Introduction to Quantum Computing

Module 2 — Part II

Ugo Dal Lago

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Inria informatiques mathématiques

Academic Year 2024/2025

Part I

Quantum Protocols

Circuits vs. Protocols

- **Quantum Circuits**
  - These are sequences of (unitary) operations applied to qubits in a prescribed manner.
  - Meant to be executed by quantum hardware or simulated through classical hardware.
  - They are seen as ways to compute functions from $\{0,1\}^n$ to $\{0,1\}^m$.

Circuits vs. Protocols

- **Quantum Circuits**
  - These are sequences of (unitary) operations applied to qubits in a prescribed manner.
  - Meant to be executed by quantum hardware or simulated through classical hardware.
  - They are seen as ways to compute functions from $\{0,1\}^n$ to $\{0,1\}^m$.
- **Quantum Protocols**
  - Communication protocols, i.e., sequence of computation and communication steps, perormed by a set of (possibly distributed) agents.
  - Besides using and exchanging classical data, the agents can use and exchange quantum data in the form of qubits.
  - The underlying task to be solved can be different from the mere computation of a function, e.g.,
    - Transmission or distribution of some information.
    - Consensus.
    - Commitment.
    - $\ldots$

What *is* a Quantum Protocol?

- One can formally define what a quantum protocol actually is, and there are *many* languages and models of quantum protocols.
- We will stay very **informal**, and describe quantum protocols by:
  - Either giving a circuit, describing who owns each of the qubits, and/or when they are exchanges between the parties.
  - Or/and describing what each of the agents is supposed to do with its data.

Part II

Quantum Teleportation

Teleporting a Qubit?

- Suppose Alice has a qubit she does not want to measure, and that she wants to “send it” to Bob.

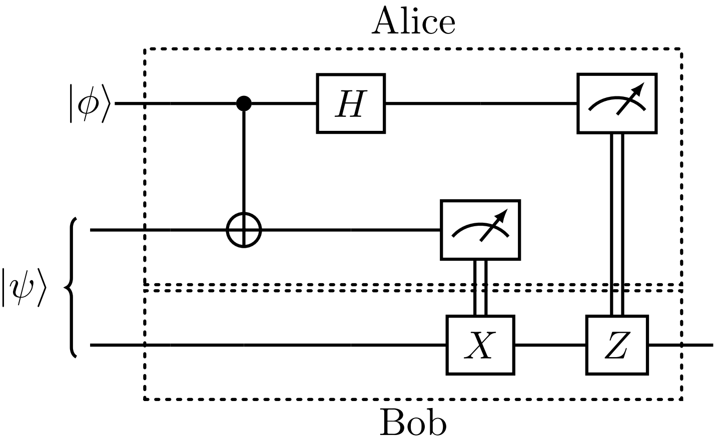
Teleporting a Qubit?

- Suppose Alice has a qubit she does not want to measure, and that she wants to “send it” to Bob.
- In doing so, se is allowed to actually send classical information, but that she cannot send quantum information.

Teleporting a Qubit?

- Suppose Alice has a qubit she does not want to measure, and that she wants to "send it" to Bob.
- In doing so, se is allowed to actually send classical information, but that she cannot send quantum information.
- Surprisingly, this can be achieved, provided Alice and Bob share a pair on entrangled qubits $|\psi\rangle$, which can be setup *prior* to the creation of Alice's qubit.
- The byproduct of the communication is that $|\psi\rangle$ is destroyed.

Quantum Teleportation as a Circuit



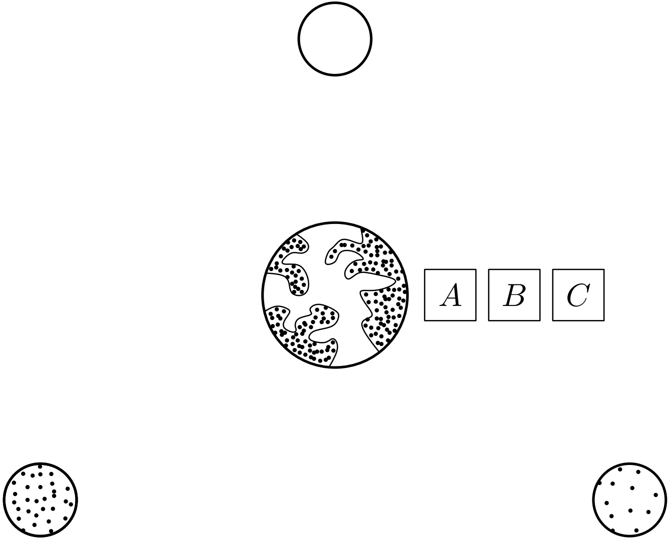
Part III

Quantum Pseudotelepathy

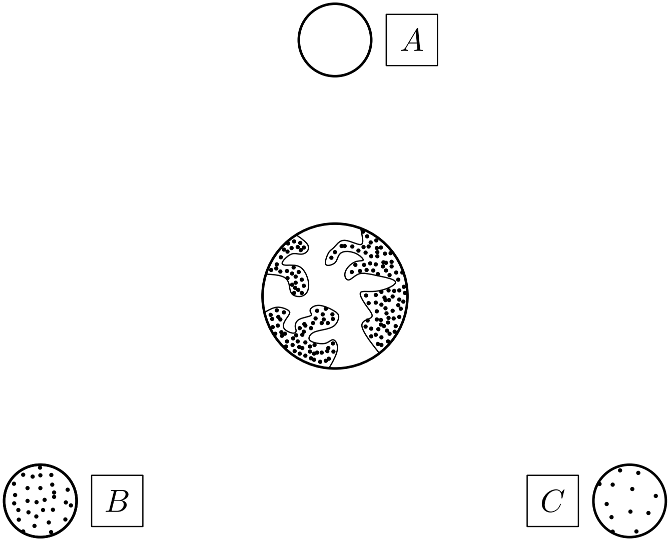
Quantum Pseudotelepahy

- This term refers to protocols which uses entanglement for the sake of proving that (part of the) communication between the parties can be avoided.
  - This is often provably impossible in classical computing.
- We will introduce only a very simple example of quantum pseudotelepathy, through a game.

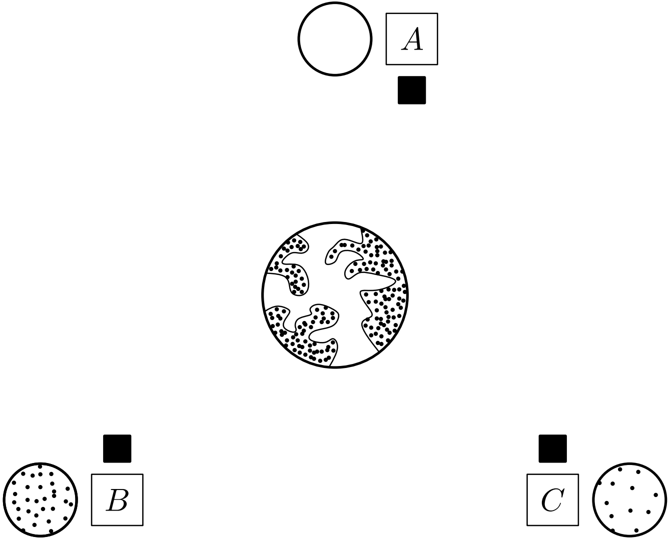
A Game



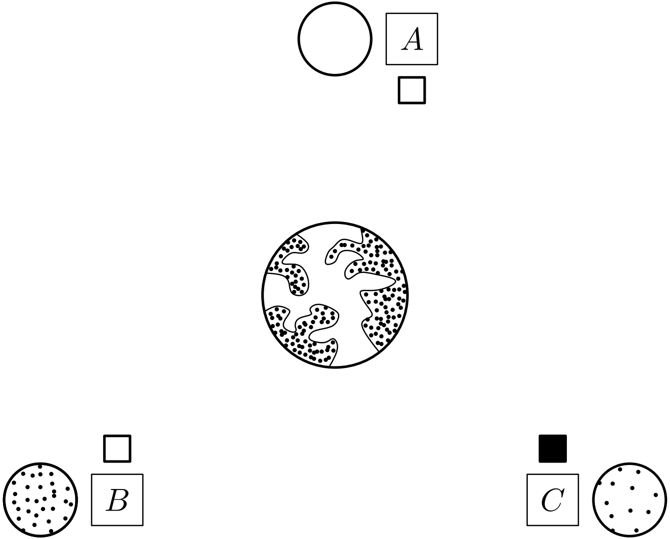
A Game



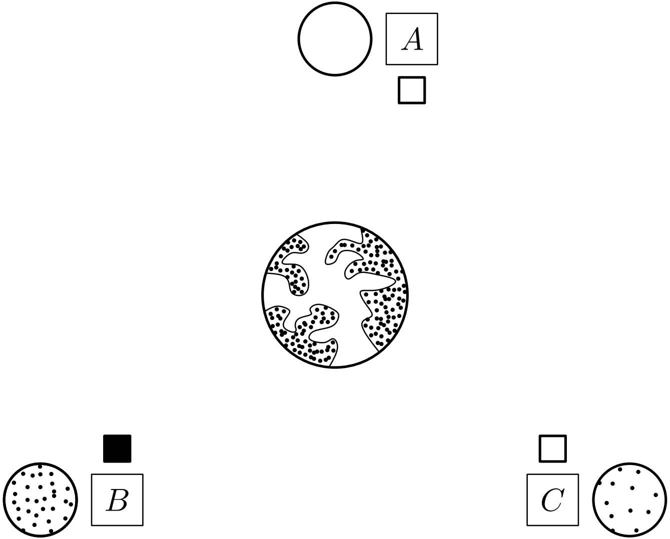
A Game



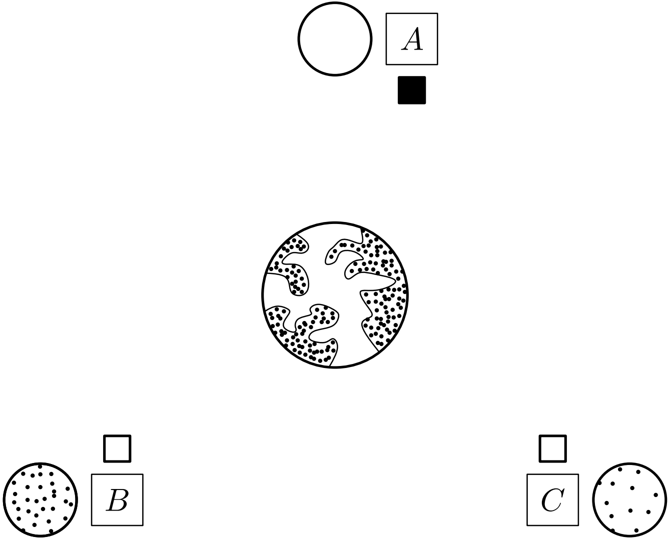
A Game



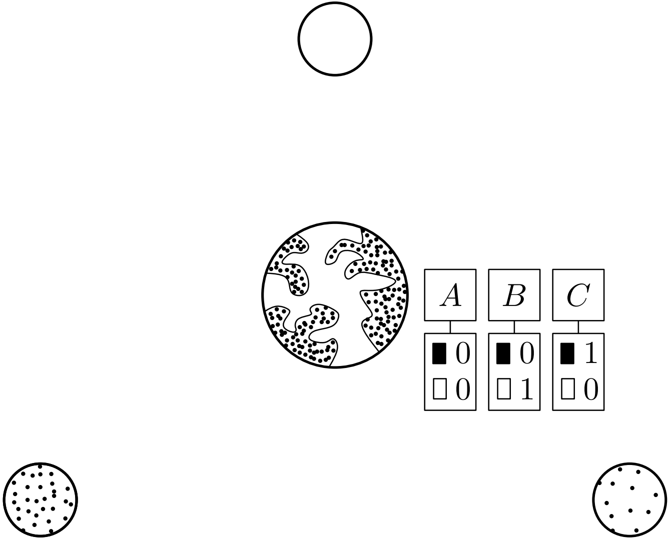
A Game



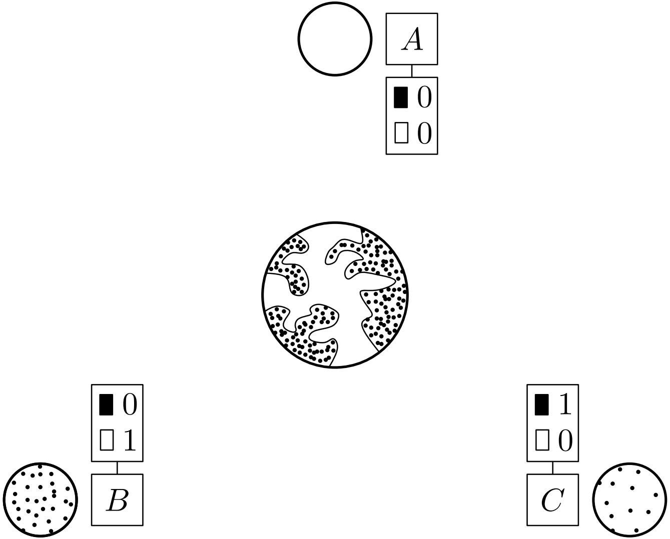
A Game



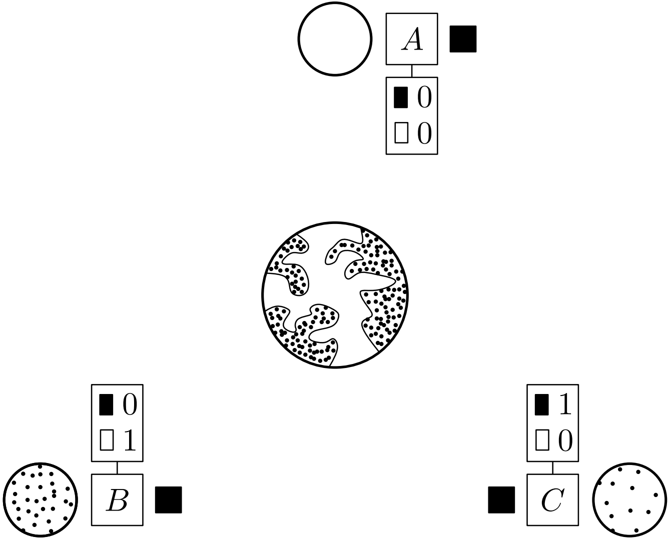
A Game



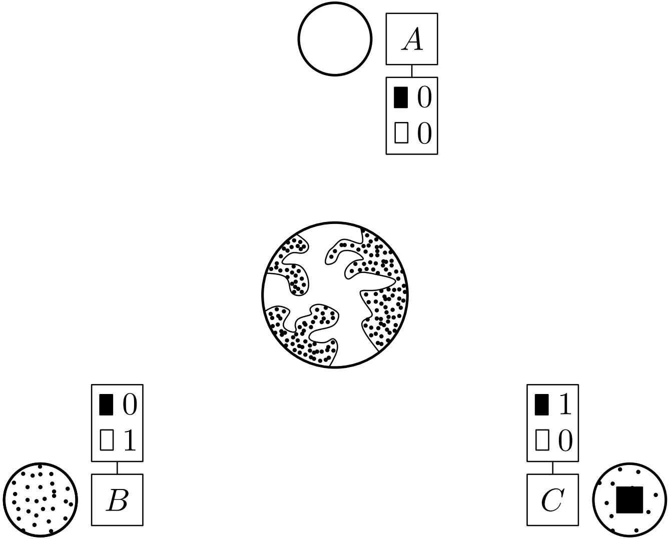
A Game



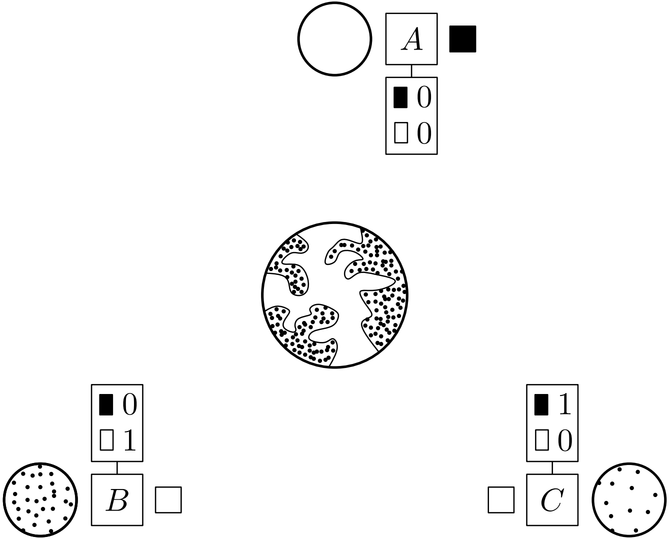
A Game



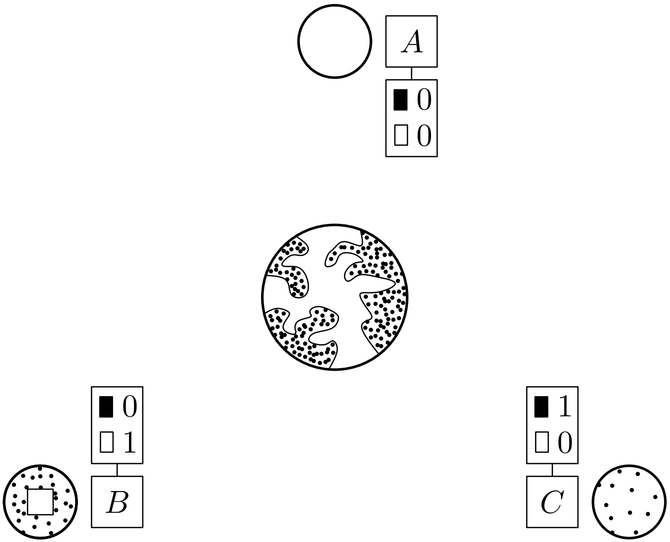
A Game



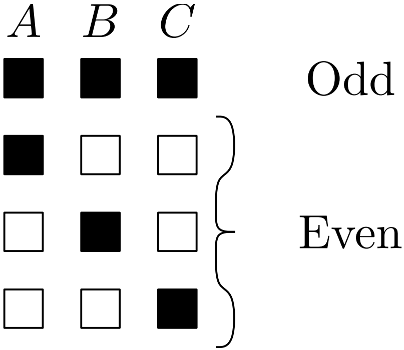
A Game



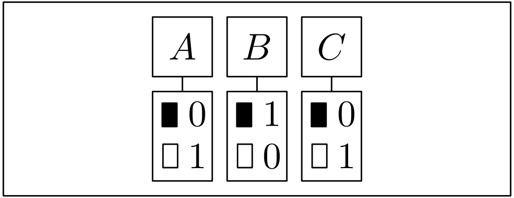
A Game



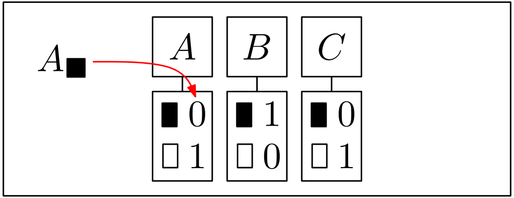
When do A, B and C Win?



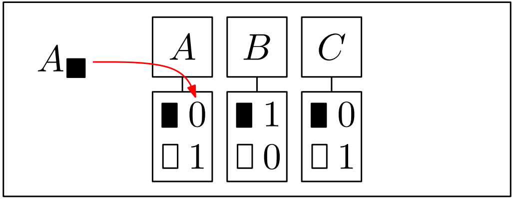
When do A, B and C Win?



When do A, B and C Win?



When do A, B and C Win?



$$A_{\blacksquare} + B_{\blacksquare} + C_{\blacksquare} = \text{Odd}$$

$$A_{\blacksquare} + B_{\square} + C_{\square} = \text{Even}$$

$$A_{\square} + B_{\blacksquare} + C_{\square} = \text{Even}$$

$$A_{\square} + B_{\square} + C_{\blacksquare} = \text{Even}$$

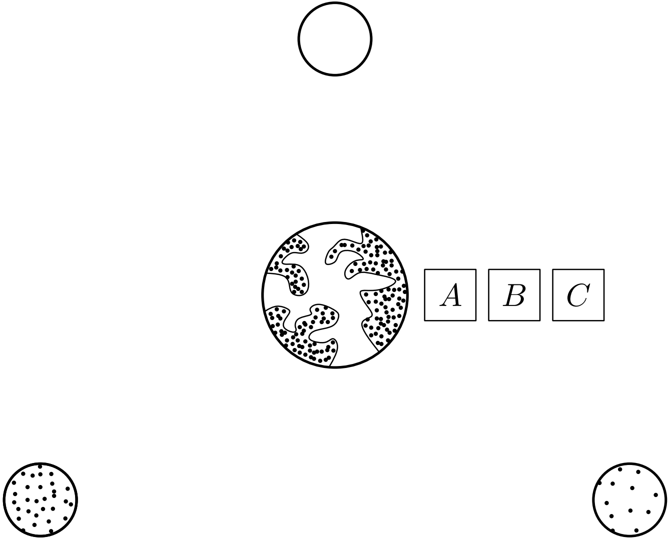
A, B e C Cannot Win!

$$2A_{\blacksquare} + 2A_{\square} + 2B_{\blacksquare} + 2B_{\square} + 2C_{\blacksquare} + 2C_{\square} = \text{Odd}$$

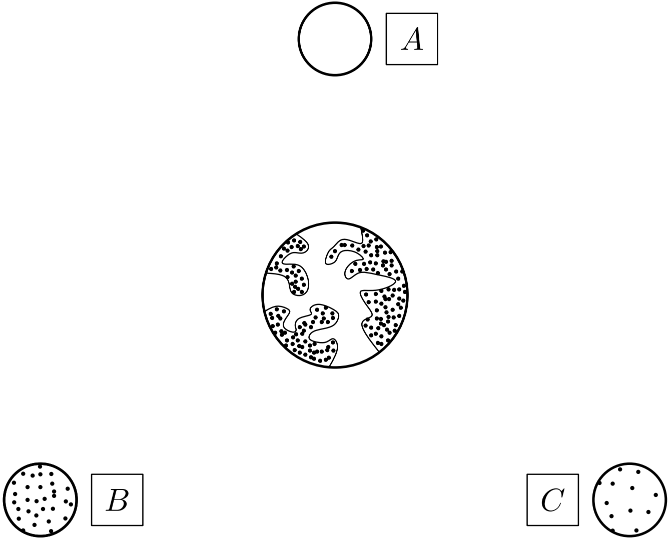
A, B e C Cannot Win!

$$2A_{\blacksquare} + 2A_{\square} + 2B_{\blacksquare} + 2B_{\square} + 2C_{\blacksquare} + 2C_{\square} = \text{Odd}$$

A Quantum Game



A Quantum Game



Quantum Strategies

$$\boxed{A}$$

$\square$

$$|1yz\rangle \rightarrow \sqrt{\tfrac{1}{2}}|1yz\rangle + \sqrt{\tfrac{1}{2}}|0yz\rangle$$

$$|0yz\rangle \rightarrow \sqrt{\tfrac{1}{2}}|1yz\rangle - \sqrt{-\tfrac{1}{2}}|0yz\rangle$$

$\blacksquare$

$$|1yz\rangle \rightarrow \sqrt{\tfrac{1}{2}}|1yz\rangle + \sqrt{\tfrac{1}{2}}|0yz\rangle$$

$$|0yz\rangle \rightarrow \sqrt{\tfrac{1}{2}}|1yz\rangle - \sqrt{\tfrac{1}{2}}|0yz\rangle$$

Quantum Strategies

A

□

$$|1yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle + \sqrt{\tfrac{1}{2}}|0yz\rangle$$

$$|0yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle - \sqrt{-\tfrac{1}{2}}|0yz\rangle$$

■

$$|1yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle + \sqrt{\tfrac{1}{2}}|0yz\rangle$$

$$|0yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle - \sqrt{\tfrac{1}{2}}|0yz\rangle$$

If ■ arrives…

Quantum Strategies

$\boxed{A}$

$\square$

$$|1yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle + \sqrt{\tfrac{1}{2}}|0yz\rangle$$

$$|0yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle - \sqrt{-\tfrac{1}{2}}|0yz\rangle$$

$\blacksquare$

$$|1yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle + \sqrt{\tfrac{1}{2}}|0yz\rangle$$

$$|0yz\rangle \to \sqrt{\tfrac{1}{2}}|1yz\rangle - \sqrt{\tfrac{1}{2}}|0yz\rangle$$

If $\blacksquare$ arrives...

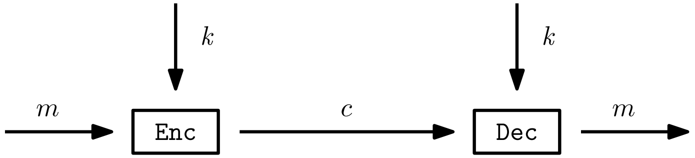
$$\sqrt{\frac{1}{2}}\,|111\rangle + \sqrt{\frac{1}{2}}\,|000\rangle \to \frac{1}{2}\,|111\rangle + \frac{1}{2}\,|011\rangle + \frac{1}{2}\,|100\rangle - \frac{1}{2}\,|000\rangle$$

Part IV

Quantum Key Distribution

Private-Key Cryptography

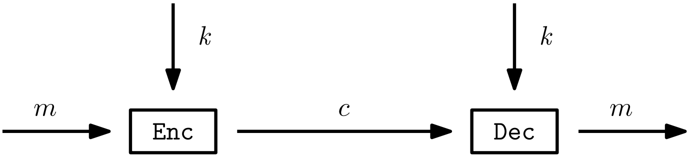
- Sometimes, encryption is done **symmetrically** rather than with distinct public and private keys:



- As a matter of fact, one can design (secure) symmetric encryption schemes such that `Enc` and `Dec` are quite efficient.

Private-Key Cryptography

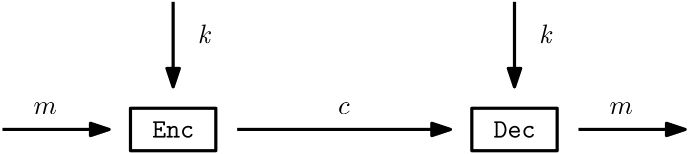
- Sometimes, encryption is done **symmetrically** rather than with distinct public and private keys:



- As a matter of fact, one can design (secure) symmetric encryption schemes such that `Enc` and `Dec` are quite efficient.
- Symmetric encryption schemes, however, pose a challenge: how could we let the sender and receiver **share** a key k in the first place?

Private-Key Cryptography

- Sometimes, encryption is done **symmetrically** rather than with distinct public and private keys:



- As a matter of fact, one can design (secure) symmetric encryption schemes such that `Enc` and `Dec` are quite efficient.
- Symmetric encryption schemes, however, pose a challenge: how could we let the sender and receiver **share** a key k in the first place?
- Many solutions possible:
  - Using a **secure** channel.
  - Using **public-key** encryption to share the key, then switching to the private-key setting.
  - Relying on **quantum computing**

Exploiting Quantum Channels

- Communication channels are traditionally assumed to be just classical.
  - Data flowing along the channel can be **observed** without being altered, and the value observed can be **duplicated**

Exploiting Quantum Channels

- Communication channels are traditionally assumed to be just classical.
  - Data flowing along the channel can be **observed** without being altered, and the value observed can be **duplicated**
- In practice, they often work according to the rules of quantum mechanics.
  - Observing some piece of data becomes a **quantum measurement**, and duplicating it is forbidden, due to the **No-Cloning Theorem**.

Exploiting Quantum Channels

- Communication channels are traditionally assumed to be just classical.
  - Data flowing along the channel can be **observed** without being altered, and the value observed can be **duplicated**
- In practice, they often work according to the rules of quantum mechanics.
  - Observing some piece of data becomes a **quantum measurement**, and duplicating it is forbidden, due to the **No-Cloning Theorem**.
- Can this be exploited? Is there a way to *take advantage of that*?

Working with Two Orthonormal Bases

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

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

Working with Two Orthonormal Bases

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

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

- Both $\mathbf{P} = \{|{\rightarrow}\rangle, |{\uparrow}\rangle\}$ and $\mathbf{T} = \{|{\nwarrow}\rangle, |{\nearrow}\rangle\}$ are orthonormal bases.

Working with Two Orthonormal Bases

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

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

- Both $\mathbf{P} = \{|\rightarrow\rangle, |\uparrow\rangle\}$ and $\mathbf{T} = \{|\nwarrow\rangle, |\nearrow\rangle\}$ are orthonormal bases.
- If the state of your system is in $\mathbf{P}$, and you measure it with respect to $\mathbf{T}$ you will end up in either $|\nwarrow\rangle$ or $|\nearrow\rangle$ each with probability $\frac{1}{2}$.

Working with Two Orthonormal Bases

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

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

- Both $\mathbf{P} = \{|{\rightarrow}\rangle, |{\uparrow}\rangle\}$ and $\mathbf{T} = \{|{\nwarrow}\rangle, |{\nearrow}\rangle\}$ are orthonormal bases.
- If the state of your system is in $\mathbf{P}$, and you measure it with respect to $\mathbf{T}$ you will end up in either $|{\nwarrow}\rangle$ or $|{\nearrow}\rangle$ each with probability $\frac{1}{2}$.
- If the state of your system is in $\mathbf{T}$, and you measure it with respect to $\mathbf{P}$ you will end up in either $|{\rightarrow}\rangle$ or $|{\uparrow}\rangle$ each with probability $\frac{1}{2}$.

The BB84 Protocol

Quantum
Insecure Channel

$$\text{Alice} \xrightarrow{\hspace{6em}} \text{Bob}$$

0	1	0	0	1	0	$\cdots$
P	**P**	**T**	**P**	**T**	**P**	$\cdots$
$\lvert\rightarrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\cdots$

The BB84 Protocol

$$\text{Alice} \xrightarrow[\text{Insecure Channel}]{\text{Quantum}} \text{Bob}$$

0	1	0	0	1	0	$\cdots$	0	1	0	0	1	0	$\cdots$
P	**P**	**T**	**P**	**T**	**P**	$\cdots$	**T**	**P**	**T**	**T**	**P**	**P**	$\cdots$
$\lvert\rightarrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\cdots$	?	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	?	?	$\lvert\rightarrow\rangle$	$\cdots$

The BB84 Protocol

Quantum
Insecure Channel

$$\text{Alice} \longrightarrow \text{Bob}$$

0	1	0	0	1	0	$\cdots$	0	1	0	0	1	0	$\cdots$
P	**P**	**T**	**P**	**T**	**P**	$\cdots$	**T**	**P**	**T**	**T**	**P**	**P**	$\cdots$
$\lvert\rightarrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\cdots$	?	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	?	?	$\lvert\rightarrow\rangle$	$\cdots$

- Alice and Bob, **after** having transmitted sequence of $\{0, 1\}$, can just compare their sequences of $\{\mathbf{T}, \mathbf{P}\}$, and they can do it on an insecure channel.
- They can also **realize** somebody has seen or altered the sequence, by comparing *some* (around *half*) of the exchanged values.

Part V

Quantum Commitment

Commitment Protocols

- A **commitment protocol** allows two parties Alice and Bob to interact so as to allow Alice to commit to a chosen value, guaranteeing that:
  - The value chosen by Alice remains *hidden* until Alice decides to reveal it.
  - Neither Alice nor Bob can *change* the value chosen by Alice, i.e., the protocol is **binding**.

Commitment Protocols

- A **commitment protocol** allows two parties Alice and Bob to interact so as to allow Alice to commit to a chosen value, guaranteeing that:
  - The value chosen by Alice remains *hidden* until Alice decides to reveal it.
  - Neither Alice nor Bob can *change* the value chosen by Alice, i.e., the protocol is **binding**.
- In (classical) cryptography, various forms of commitment protocols have been introduced. All of them rely on cyrptographic assumptions, like the existence of one-way functions.
- Quantum computing, given the fact that observations can possibly alter the value of data, seems like a promising approach.

Quantum Bit Commitment

- Suppose Alice and Bob wants to commit on the value of a single bit, chosen by Alice.

Quantum Bit Commitment

- Suppose Alice and Bob wants to commit on the value of a single bit, chosen by Alice.
- Alice chooses a value b, and prepares n qubits $|x_1\rangle, \ldots, |x_n\rangle$ as follows, after having drawn n bits at random, obtaining values $v_1, \ldots, v_n \in \{0,1\}$:
  - If $b = 1$, then $|x_i\rangle$ will be set to $|v_i\rangle$.
  - If $b = 0$, then $|x_i\rangle$ will be set to $H(|v_i\rangle)$.

  She then noted the values $v_1 \ldots, v_n$, and send $|x_1\rangle, \ldots, |x_n\rangle$ to Bob, who keeps them in a safe place.
- When the time comes for Alice to reveal the value of b, she tells Bob not only b, but also $v_1, \ldots, v_n$. Bob can then verify whether Alice is cheating by just measuring $|x_1\rangle, \ldots, |x_n\rangle$.

On the Security of the Quantum Bit Commitment

- One can show that **no information** Bob can extract from the collection of qubits Alice sends him can distinguish between the case $b = 0$ and the case $b = 1$.

On the Security of the Quantum Bit Commitment

- One can show that **no information** Bob can extract from the collection of qubits Alice sends him can distinguish between the case $b = 0$ and the case $b = 1$.
- The protocol, however, **cannot be considered secure**:
  - Instead of preparing $|x_1\rangle, \ldots, |x_n\rangle$ as prescribed by the protocol, Alice could have prepared n pairs of entangled qubits, each pair being a Bell state, and send *the first qubit* of each pair to Bob.
  - The qubits Bob receives do not have states of their own, being entangled with the qubits Alice keeps for herself.
  - Before revealing her choice, Alice makes a direct measurement on each of the qubits she has kept and correctly informs Bob. Crucially, however, **she can change the value of** b by applying the H gate to its qubit.

On the Security of the Quantum Bit Commitment

- One can show that **no information** Bob can extract from the collection of qubits Alice sends him can distinguish between the case $b = 0$ and the case $b = 1$.
- The protocol, however, **cannot be considered secure**:
  - Instead of preparing $|x_1\rangle, \dots, |x_n\rangle$ as prescribed by the protocol, Alice could have prepared n pairs of entangled qubits, each pair being a Bell state, and send *the first qubit* of each pair to Bob.
  - The qubits Bob receives do not have states of their own, being entangled with the qubits Alice keeps for herself.
  - Before revealing her choice, Alice makes a direct measurement on each of the qubits she has kept and correctly informs Bob. Crucially, however, **she can change the value of** b by applying the H gate to its qubit.
- There is more: as proved by Mayers, unconditionally secure quantum bit commitment is impossible.