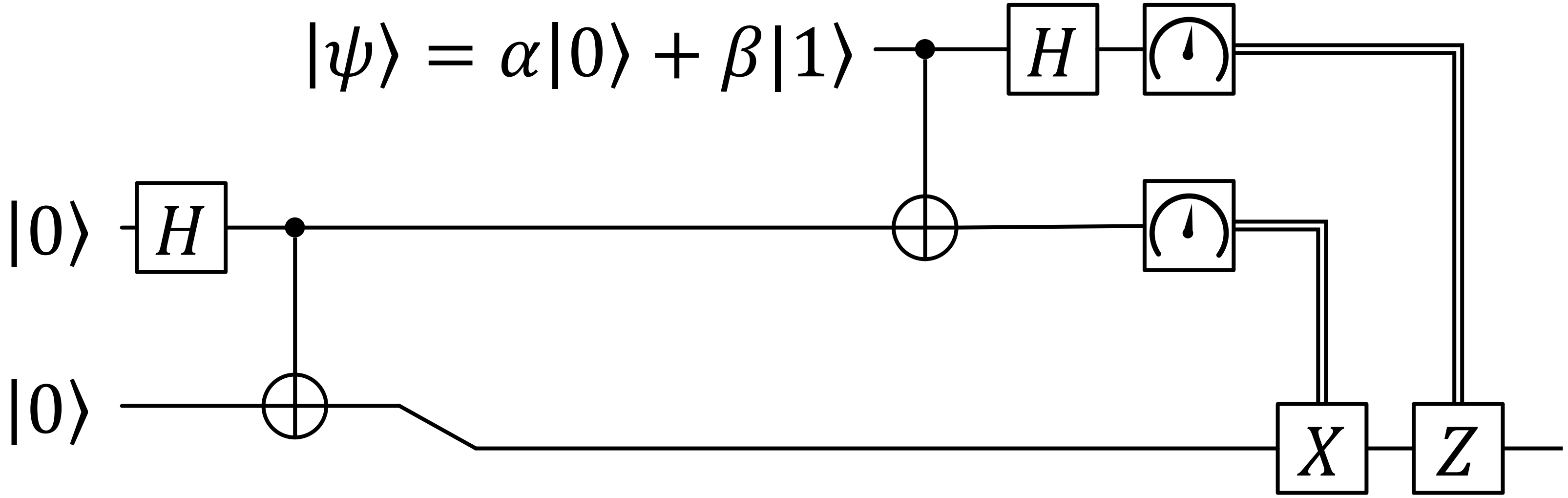
Quantum Communication Algorithms



Mariia Mykhailova
Principal Software Engineer
Microsoft Quantum Systems

Lecture outline

No-cloning and no-deleting theorems

Quantum key distribution: BB84 protocol

Teleportation

Superdense coding

No-cloning and no-deleting theorems

No-cloning theorem

Can we copy an arbitrary unknown state of a qubit?

Let's assume there is a unitary "clone" transformation C that starts with a state $|s\rangle$ and clones an arbitrary state onto it:

$$C(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$C(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Let's take inner product of these equations:

Inner product of left sides $$(\langle\varphi| \otimes \langle s|)C^{\dagger}C(|\psi\rangle \otimes |s\rangle) = \langle\varphi|\psi\rangle$$

$$\langle\varphi| \otimes \langle\varphi||\psi\rangle \otimes |\psi\rangle = \langle\varphi|\psi\rangle^2$$ Inner product of right sides

$$\langle\varphi|\psi\rangle^2 = \langle\varphi|\psi\rangle$$

Our assumed cloning only works on orthogonal ($\langle\varphi|\psi\rangle = 0$) or identical ($\langle\varphi|\psi\rangle = 1$) states

No-cloning theorem vs measurements

- We can not distinguish non-orthogonal states perfectly
- And we can not clone non-orthogonal states
- How could we build a cloning device for a pair of non-orthogonal states if we were able to distinguish them?
- How could we distinguish states if we could clone them?

No-deleting theorem

If we are given two copies of an arbitrary unknown state of a qubit, can we delete one of them?

Same as the no-cloning theorem, no-deleting theorem asks for a unitary transformation that would allow us to transform one of the copies of the state into the $|0\rangle$ state.

The reasoning is exactly the same as for the no-cloning theorem, but in reversed time.

It's really easy to delete one of the states using measurements!

Microsoft

Quantum key distribution: BB84 protocol

Quantum cryptography: an overview

Quantum cryptography exploits quantum-mechanical phenomena to perform cryptographic tasks

Quantum key distribution: using quantum communication to generate a random secret key shared between two parties securely (without possibility of eavesdropping)

Mistrustful cryptography: several parties performing tasks jointly without trusting each other

- coin flipping
- commitment schemes: a party commits to a value without revealing it
- secure computations: uses data from multiple parties that is kept secret

BB84 protocol (1984, Bennet and Brassard)

Alice generates two random strings of n bits: bits and bases

- Alice prepares n qubits: qubit k is encoded in rectangular (computational) or diagonal (Hadamard) basis depending on bases[k], and it's $|0\rangle/|1\rangle$ or $|+\rangle/|-\rangle$ depending on bits[k]
- Alice sends the qubits to Bob
- Bob measures each qubit in random basis – rectangular or diagonal
- Alice and Bob compare the bases they used and discard the bits where the bases didn't match

The bits where the bases matched are equal - they form a shared secret key!

BB84 protocol: example

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Source: Quantum cryptography: Public key distribution and coin tossing
https://www.sciencedirect.com/science/article/pii/S0304397514004241

Teleportation

Teleportation: obligatory XKCD

https://xkcd.com/465/

Teleportation

Alice needs to deliver a qubit state $\alpha|0\rangle + \beta|1\rangle$ to Bob.

Alice has a qubit in this state but does not know the state.

She can only send *classical information* to Bob.

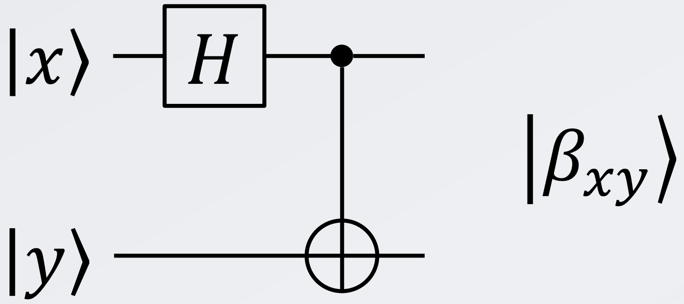
What does she do?

- **If Alice knew α and β, she could send Bob the values**
  Requires infinitely many bits for perfect precision
- **If Alice does not know α or β, she can't learn them from a single qubit**
  And cannot produce more copies of the qubit due to the no-cloning theorem!
- **What if they share an entangled pair of qubits beforehand?**

Review: Bell states (a.k.a. EPR pairs)

$$|\Phi^+\rangle = |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\Psi^+\rangle = |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Phi^-\rangle = |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\Psi^-\rangle = |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



$$|x, y\rangle \mapsto \frac{1}{\sqrt{2}}(|0, y\rangle + (-1)^x|1, \neg y\rangle)$$

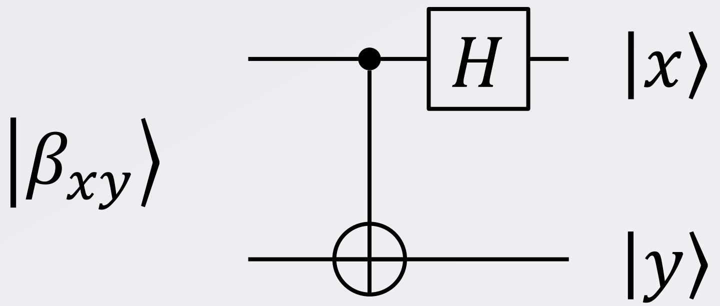
These states form *Bell basis* for 2-qubit systems

(you can check that they are normalized and pairwise orthogonal)

Review: Bell state measurements

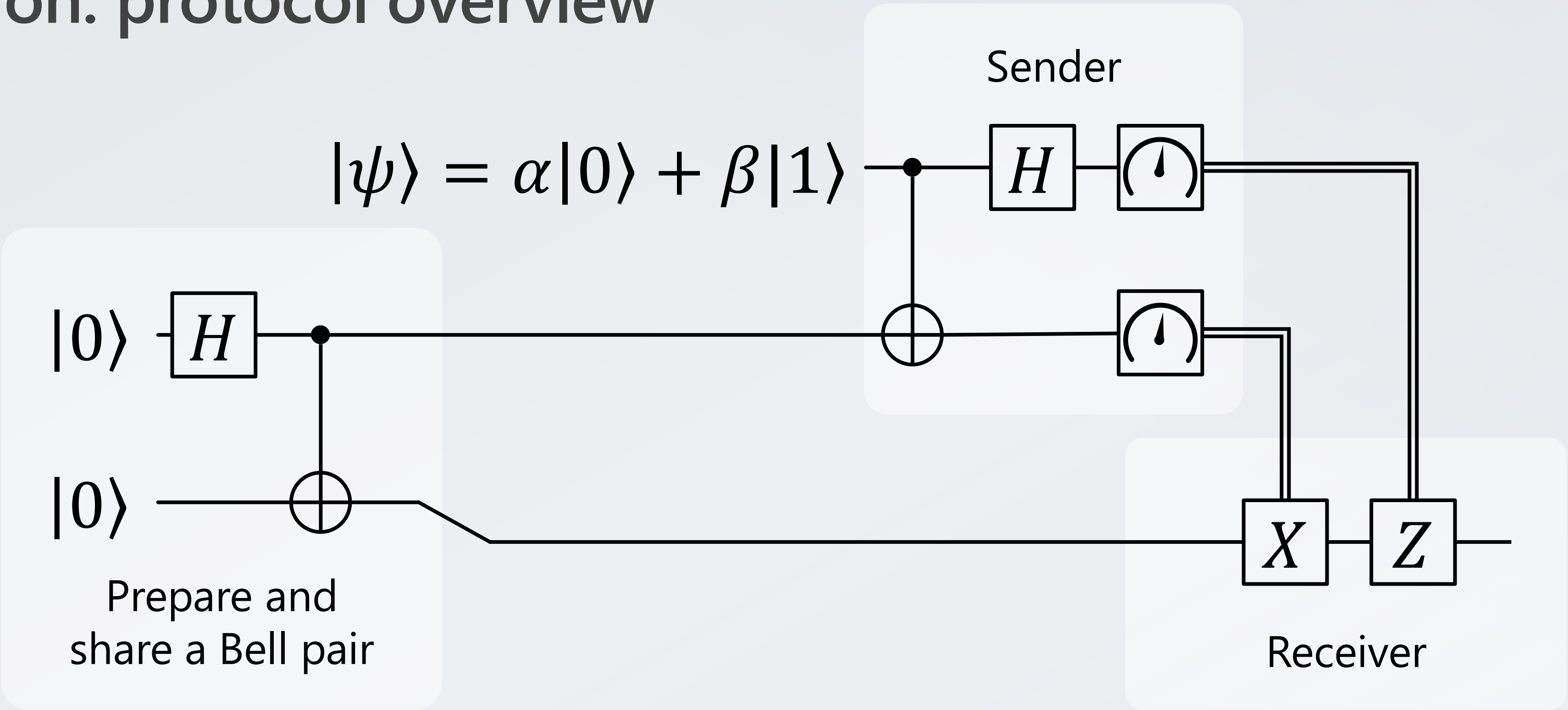
How to do a measurement in the Bell basis?

Run *adjoint* of the unitary transformation that maps the states of the computational basis to the Bell states to map Bell states back to the computational basis, and measure both qubits



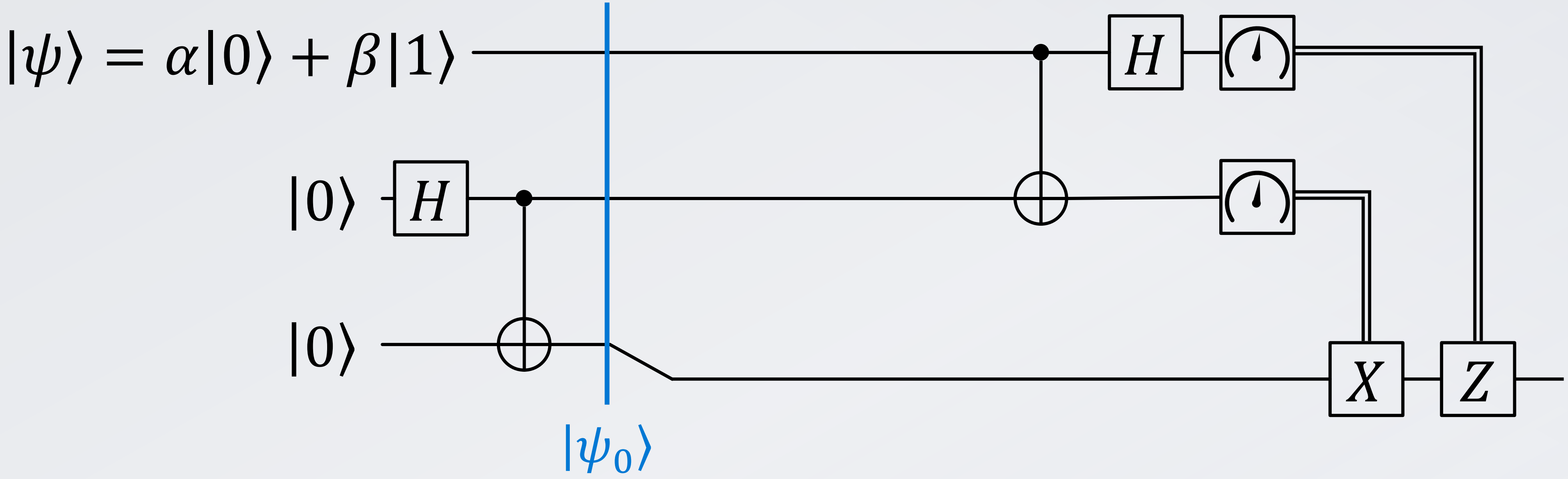
$$\frac{1}{\sqrt{2}}(|0, y\rangle + (-1)^x|1, \neg y\rangle) \mapsto |x, y\rangle$$

Teleportation: protocol overview



- Alice and Bob share a pair of entangled qubits
- Alice entangles her data qubit with her half of the pair
- Alice measures her qubits and sends the results to Bob
- Bob applies “fixup” to his half of the pair

Teleportation: setup

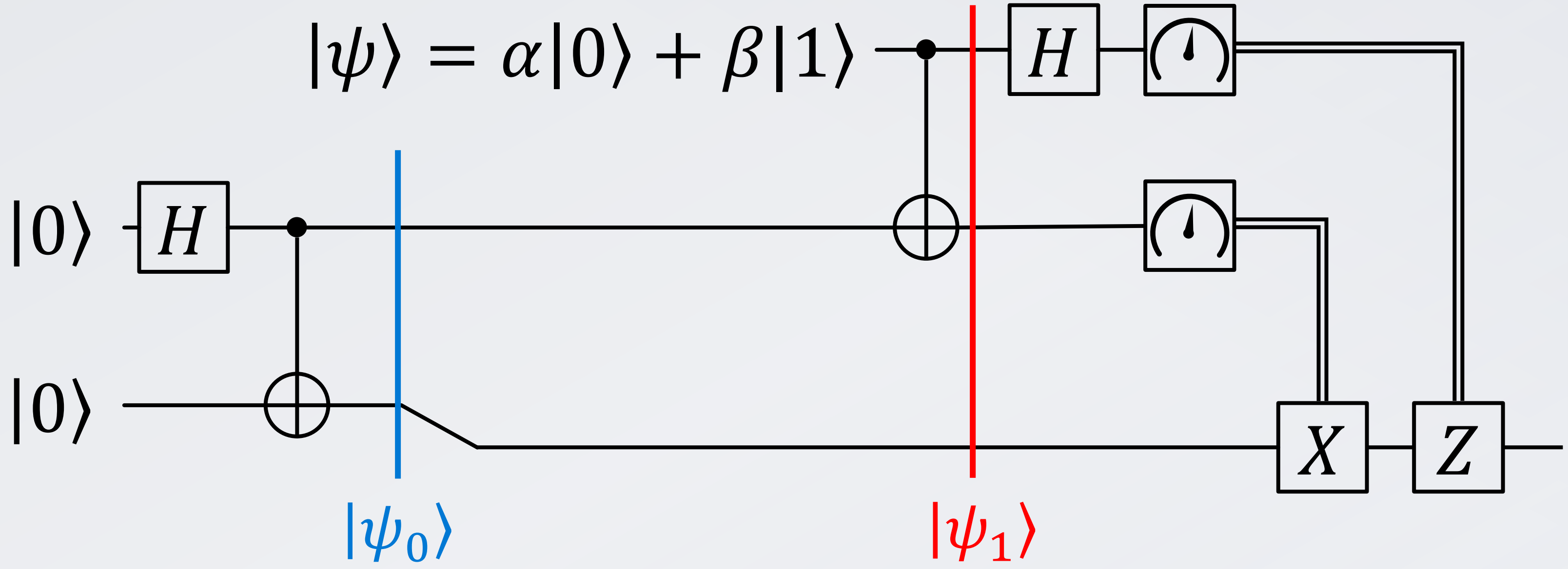


$|\psi_0\rangle$ is a union (tensor product) of two independent systems:

- Entangled pair $|\beta_{00}\rangle$ (shared between Alice and Bob)
- And Alice's data qubit $|\psi\rangle$

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\otimes\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Teleportation: CNOT

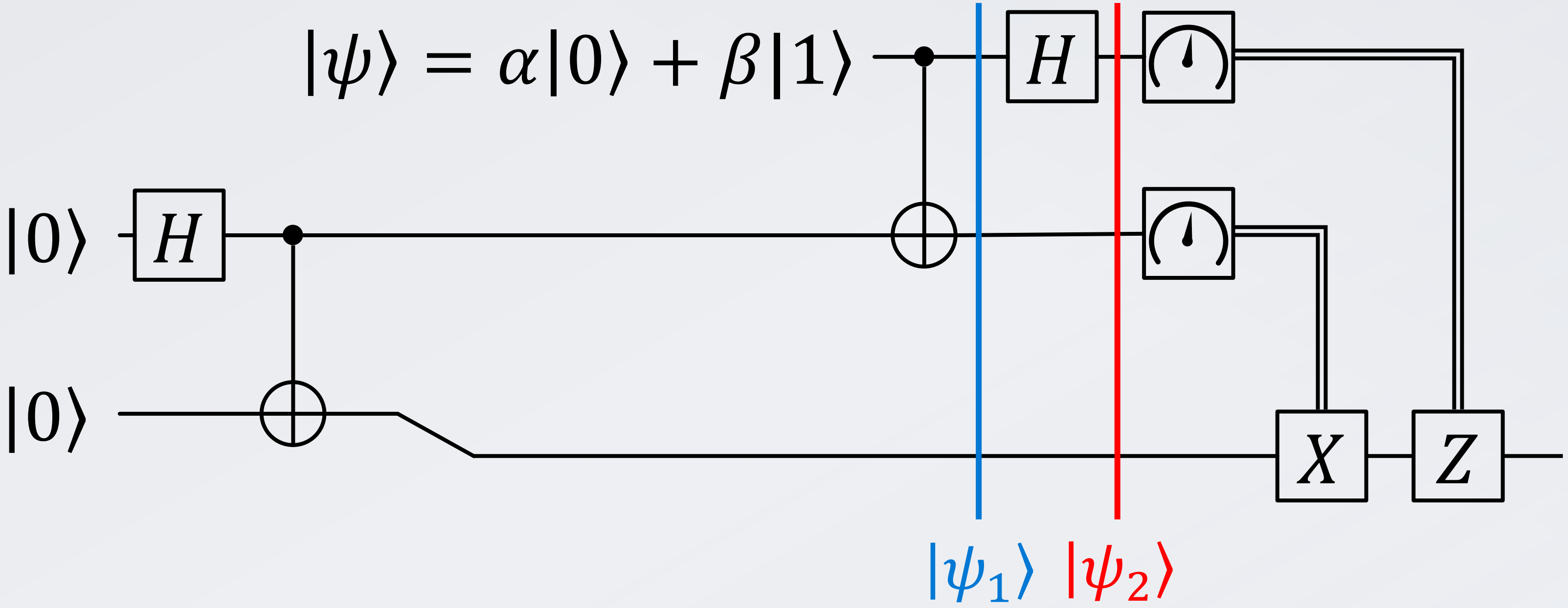


$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle))$$

$$\Downarrow$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle))$$

Teleportation: H

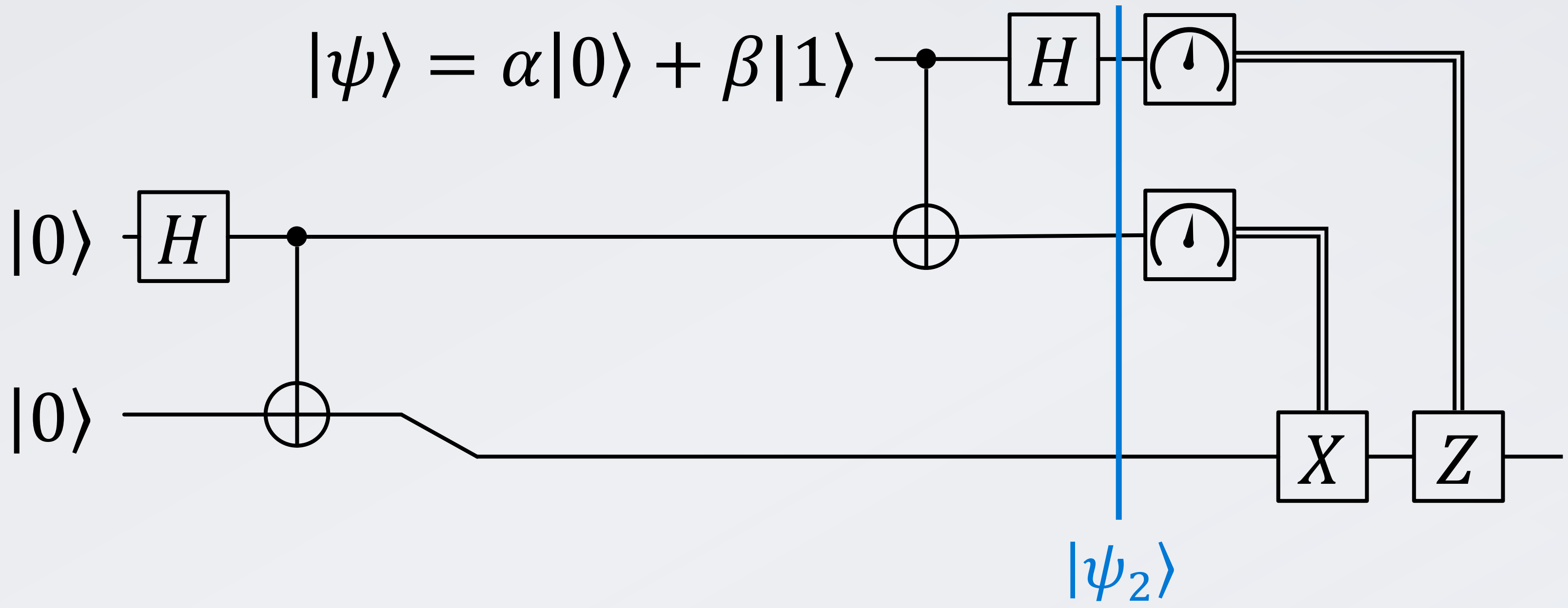


$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle))$$

$$\Downarrow$$

$$|\psi_2\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$

Teleportation: state before measurements, rewritten

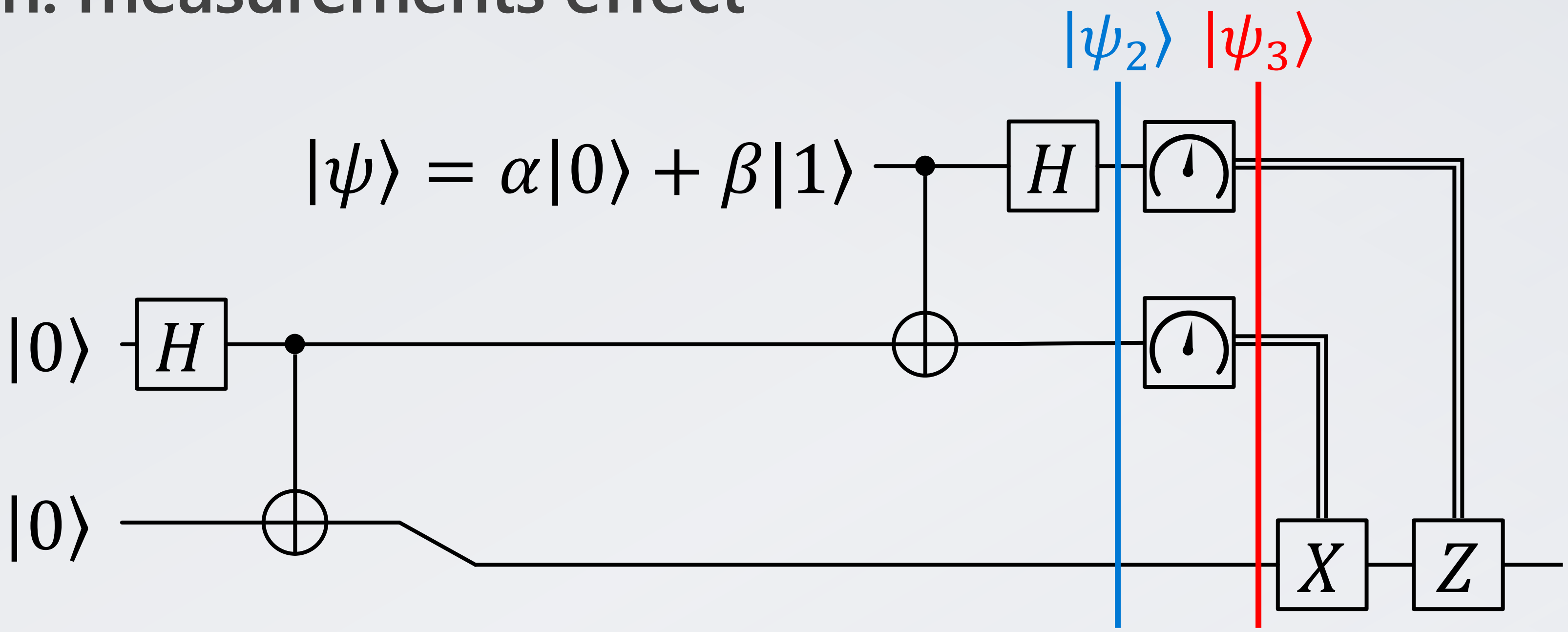


$$|\psi_2\rangle = \tfrac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$

$$= \tfrac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) +$$

$$+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$$

Teleportation: measurements effect



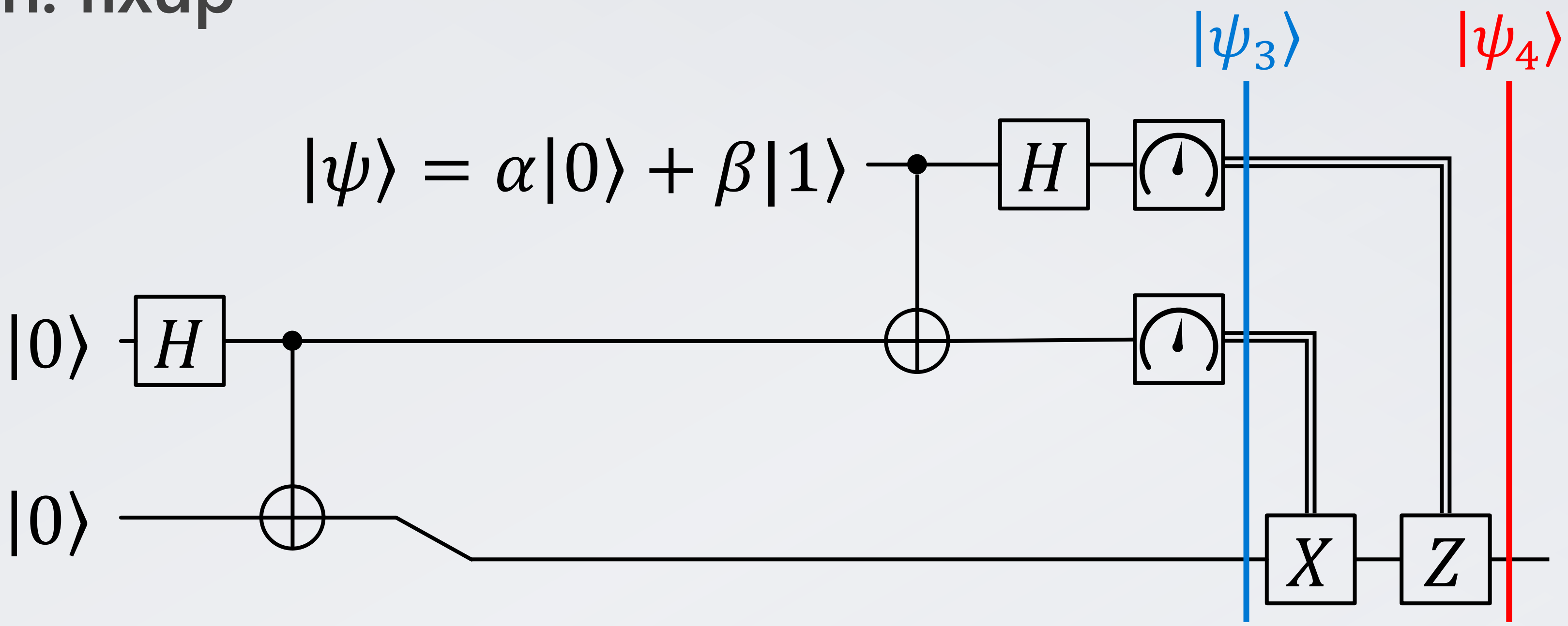
$$|\psi_2\rangle = \tfrac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$$

When Alice measures her two qubits, the state of Bob's qubit becomes:

$$00 \mapsto |\psi_3\rangle \equiv \alpha|0\rangle + \beta|1\rangle, \qquad 01 \mapsto |\psi_3\rangle \equiv \alpha|1\rangle + \beta|0\rangle$$

$$10 \mapsto |\psi_3\rangle \equiv \alpha|0\rangle - \beta|1\rangle, \qquad 11 \mapsto |\psi_3\rangle \equiv \alpha|1\rangle - \beta|0\rangle$$

Teleportation: fixup



$$00 \mapsto |\psi_3\rangle \equiv \alpha|0\rangle + \beta|1\rangle, \qquad 01 \mapsto |\psi_3\rangle \equiv \alpha|1\rangle + \beta|0\rangle$$
$$10 \mapsto |\psi_3\rangle \equiv \alpha|0\rangle - \beta|1\rangle, \qquad 11 \mapsto |\psi_3\rangle \equiv \alpha|1\rangle - \beta|0\rangle$$

Bob can correct the state of his qubit using Alice's measurement results:

$$00 \mapsto I(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle, \qquad 01 \mapsto X(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle,$$
$$10 \mapsto Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle, \qquad 11 \mapsto ZX(\alpha|1\rangle - \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle$$

Teleportation: final remarks

Teleportation is not…

- Cloning: the state of the original qubit is collapsed after the measurement
- Sending infinite classical information with 2 bits: Bob still cannot learn α and β precisely

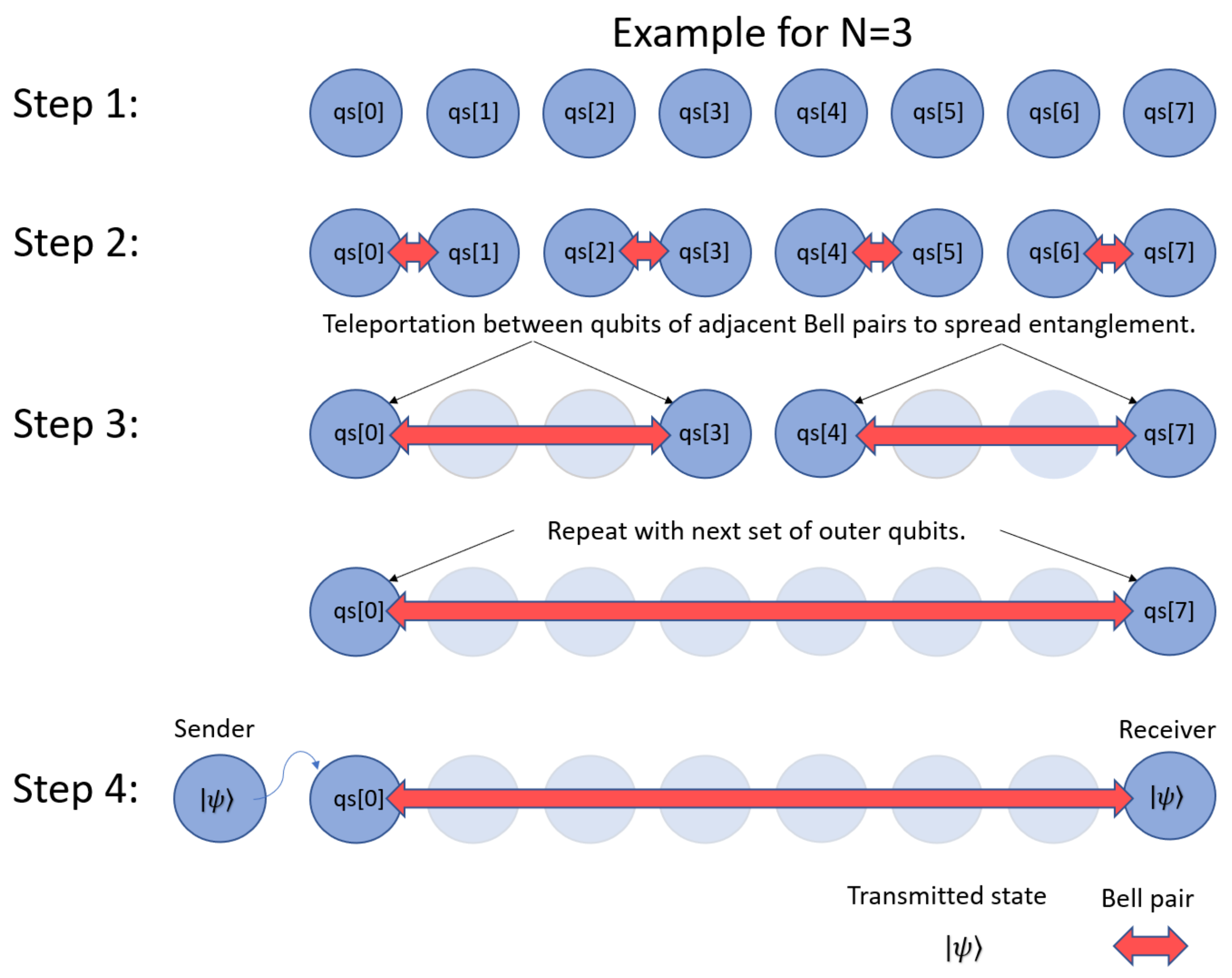
Does teleportation allow us to send information faster than speed of light?

- The change in the state of Bob's qubit happens instantly
- But all measurement results have equal probability, so Bob cannot decode the information sent
- Without Alice's classical results teleportation doesn't transmit information

Shows how to "push" information around the system

- Entanglement is a resource – we can "spend" it to do something
- Alice's part of the protocol is "measuring in the Bell basis" – it converts Bell states into corresponding computational basis states and measures them
- Teleportation is a building block for entanglement swapping and quantum repeaters

Quantum repeater network: long-distance transmission



Superdense coding

Superdense coding

Alice needs to send two classical bits to Bob

She can only send a qubit to Bob (not classical information)

Alice and Bob share an entangled pair of qubits

What does she do?

- **Alice encodes bits using her qubit**
  You can switch between Bell states using operations on only one qubit!
- **Alice sends her qubit to Bob**
- **Bob performs measurement in Bell basis to recover the bits**

Superdense coding: transforming Bell states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \xrightarrow{X} \quad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$\downarrow\ Z \qquad\qquad \searrow\ ZX \qquad\qquad \downarrow\ Z$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad \xrightarrow[-X]{} \quad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Superdense coding: protocol