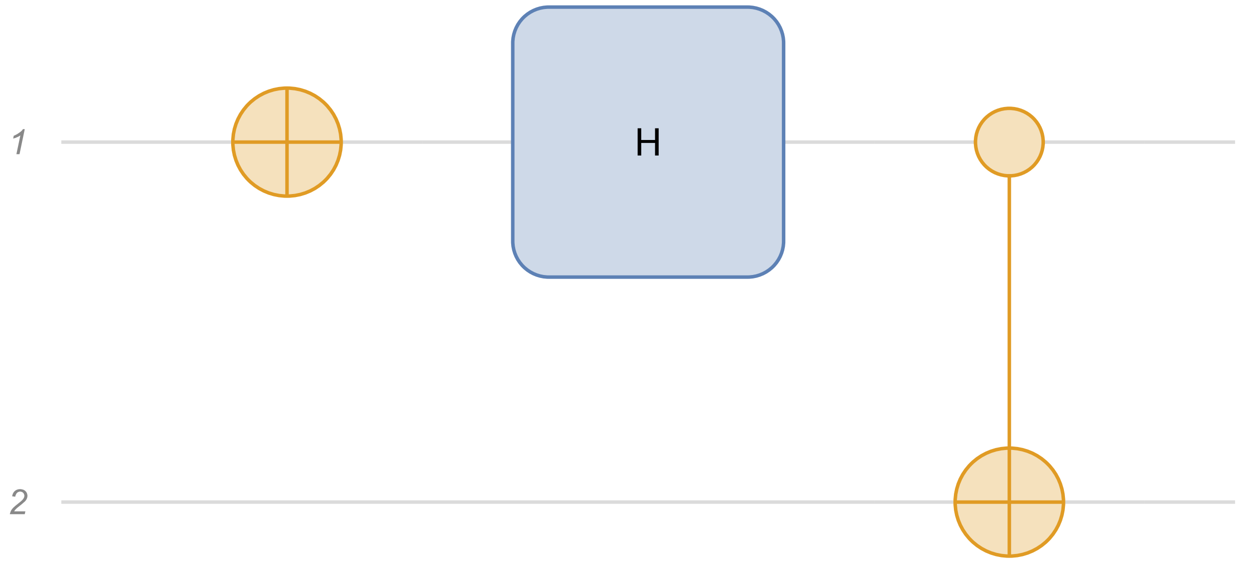
Entanglement swapping circuit



Entanglement swapping circuit

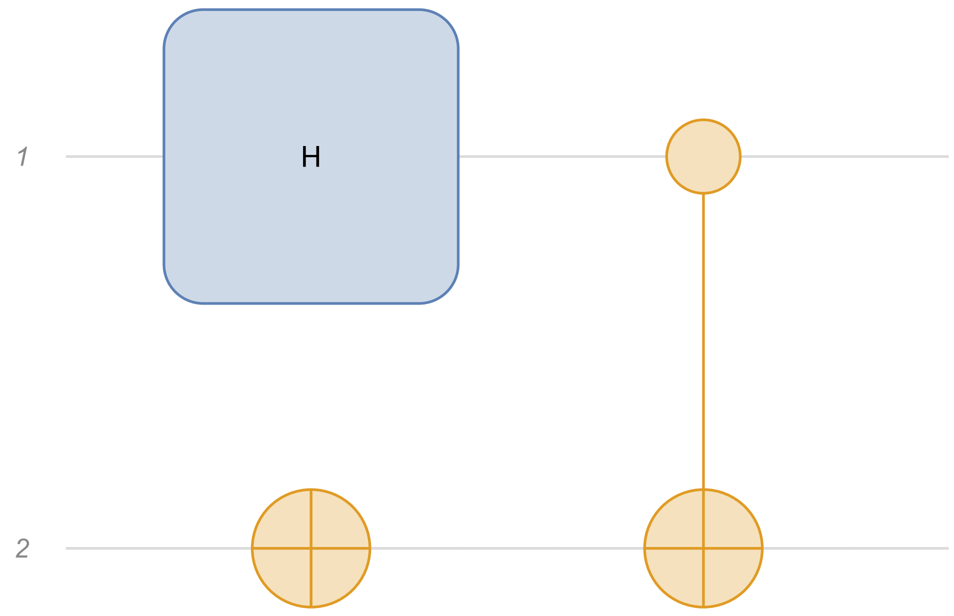
- Bell states
- $|\phi_+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$; $|\phi_-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$

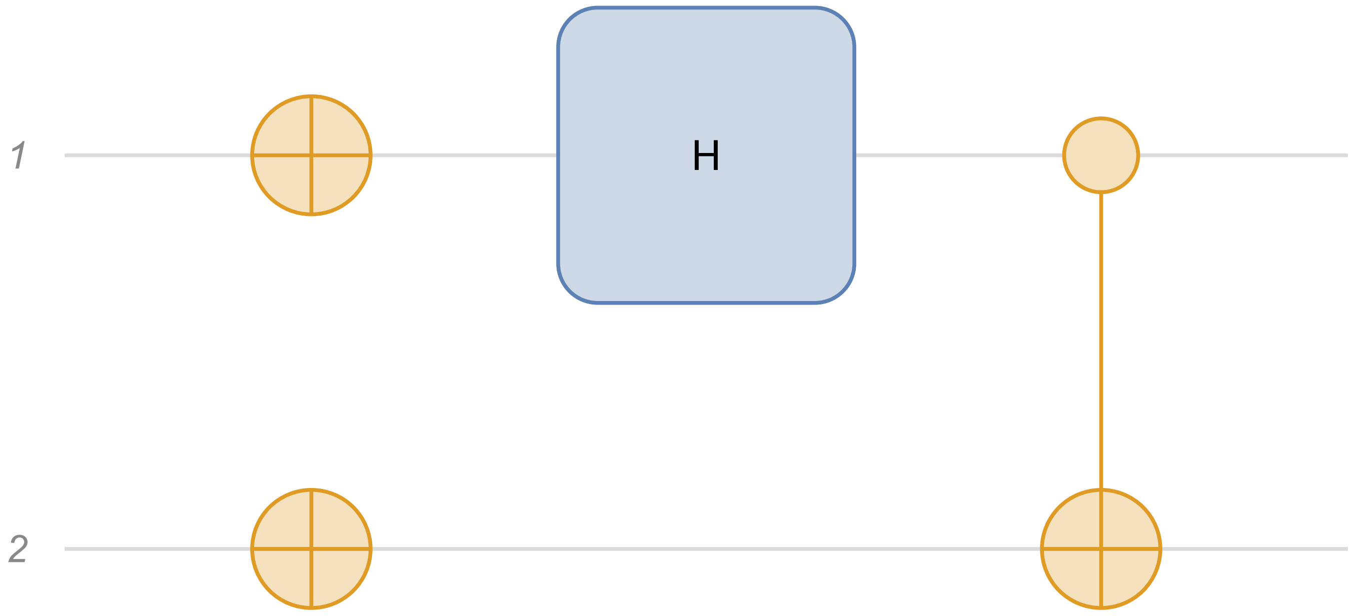




Entanglement swapping circuit

- Bell states
- $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$; $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$





Entanglement swapping circuit

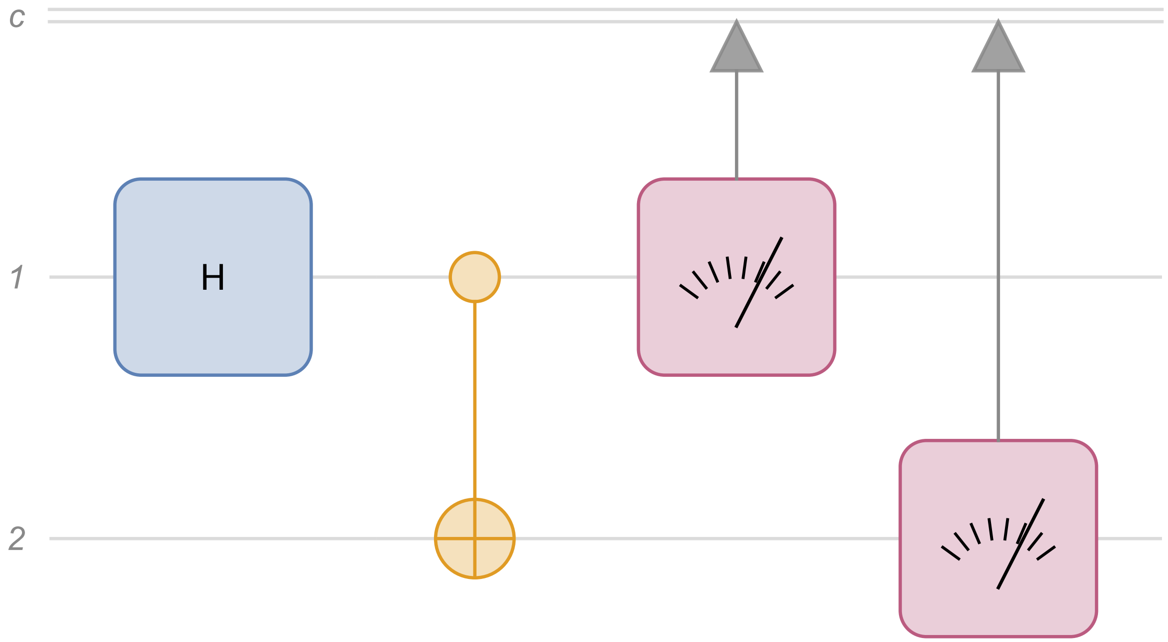
- Bell states analyzer

$|\phi_+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

$|\phi_-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$

$|\psi_+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$

$|\psi_-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$



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

Entanglement swapping circuit

- Bell state converter

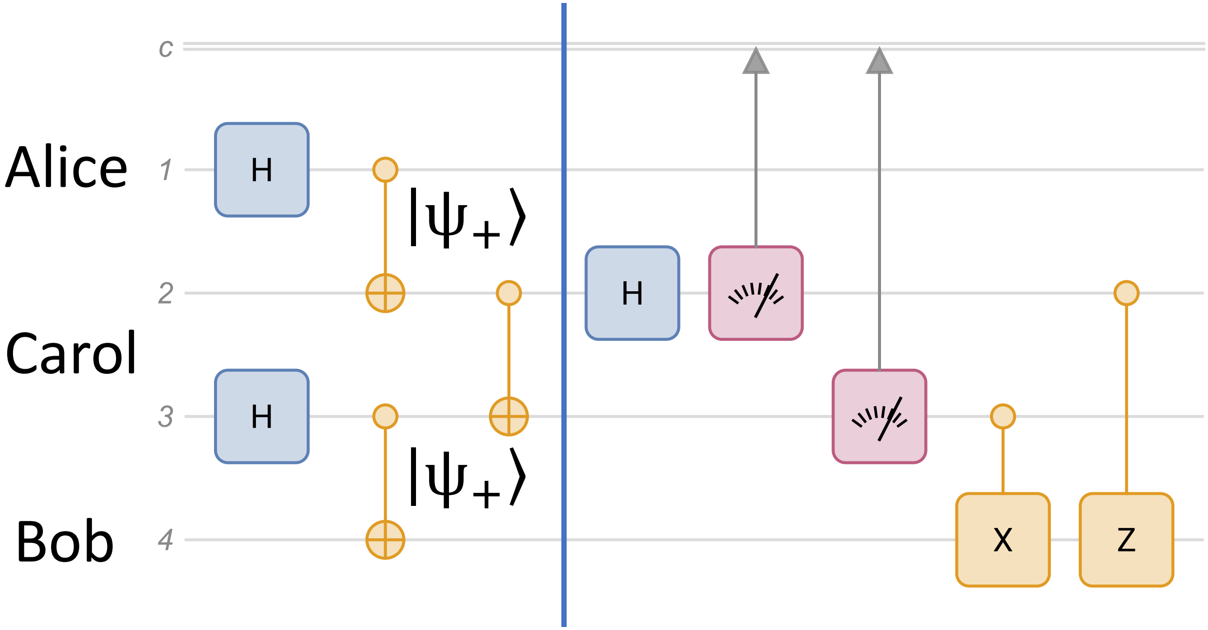
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$I \otimes Z|\phi_-\rangle = |\phi_+\rangle$$

$$I \otimes X\,|\psi_+\rangle = |\phi_+\rangle$$

$$I \otimes (XZ)\,|\psi_-\rangle = |\phi_+\rangle$$

Entanglement swapping circuit



$$|\phi_+\rangle + |\phi_-\rangle = \sqrt{2}\,|00\rangle \Rightarrow |00\rangle = \tfrac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle)$$

$$|11\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle - |\phi_-\rangle)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle + |\psi_-\rangle)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle - |\psi_-\rangle)$$

$$\tfrac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_{C1} + |1\rangle_A|1\rangle_{C1}\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle_{C2}|0\rangle_B + |1\rangle_{C2}|1\rangle_B\right)$$

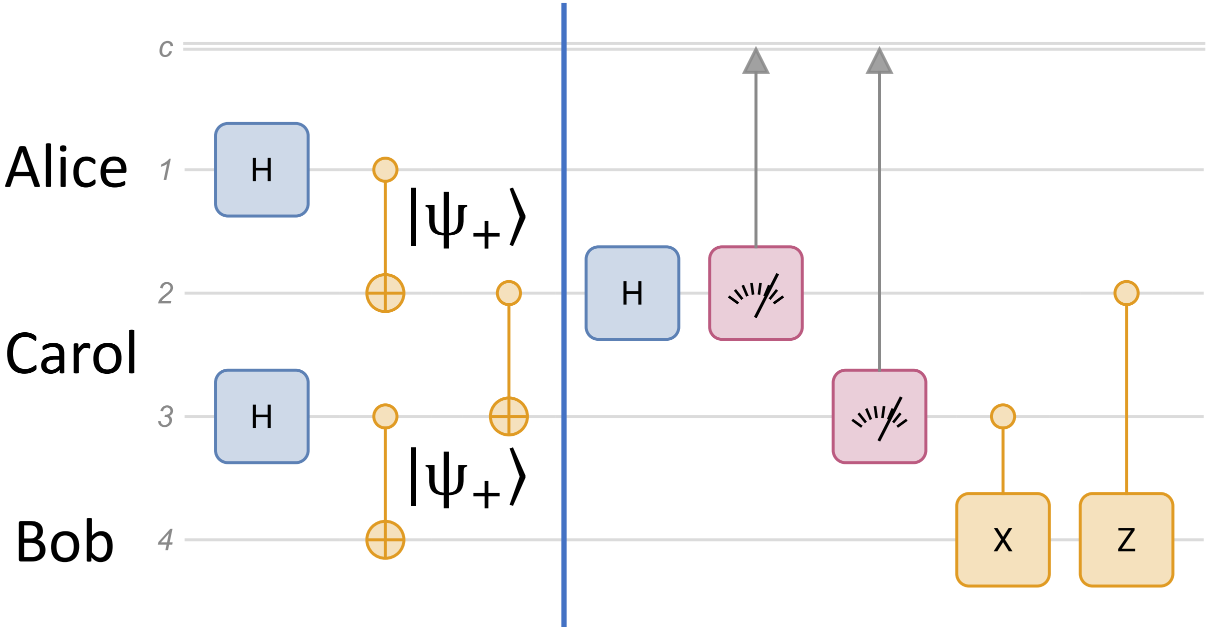
$$= \tfrac{1}{2}\left(|0\rangle_A|0\rangle_{C1}|0\rangle_{C2}|0\rangle_B + |0\rangle_A|0\rangle_{C1}|1\rangle_{C2}|1\rangle_B + |1\rangle_A|1\rangle_{C1}|0\rangle_{C2}|0\rangle_B + |1\rangle_A|1\rangle_{C1}|1\rangle_{C2}|1\rangle_B\right)$$

$$= \tfrac{1}{2}\left(|0\rangle_A|0\rangle_B|0\rangle_{C1}|0\rangle_{C2} + |0\rangle_A|1\rangle_B|0\rangle_{C1}|1\rangle_{C2} + |1\rangle_A|0\rangle_B|1\rangle_{C1}|0\rangle_{C2} + |1\rangle_A|1\rangle_B|1\rangle_{C1}|1\rangle_{C2}\right)$$

$$= \tfrac{1}{2}\left(|0\rangle_A|0\rangle_B|0\rangle_{C1}|0\rangle_{C2} + |0\rangle_A|1\rangle_B|0\rangle_{C1}|1\rangle_{C2} + |1\rangle_A|0\rangle_B|1\rangle_{C1}|0\rangle_{C2} + |1\rangle_A|1\rangle_B|1\rangle_{C1}|1\rangle_{C2}\right)$$

$$= \tfrac{1}{4}\Big((|\phi_+\rangle_{AB}+|\phi_-\rangle_{AB})(|\phi_+\rangle_{C1C2}+|\phi_-\rangle_{C1C2}) + (|\psi_+\rangle_{AB}+|\psi_-\rangle_{AB})(|\psi_+\rangle_{C1C2}+|\psi_+\rangle_{C1C2}) +$$
$$(|\psi_+\rangle_{AB}-|\psi_-\rangle_{AB})(|\psi_+\rangle_{C1C2}-|\psi_+\rangle_{C1C2}) + (|\phi_+\rangle_{AB}-|\phi_-\rangle_{AB})(|\phi_+\rangle_{C1C2}-|\phi_-\rangle_{C1C2})\Big)$$

Entanglement swapping circuit



$$|\phi_+\rangle + |\phi_-\rangle = \sqrt{2}\,|00\rangle \Rightarrow |00\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle)$$

$$|11\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle - |\phi_-\rangle)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle + |\psi_-\rangle)$$

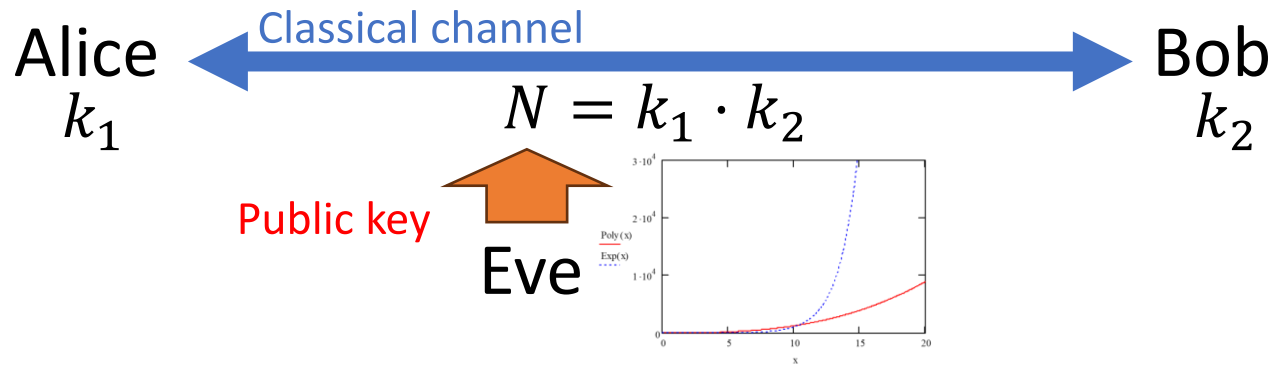
$$|10\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle - |\psi_-\rangle)$$

$$\frac{1}{2}\left(|\phi_+\rangle_{AB}|\phi_+\rangle_{C1C2} + |\phi_-\rangle_{AB}|\phi_-\rangle_{C1C2} + |\psi_+\rangle_{AB}|\psi_+\rangle_{C1C2} + |\psi_-\rangle_{AB}|\psi_-\rangle_{C1C2}\right)$$

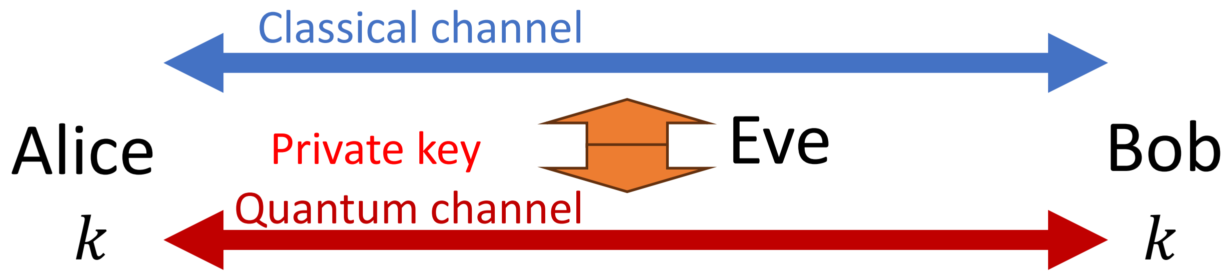
$$\xrightarrow{\text{Bell analyzer C1C2}} \begin{cases} 00 \text{ with } |\phi_+\rangle_{AB} \\ 01 \text{ with } |\psi_+\rangle_{AB} \\ 10 \text{ with } |\phi_-\rangle_{AB} \\ 11 \text{ with } |\psi_-\rangle_{AB} \end{cases}$$

Quantum key distribution

- The BB84 protocol: Charles Bennett and Gilles Brassard, 1984
- Conventional cryptography – public key



- QKD communication



BB84: useful quantum properties

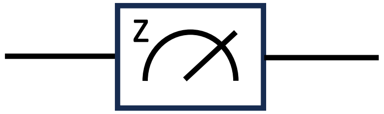
- Qubit basis-z (computational): $\{|0\rangle, |1\rangle\}$
- Qubit basis-x: $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\} = \{|+\rangle, |-\rangle\}$
- Basis transformation

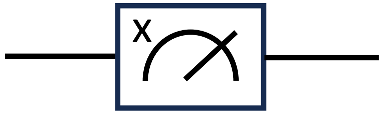
$$|0\rangle \; \text{—}\boxed{H}\text{—} \; \boxed{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)} \; \text{—}\boxed{H}\text{—} \; |0\rangle$$

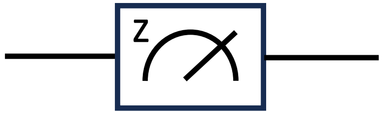
$$|1\rangle \; \text{—}\boxed{H}\text{—} \; \boxed{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)} \; \text{—}\boxed{H}\text{—} \; |1\rangle$$

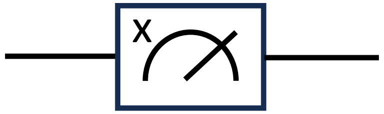
BB84: useful quantum properties

- Measurement in z and x bases

$|0\rangle$  $|0\rangle$

$|0\rangle$  $\begin{cases} |+\rangle \text{ prob. } 0.5 \\ |-\rangle \text{ prob. } 0.5 \end{cases}$

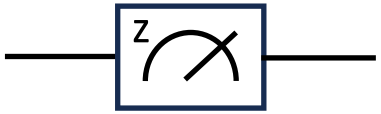
$|1\rangle$  $|1\rangle$

$|1\rangle$  $\begin{cases} |+\rangle \text{ prob. } 0.5 \\ |-\rangle \text{ prob. } 0.5 \end{cases}$

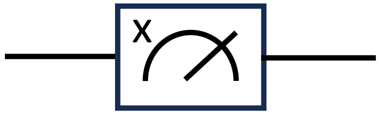
$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \qquad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

BB84: useful quantum properties

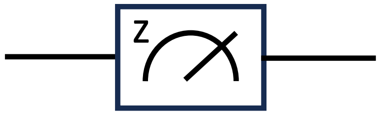
- Measurement in z and x bases

$|+\rangle$ 

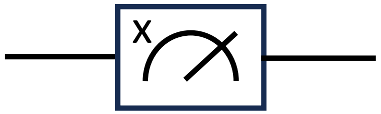
$\begin{cases} |0\rangle \text{ prob. } 0.5 \\ |1\rangle \text{ prob. } 0.5 \end{cases}$

$|+\rangle$ 

$|+\rangle$

$|-\rangle$ 

$\begin{cases} |0\rangle \text{ prob. } 0.5 \\ |1\rangle \text{ prob. } 0.5 \end{cases}$

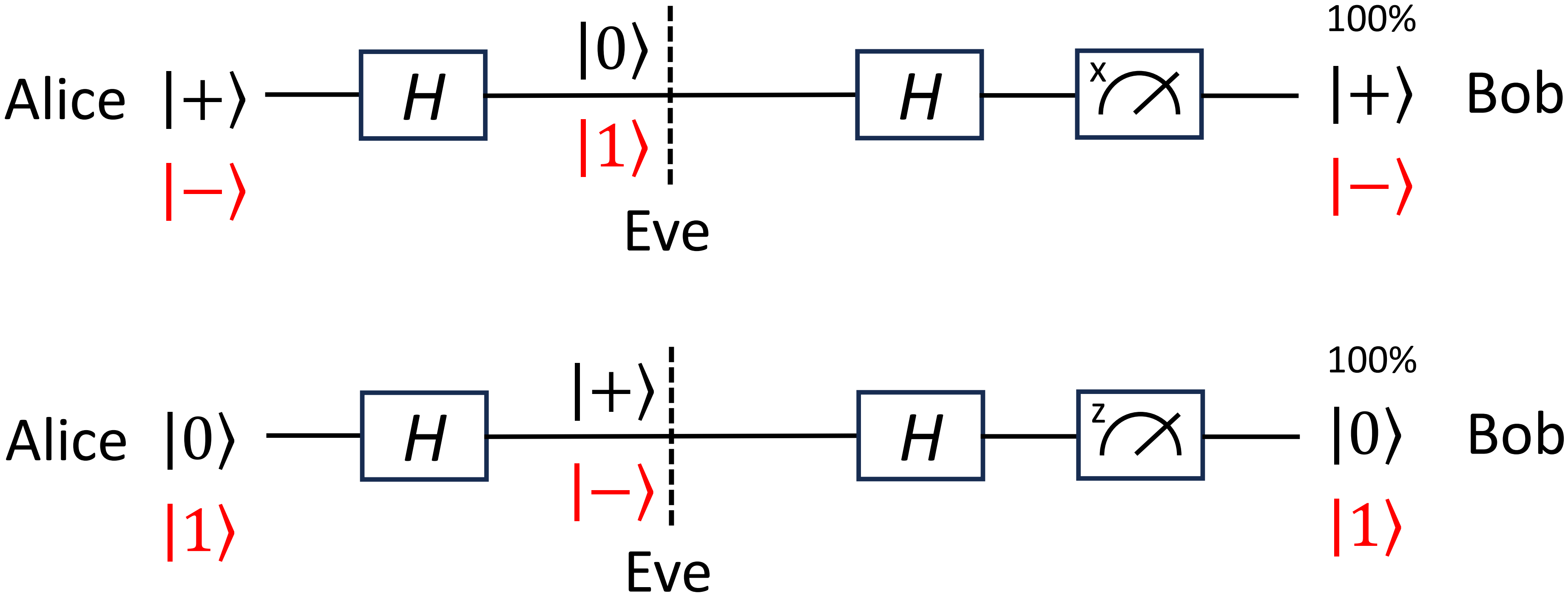
$|-\rangle$ 

$|-\rangle$

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

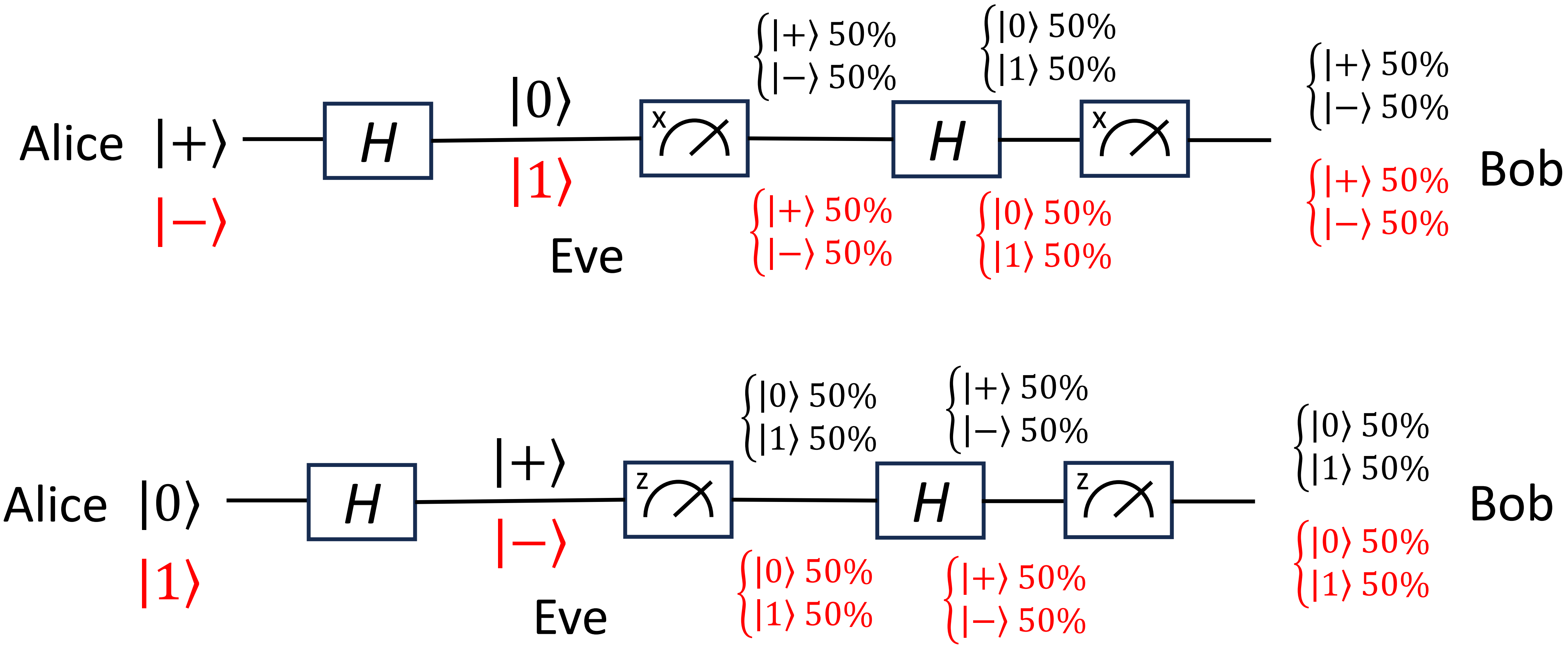
BB84: useful quantum properties

- Information transmission – no attack



BB84: useful quantum properties

- Information transmission – attack



BB84: the protocol

- **Step 1** Alice choses a string of bits (at random) and a basis for each bit (also at random, encoded as Z → 0, X → 1); she keeps the two pieces of info for herself

  1000 1010 1101 0100 (bits)

  ZZXZ XXXZ XZXX XXXX (basis)

  0010 1110 1011 1111 (basis encoded)

- **Step 2** Alice encodes the info (each bit in its respective basis)

  $|1\rangle|0\rangle|+\rangle|0\rangle \;\; |-\rangle|+\rangle|-\rangle|0\rangle \;\; |-\rangle|1\rangle|+\rangle|-\rangle \;\; |+\rangle|-\rangle|+\rangle|+\rangle$

  This is the message that Alice sends to Bob

BB84: the protocol

- **Step 3** Bob measures the qubits received from Alice – each on a random basis

$|1\rangle|0\rangle|+\rangle|0\rangle\ \ |-\rangle|+\rangle|-\rangle|0\rangle\ \ |-\rangle|1\rangle|+\rangle|-\rangle\ \ |+\rangle|-\rangle|+\rangle|+\rangle$ (received)

X Z Z Z X Z X Z X Z X Z Z Z X Z (random basis)

=> $|?\rangle|0\rangle|?\rangle|0\rangle\ \ |-\rangle|?\rangle|-\rangle|0\rangle\ \ |-\rangle|1\rangle|+\rangle|?\rangle\ \ |?\rangle|?\rangle|+\rangle|?\rangle$

$$|?\rangle = \begin{cases} |+\rangle\ 50\% \\ |-\rangle\ 50\% \end{cases} \qquad |?\rangle = \begin{cases} |0\rangle\ 50\% \\ |1\rangle\ 50\% \end{cases}$$

Bob stores this information

- **Step 4** Bob and Alice publicly share which basis they used for each qubit

BB84: the protocol

- **Step 4** Bob and Alice publicly share which basis they used for each qubit

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Z	Z	X	Z	X	X	X	Z	X	Z	X	X	X	X	X	X	Alice's basis
X	Z	Z	Z	X	Z	X	Z	X	Z	X	Z	Z	Z	X	Z	Bob's basis

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	Alice's bits
$\|?\rangle$	$\|0\rangle$	$\|?\rangle$	$\|0\rangle$	$\|-\rangle$	$\|?\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|?\rangle$	$\|?\rangle$	$\|?\rangle$	$\|+\rangle$	$\|?\rangle$	Bob's qubits

0 0 1 1 0 1 1 0 0 (Alice's key)

0 0 $-$ $-$0 $-$ 1 + + (Bob's key)

$|0\rangle \rightarrow 0$ $\quad |1\rangle \rightarrow 1$

$|+\rangle \rightarrow 0$ $\quad |-\rangle \rightarrow 1$

BB84: the protocol

- **Step 5** Alice and Bob share a random sample of their keys; if they match, they can be sure that their transmission is safe

Eve has a low probability of guessing the resulting key

QKD networks

- [1991] John Rarity, Paul Tapster and Artur Ekert, UK Defence Research Agency and Oxford University, demonstrated QKD
- [2007] Los Alamos National Laboratory/NIST achieved quantum key distribution over a 148.7 km of optic fibre using the BB84 protocol
- [2022] EuroQCI (European Quantum Communication Infrastructure) Initiative

Quantum Experiments at Space Scale - QUESS

- 2017: BB84 was successfully implemented over satellite links from Micius to ground stations in China and Austria.
- The keys were combined and the result was used to transmit images and video between Beijing, China, and Vienna, Austria.
- Photons were sent from one ground station to the satellite Micius and back down to another ground station, along a “summed length varying from 1600 to 2400 kilometers”