African School of Fundamental Physics and Applications

Quantum Information

Lecture 3 : Quantum Cryptography and Quantum Computing

Mourad Telmini
mourad.telmini@fst.utm.tn

Department of Physics
Faculty of Science of Tunis
University of Tunis El Manar

30 July 2021

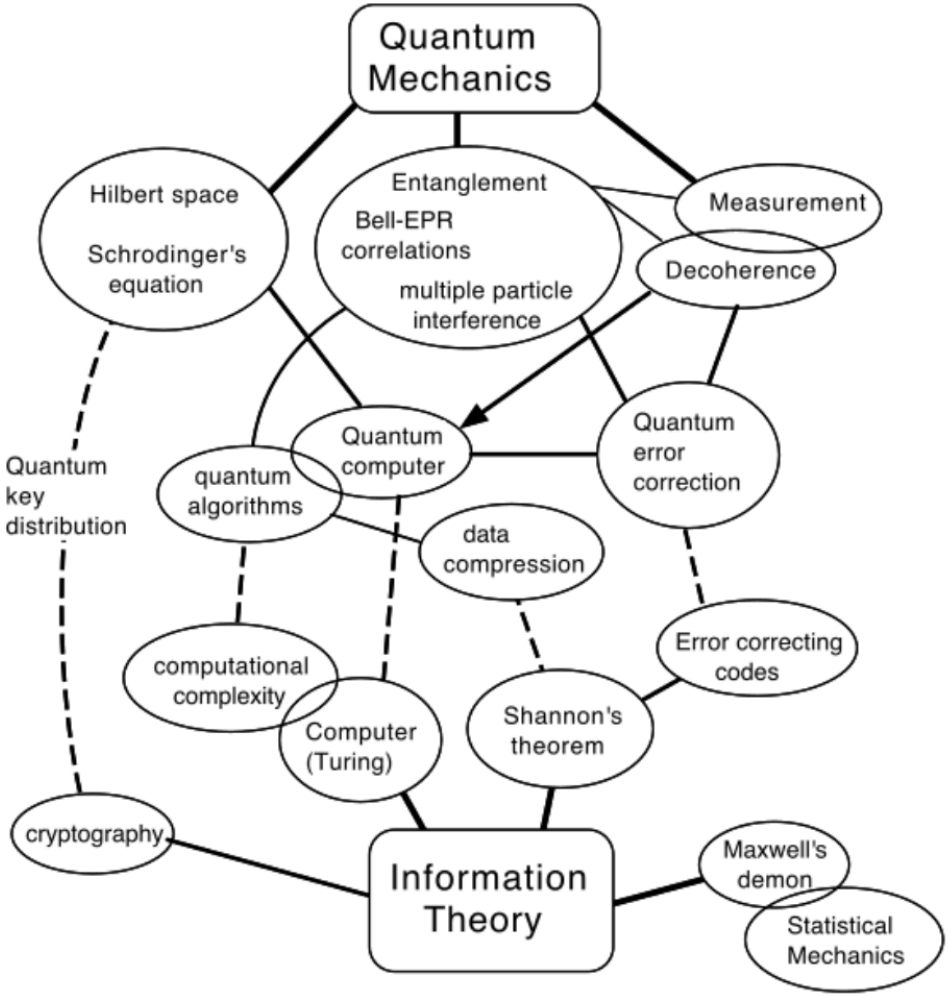
Outline

Outline

Outline

Outline

Quantum Mechanics and Information Theory



[1] Andrew Steane 1998 Rep. Prog. Phys. 61 117

Quantum Supremacy

nature

Explore our content ⌄ Journal information ⌄

nature › articles › article

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis ✉

Nature **574**, 505–510(2019) | Cite this article

Abstract

- The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor.

Abstract

- The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor.
- A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space.

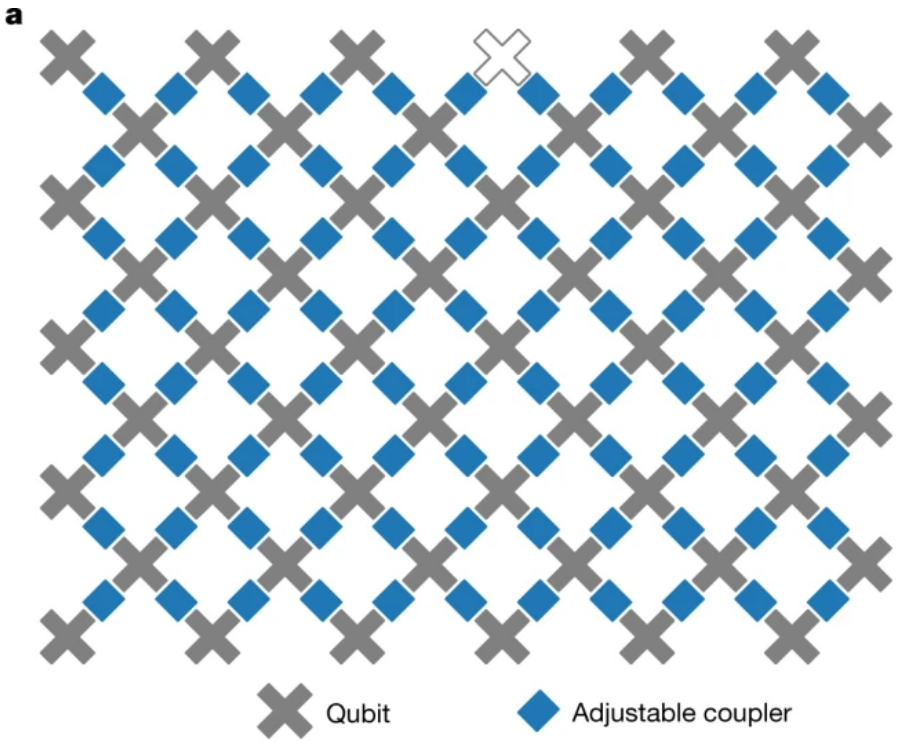
Abstract

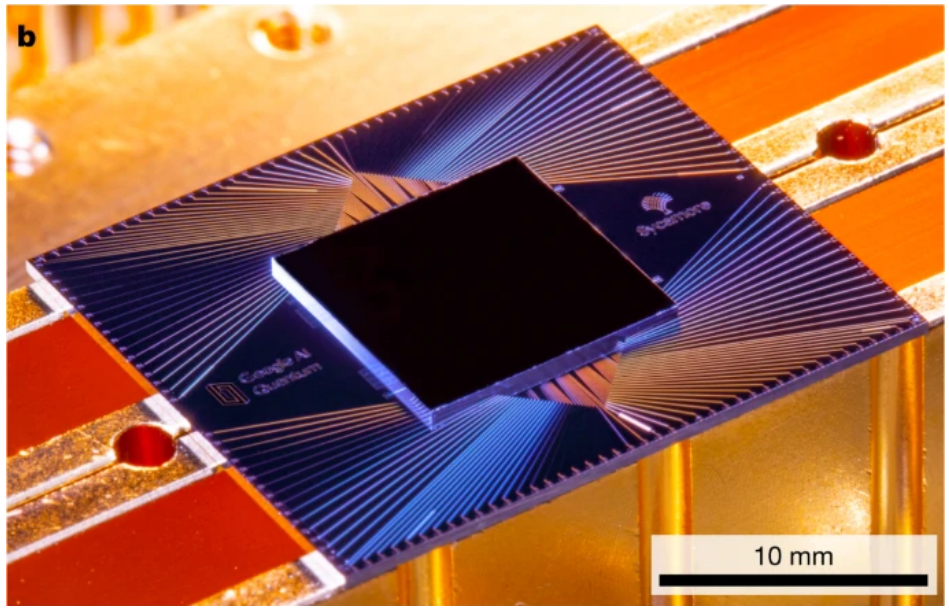
- The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor.
- A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space.
- Here we report the use of a processor with programmable superconducting qubits to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 253 (about 1016).

Abstract

- The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor.
- A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space.
- Here we report the use of a processor with programmable superconducting qubits to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 253 (about 1016).
- Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years.

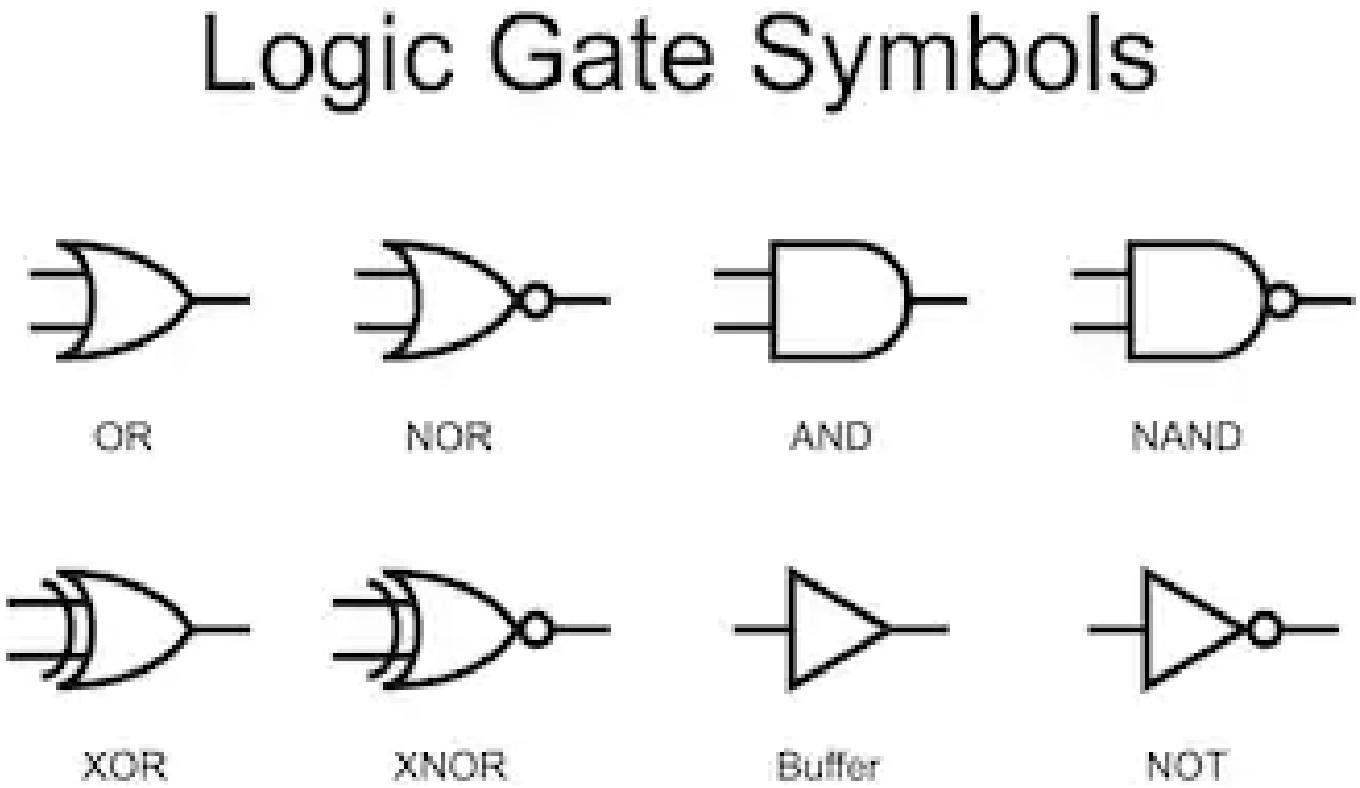
Sycamore processor





The Sycamore processor is made up of 53 qubits.

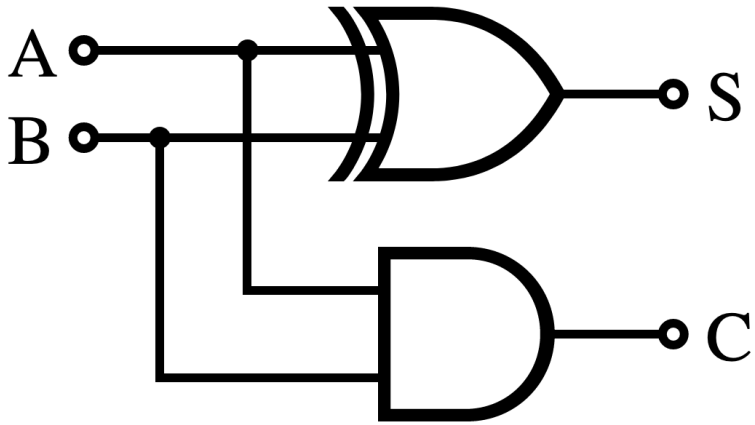
Summary of logic gates



See Appendix 1 for more details about classical logic gates

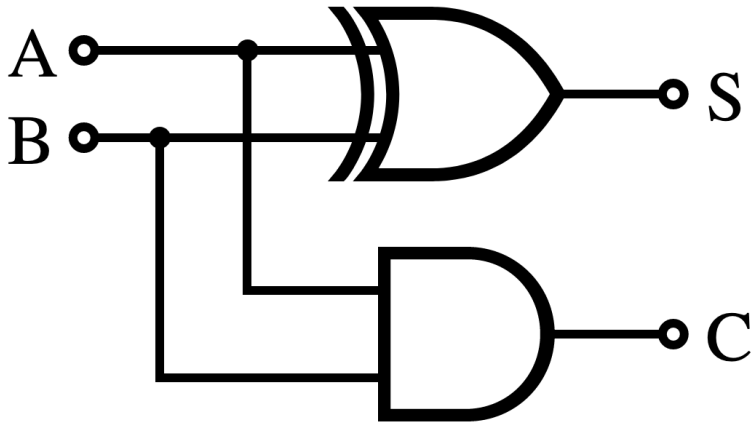
Half-adder circuit

- The half-adder takes two bits E_1 and E_2 as input and delivers 2 outputs, the sum S and the carry R, in accordance with the truth table presented above.



Half-adder circuit

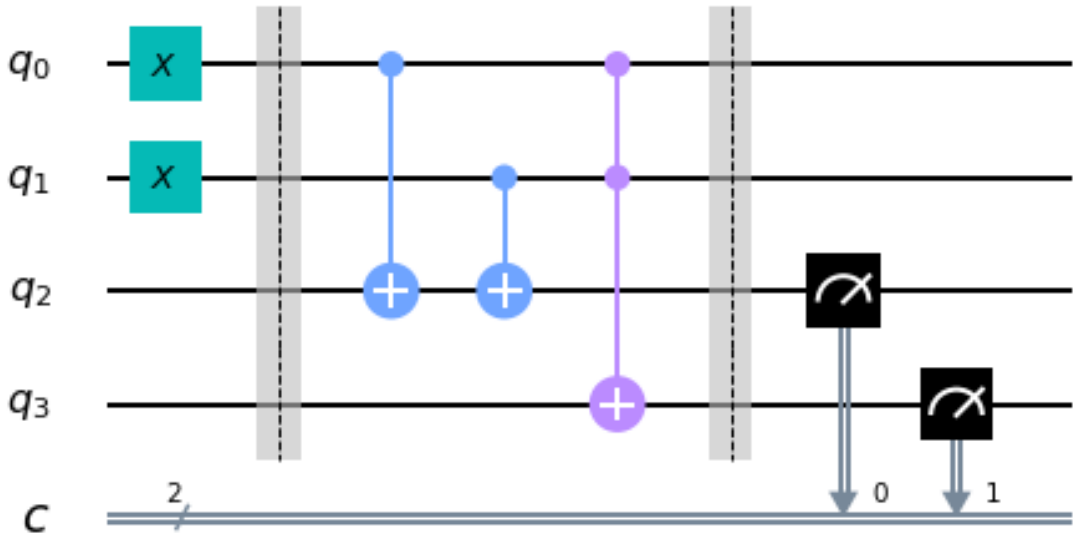
- The half-adder takes two bits E_1 and E_2 as input and delivers 2 outputs, the sum S and the carry R, in accordance with the truth table presented above.



- See Appendix 1 full-adder circuit

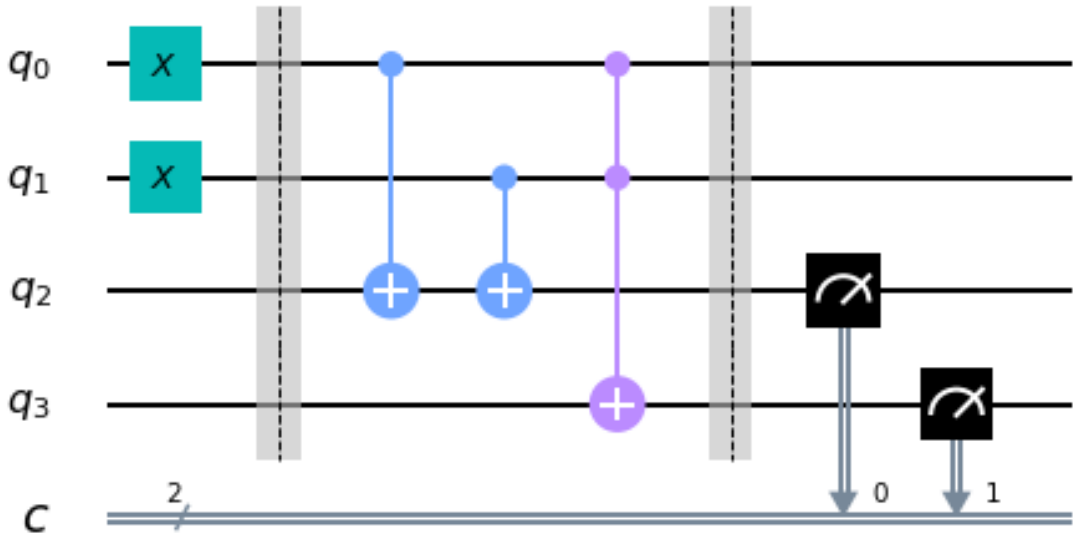
Half-adder quantum circuit

- Here's what a half-adding quantum circuit looks like:



Half-adder quantum circuit

- Here's what a half-adding quantum circuit looks like:



- How to build this Quantum circuit ?

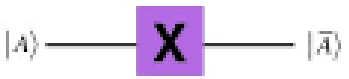
1-qubit quantum gates

- In quantum computation, a 1-qubit quantum gate is a unit transformation that transforms an the quantum state of input qubit into another quantum state or an output qubit.

- 1-qubit quantum gates are represented by unitary matrices 2×2.

A	$\bar{A}$
0	1
1	0

PAULI X GATE



$\|A\rangle$	$\|\bar{A}\rangle$
0	1
1	0

Quantum Logic Gates

X (NOT)
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

Y
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & 0 & -i \\ 1 & i & 0 \end{array}$$

Z
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{array}$$

S
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & i \end{array}$$

T
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & e^{i\pi/4} \end{array}$$

Hadamard (H)
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 1 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}$$

Sqrt NOT
$$\begin{array}{c|cc} & 0 & 1 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 1 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{array}$$

1-qubit quantum gates

- The main 1-qubit quantum gates are:

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z
  - Hadamard Gate H

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z
  - Hadamard Gate H
  - R_Φ gate

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z
  - Hadamard Gate H
  - R_Φ gate
  - Gates I, S and T

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z
  - Hadamard Gate H
  - R_Φ gate
  - Gates I, S and T
  - General gate U_3

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z
  - Hadamard Gate H
  - R_Φ gate
  - Gates I, S and T
  - General gate U_3
- In this section, we'll go over them. For example, we will find the Pauli matrices that we have already studied in the previous lecture.

1-qubit quantum gates

- The main 1-qubit quantum gates are:
  - Pauli gates X, Y and Z
  - Hadamard Gate H
  - R_Φ gate
  - Gates I, S and T
  - General gate U_3
- In this section, we'll go over them. For example, we will find the Pauli matrices that we have already studied in the previous lecture.
- We will use for the graphs, those of the IBM Qiskit environment (www.qiskit.org) where a 1 qubit gate (for example the X gate) is represented as follows:

Pauli Gates

- The Pauli gates X, Y and Z are represented by the 3 Pauli matrices σ_x, σ_y and σ_z.

Pauli Gates

- The Pauli gates X, Y and Z are represented by the 3 Pauli matrices σ_x, σ_y and σ_z.
- Thus, the gate X is described by the matrix:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Pauli Gates

- The Pauli gates X, Y and Z are represented by the 3 Pauli matrices σ_x, σ_y and σ_z.
- Thus, the gate X is described by the matrix:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- The gate Y is described by the matrix:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Pauli Gates

- The Pauli gates X, Y and Z are represented by the 3 Pauli matrices σ_x, σ_y and σ_z.
- Thus, the gate X is described by the matrix:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- The gate Y is described by the matrix:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

- Finally, the gate Z is described by the matrix :

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Pauli Gates

- The Pauli gates X, Y and Z are represented by the 3 Pauli matrices σ_x, σ_y and σ_z.
- Thus, the gate X is described by the matrix:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- The gate Y is described by the matrix:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

- Finally, the gate Z is described by the matrix :

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- here we adopted a specific notation with parentheses [ ] rather than the traditional parentheses ()

Hadamard Gate H

- The Hadamard gate H is fundamental in quantum computation. It is represented by the matrix:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Hadamard Gate H

- The Hadamard gate H is fundamental in quantum computation. It is represented by the matrix:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- It is used to generate state superpositions by acting on the state $|0\rangle$ or $|1\rangle$. Indeed :

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

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

Hadamard Gate H

- The Hadamard gate H is fundamental in quantum computation. It is represented by the matrix:

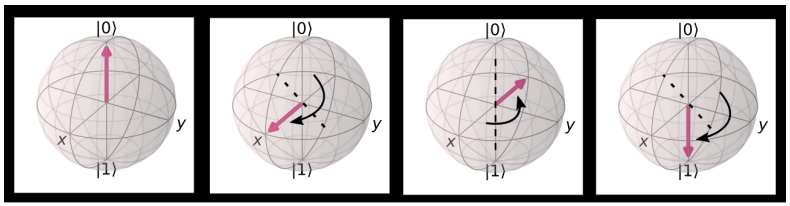
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- It is used to generate state superpositions by acting on the state $|0\rangle$ or $|1\rangle$. Indeed :

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

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

- The states $|+\rangle$ and $|-\rangle$ are particularly important in quantum cryptography.
- Exercice : verify the identity $X = HZH$



$n-$qubits Quantum gates

- In the previous section, we reviewed 1-qubit quantum gates. However, the real power of quantum computing takes advantage of superposition and entanglement, which requires at least 2 qubits.

$n-$qubits Quantum gates

- In the previous section, we reviewed 1-qubit quantum gates. However, the real power of quantum computing takes advantage of superposition and entanglement, which requires at least 2 qubits.
- We will see below the main gates at n qubits, focusing our attention on the central cases $n = 2.3$, with in particular the introduction of the CNOT gate (2 qubits) and the Toffoli gate (3 qubits).

$n-$qubits Quantum gates

- In the previous section, we reviewed 1-qubit quantum gates. However, the real power of quantum computing takes advantage of superposition and entanglement, which requires at least 2 qubits.
- We will see below the main gates at n qubits, focusing our attention on the central cases $n = 2.3$, with in particular the introduction of the CNOT gate (2 qubits) and the Toffoli gate (3 qubits).
- Thus, with 1, 2 and 3 qubit gates, we will be able to build circuits capable of performing quantum calculations (Quantum Computing).

Action of 1-qubit gates on n-qubits register

- Let us start a system with 2 qubits, which we will note for the purposes of quantum computation $|q_0\rangle$ and $|q_1\rangle$.

Action of 1-qubit gates on n-qubits register

- Let us start a system with 2 qubits, which we will note for the purposes of quantum computation $|q_0\rangle$ and $|q_1\rangle$.
- We have already defined the tensor product $|q_1\rangle \otimes |q_0\rangle \equiv |q_1 q_0\rangle$.

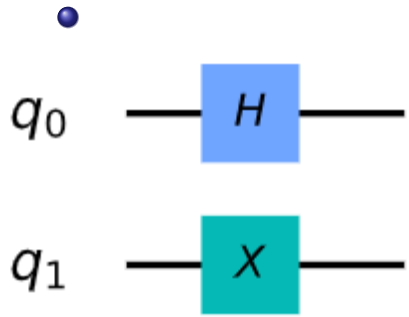
Action of 1-qubit gates on n-qubits register

- Let us start a system with 2 qubits, which we will note for the purposes of quantum computation $|q_0\rangle$ and $|q_1\rangle$.
- We have already defined the tensor product $|q_1\rangle \otimes |q_0\rangle \equiv |q_1 q_0\rangle$.
- We can construct operations which act on the tensor product, with the tensor products of 1-qubit gates.

Action of 1-qubit gates on n-qubits register

- Let us start a system with 2 qubits, which we will note for the purposes of quantum computation $|q_0\rangle$ and $|q_1\rangle$.
- We have already defined the tensor product $|q_1\rangle \otimes |q_0\rangle \equiv |q_1 q_0\rangle$.
- We can construct operations which act on the tensor product, with the tensor products of 1-qubit gates.
- For example, with a gate H acting on $|q_0\rangle$ and a gate X acting on $|q_1\rangle$, we construct:

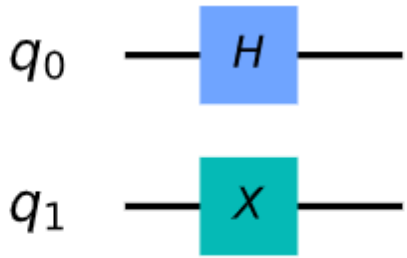
$$(X \otimes H)|q_1 q_0\rangle = X|q_1\rangle \otimes H|q_0\rangle$$



Action of 1-qubit gates on n-qubits register

- In accordance with the rules of the tensor product of 2 matrices, we have:

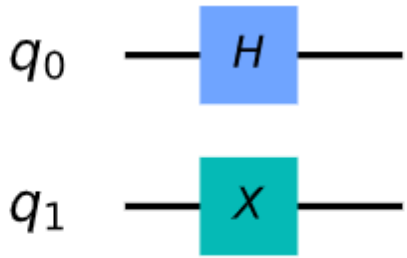
$$(X \otimes H) = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix}$$



Action of 1-qubit gates on n-qubits register

- In accordance with the rules of the tensor product of 2 matrices, we have:

$$(X \otimes H) = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix}$$



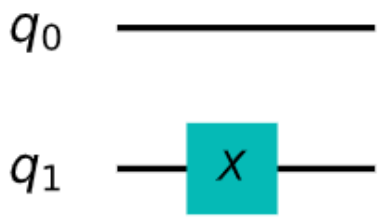
- By noting that the blocks 2×2 are none other than the gate H (by including the factor $(1/\sqrt{2})$, we can use the more compact notation for the same 2 qubit gate :

$$(X \otimes H) = \begin{bmatrix} 0 & H \\ H & 0 \end{bmatrix}$$

Action of 1-qubit gates on n-qubits register

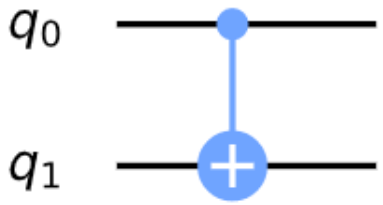
- If we want to apply a single gate to 1 qubit on one of the 2 qubits, we use the tensor product with the identity operator:

$$(X \otimes I) = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$



CNOT gate

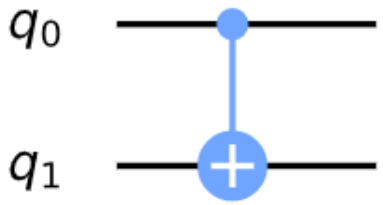
- The CNOT gate is a 2-qubits gate



CNOT gate

- The CNOT gate is a 2-qubits gate
- Its matrix representation is:

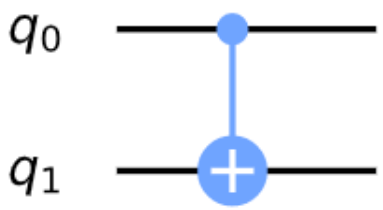
$$(CNOT) = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



CNOT gate

- The CNOT gate is a 2-qubits gate
- Its matrix representation is:

$$(CNOT) = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

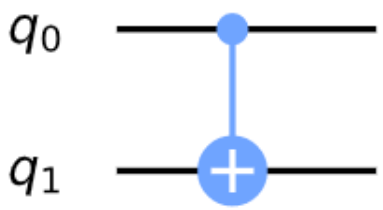


- It is a conditional gate which causes a gate X to act on the second qubit $|q_1\rangle$ (target), if the first qubit $|q_0\rangle$ (control) is in state $|1\rangle$.

CNOT gate

- The CNOT gate is a 2-qubits gate
- Its matrix representation is:

$$(CNOT) = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



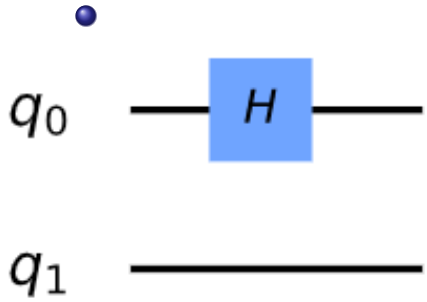
- It is a conditional gate which causes a gate X to act on the second qubit $|q_1\rangle$ (target), if the first qubit $|q_0\rangle$ (control) is in state $|1\rangle$.
- In this case, the CNOT gate reverses the amplitudes of the target qubit. Otherwise, she does not change her condition.

First Quantum Circuit

- The major interest of the CNOT gate is to create an entangled state.

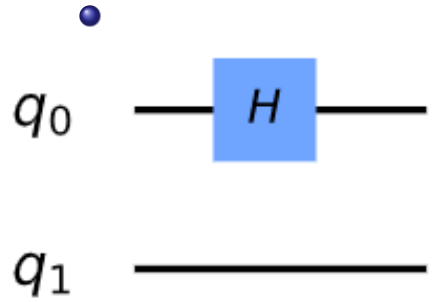
First Quantum Circuit

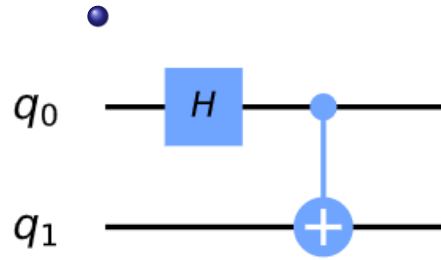
- The major interest of the CNOT gate is to create an entangled state.
- In the first step, to create a superimposed state, we make a gate of H act on $|q_0\rangle$, which produces the state $|+\rangle$ from the initial state $|0\rangle$. This is done by applying a $(H \otimes I)$ gate to the system.



First Quantum Circuit

- The major interest of the CNOT gate is to create an entangled state.
- In the first step, to create a superimposed state, we make a gate of H act on $|q_0\rangle$, which produces the state $|+\rangle$ from the initial state $|0\rangle$. This is done by applying a $(H \otimes I)$ gate to the system.
- Then the CNOT gate is applied, which amounts to creating a first quantum circuit.



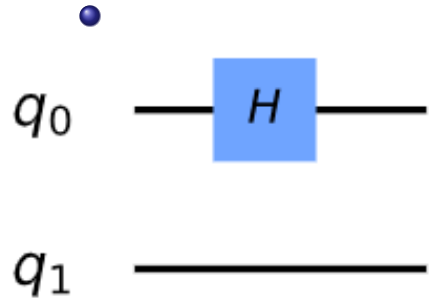


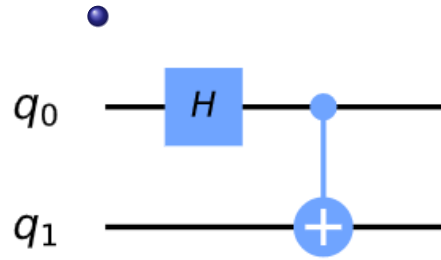
First Quantum Circuit

- The major interest of the CNOT gate is to create an entangled state.
- In the first step, to create a superimposed state, we make a gate of H act on $|q_0\rangle$, which produces the state $|+\rangle$ from the initial state $|0\rangle$. This is done by applying a $(H \otimes I)$ gate to the system.
- Then the CNOT gate is applied, which amounts to creating a first quantum circuit.
- The action of this circuit on the 2 qubit system initially in the state $|00\rangle$ is:

$$(CNOT.(H \otimes I))|00\rangle = CNOT|0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

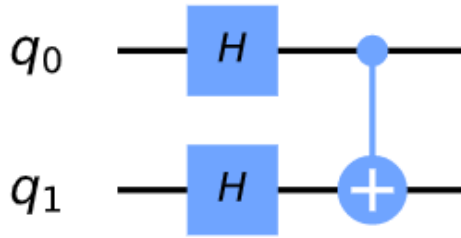
which is a Bell state.





Other quantum circuits

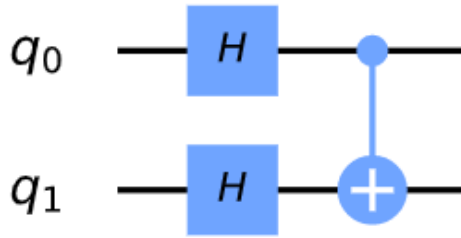
- We are going to complicate the previous circuit a bit, by adding a H gate on the second qubit.



Other quantum circuits

- We are going to complicate the previous circuit a bit, by adding a H gate on the second qubit.
- This circuit produces at output the state:

$$|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$



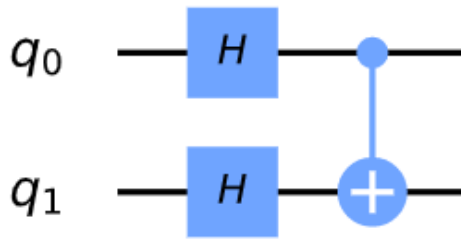
Other quantum circuits

- We are going to complicate the previous circuit a bit, by adding a H gate on the second qubit.
- This circuit produces at output the state:

$$|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

- If we put the target in the state $|-\rangle$, by applying a gate X after the gate H, and we add a gate CNOT, the circuit produces the state

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



Other quantum circuits

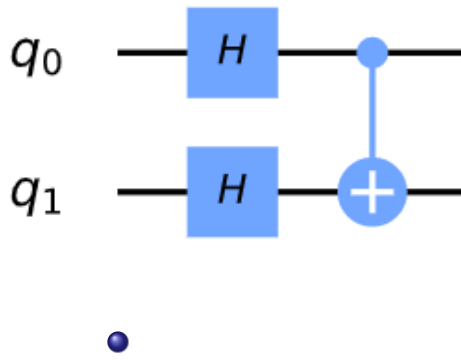
- We are going to complicate the previous circuit a bit, by adding a H gate on the second qubit.
- This circuit produces at output the state:

$$|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

- If we put the target in the state $|-\rangle$, by applying a gate X after the gate H, and we add a gate CNOT, the circuit produces the state

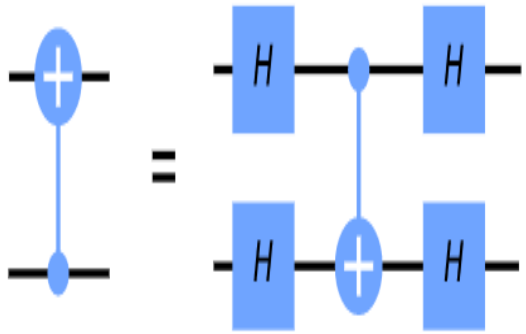
$$|--\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

- Note that this circuit changes the state of the control qubit, without modifying that of the target qubit.



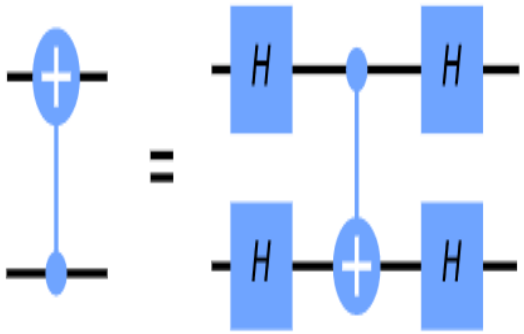
Phase kickback

- This circuit makes it possible to create a kind of CNOT gate upside down.



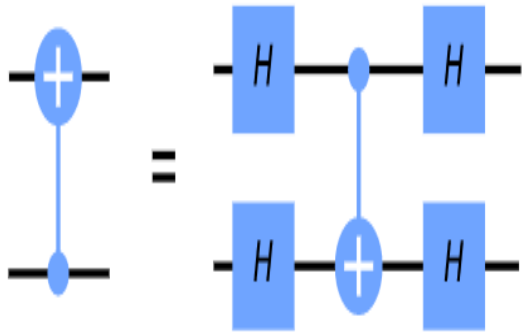
Phase kickback

- This circuit makes it possible to create a kind of CNOT gate upside down.
- We sandwich a CNOT gate between 2 pairs of Hadamard gates on each qubit.



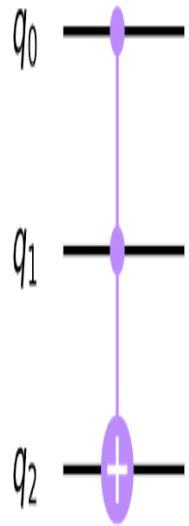
Phase kickback

- This circuit makes it possible to create a kind of CNOT gate upside down.
- We sandwich a CNOT gate between 2 pairs of Hadamard gates on each qubit.
- Phase reversal is useful in some quantum circuits, where one needs to change the control qubit of the CNOT gate



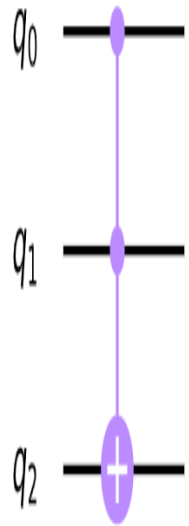
Toffoli gate

- The Toffoli gate is a 3 qubit gate, of which 2 are control qubits and 1 target qubit.



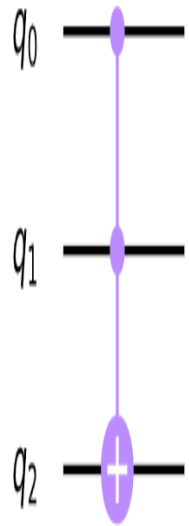
Toffoli gate

- The Toffoli gate is a 3 qubit gate, of which 2 are control qubits and 1 target qubit.
- It operates an X gate on the target if and only if the 2 control qubits are in the $|1\rangle$ state.



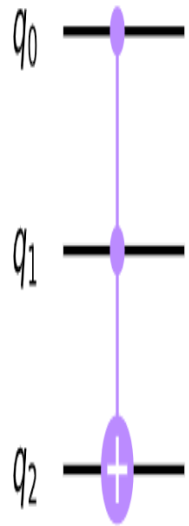
Toffoli gate

- The Toffoli gate is a 3 qubit gate, of which 2 are control qubits and 1 target qubit.
- It operates an X gate on the target if and only if the 2 control qubits are in the $|1\rangle$ state.
- It is a kind of a NOT gate with double control, sometimes denoted by CCX, which can be built with 1 and 2 qubit gates.



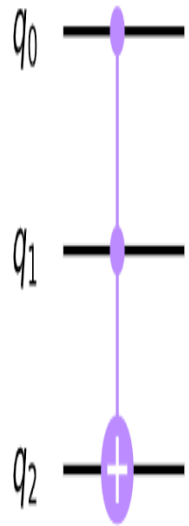
Toffoli gate

- The Toffoli gate is a 3 qubit gate, of which 2 are control qubits and 1 target qubit.
- It operates an X gate on the target if and only if the 2 control qubits are in the $|1\rangle$ state.
- It is a kind of a NOT gate with double control, sometimes denoted by CCX, which can be built with 1 and 2 qubit gates.
- Its main interest is to produce AND and NAND gates necessary for quantum computation.



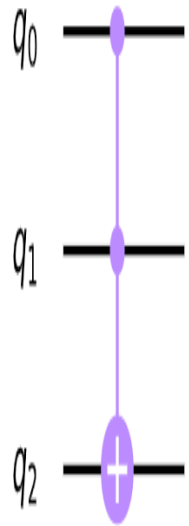
Toffoli gate

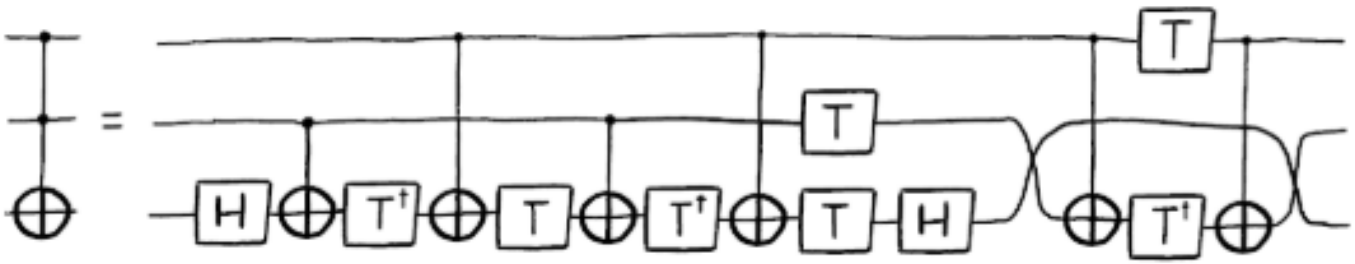
- The Toffoli gate is a 3 qubit gate, of which 2 are control qubits and 1 target qubit.
- It operates an X gate on the target if and only if the 2 control qubits are in the $|1\rangle$ state.
- It is a kind of a NOT gate with double control, sometimes denoted by CCX, which can be built with 1 and 2 qubit gates.
- Its main interest is to produce AND and NAND gates necessary for quantum computation.
- Exercise ☺: Write the matrix of the Toffoli gate.



Toffoli gate

- The Toffoli gate is a 3 qubit gate, of which 2 are control qubits and 1 target qubit.
- It operates an X gate on the target if and only if the 2 control qubits are in the $|1\rangle$ state.
- It is a kind of a NOT gate with double control, sometimes denoted by CCX, which can be built with 1 and 2 qubit gates.
- Its main interest is to produce AND and NAND gates necessary for quantum computation.
- Exercise ☺: Write the matrix of the Toffoli gate.
- Exercise ☺: Check the equivalence scheme below





What is a quantum circuit?

- In general, what is a quantum circuit?

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.
- A quantum calculation is repeated a large number of times, and the results are measurement probabilities.

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.
- A quantum calculation is repeated a large number of times, and the results are measurement probabilities.
- It is therefore necessary to repeat the cycle:

,

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.
- A quantum calculation is repeated a large number of times, and the results are measurement probabilities.
- It is therefore necessary to repeat the cycle:
  - (re)initialization (or reset to zero of the states of the input qubits,

,

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.
- A quantum calculation is repeated a large number of times, and the results are measurement probabilities.
- It is therefore necessary to repeat the cycle:
  - (re)initialization (or reset to zero of the states of the input qubits,
  - succession of unitary transformations operated by quantum gates,

,

What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.
- A quantum calculation is repeated a large number of times, and the results are measurement probabilities.
- It is therefore necessary to repeat the cycle:
  - (re)initialization (or reset to zero of the states of the input qubits,
  - succession of unitary transformations operated by quantum gates,
  - state measurements of some qubits

,

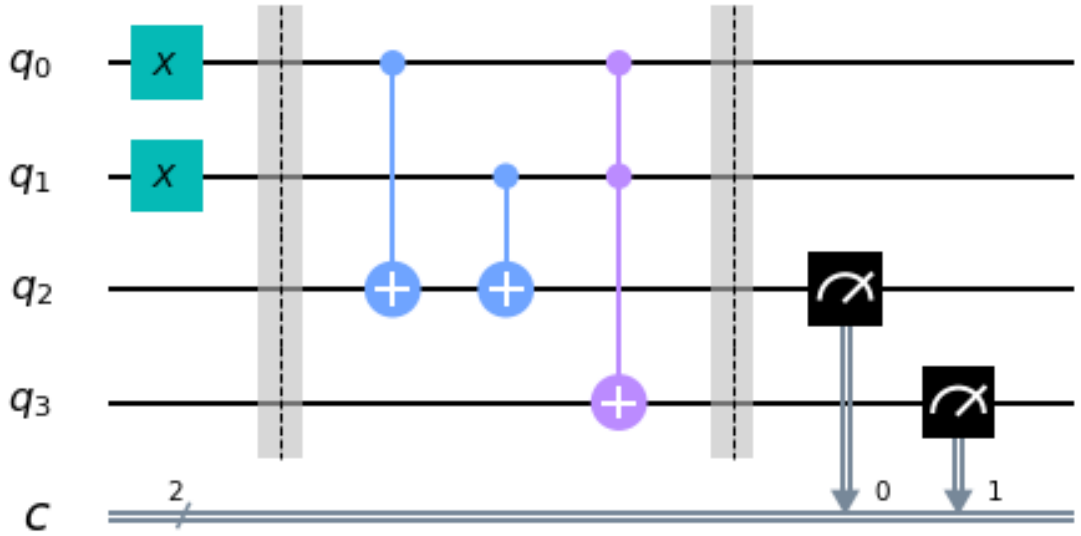
What is a quantum circuit?

- In general, what is a quantum circuit?
- A quantum circuit is a computing device which consists of a succession of coherent operations on qubits and of concomitant classical calculations in real time.
- The quantum circuit is an ordered series of quantum gates, measurements and resets, the whole being conditioned by the use of data resulting from classical calculations in real time.
- A quantum calculation is repeated a large number of times, and the results are measurement probabilities.
- It is therefore necessary to repeat the cycle:
  - (re)initialization (or reset to zero of the states of the input qubits,
  - succession of unitary transformations operated by quantum gates,
  - state measurements of some qubits
  - writing of the measurement results in conventional classical registers, either to read them directly as results of quantum computation, or to reuse them in a new iterative computation cycle.

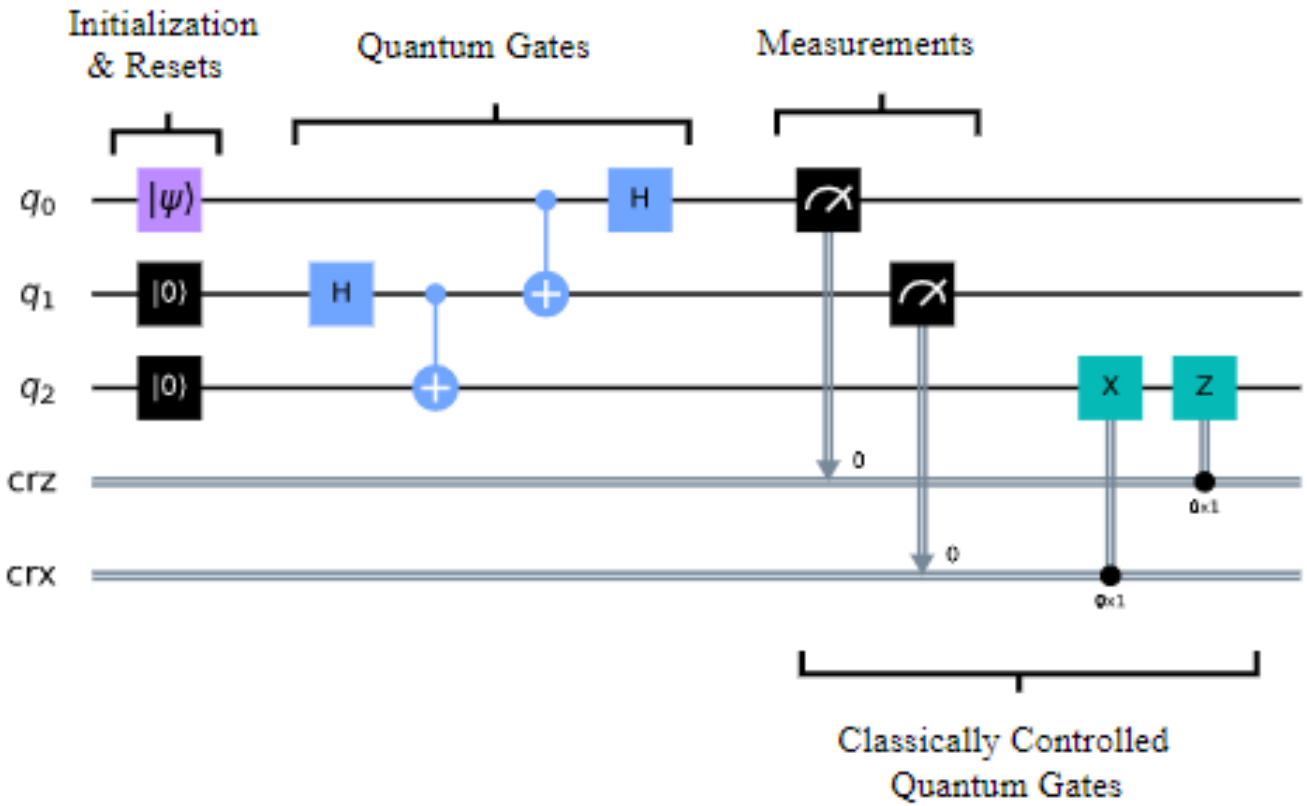
,

Example 1: Half-adder circuit

- Here again is a half-adder quantum circuit:



Example 2: Teleportation circuit



Why is there a classic part?

- Although a universal quantum computer can perform all the calculations that a classical computer can perform, classical parts are always added to quantum circuits, because quantum states are fragile, due to the phenomena of decoherence.

Why is there a classic part?

- Although a universal quantum computer can perform all the calculations that a classical computer can perform, classical parts are always added to quantum circuits, because quantum states are fragile, due to the phenomena of decoherence.
- Because of the postulate of wavepacket collapse, a measurement on a quantum system irreversibly changes its state and generates a loss of information on its state prior to the measurement.
- In most algorithms, we measure the qubits so that we can send the results through stable classical channels instead of noisy and fragile quantum channels.

Why is there a classic part?

- Although a universal quantum computer can perform all the calculations that a classical computer can perform, classical parts are always added to quantum circuits, because quantum states are fragile, due to the phenomena of decoherence.
- Because of the postulate of wavepacket collapse, a measurement on a quantum system irreversibly changes its state and generates a loss of information on its state prior to the measurement.
- In most algorithms, we measure the qubits so that we can send the results through stable classical channels instead of noisy and fragile quantum channels.

Why is there a classic part?

- Although a universal quantum computer can perform all the calculations that a classical computer can perform, classical parts are always added to quantum circuits, because quantum states are fragile, due to the phenomena of decoherence.
- Because of the postulate of wavepacket collapse, a measurement on a quantum system irreversibly changes its state and generates a loss of information on its state prior to the measurement.
- In most algorithms, we measure the qubits so that we can send the results through stable classical channels instead of noisy and fragile quantum channels.
- Finally, we need to use the results of quantum computation in a classical form that we can use in practice.

Quantum algorithms

- Several quantum algorithms have been proposed and implemented. Here is a list of the main ones:

Quantum algorithms

- Several quantum algorithms have been proposed and implemented. Here is a list of the main ones:
  - Deutsch's and Deutsch-Jozsa Algorithms
  - Bernstein-Vazirani Algorithm
  - Simon's Algorithm
  - Quantum counting
  - Quantum Teleportation
  - Shor's Algorithm
  - Grover's Algorithm
  - Quantum Key Distribution (Quantum Cryptography)
  - Quantum Fourier Transform (QFT)
  - Super-dense Coding
  - Quantum Phase Estimation (QPE)
  - Variationl Quantum Eigensolver (VQE)

Quantum algorithms

- Several quantum algorithms have been proposed and implemented. Here is a list of the main ones:
  - Deutsch's and Deutsch-Jozsa Algorithms
  - Bernstein-Vazirani Algorithm
  - Simon's Algorithm
  - Quantum counting
  - Quantum Teleportation
  - Shor's Algorithm
  - Grover's Algorithm
  - Quantum Key Distribution (Quantum Cryptography)
  - Quantum Fourier Transform (QFT)
  - Super-dense Coding
  - Quantum Phase Estimation (QPE)
  - Variationl Quantum Eigensolver (VQE)
- In this lecture, we will have time to see some of these algorithms: Quantum Teleportation and Quantum Cryptography

Quantum Teleportation & non-cloning theorem

- Alice wants to send a qubit q_0 to Bob (more precisely the quantum state of the qubit q_0). However, the quantum non-cloning theorem prohibits this operation if the only parties involved are the sender (Alice) and the receiver (Bob).
- If $|\chi\rangle$ is any state of system A (for example a qubit), it is not possible to clone it, *i.e.* to copy it to a system B (for example another qubit).

Quantum Teleportation & non-cloning theorem

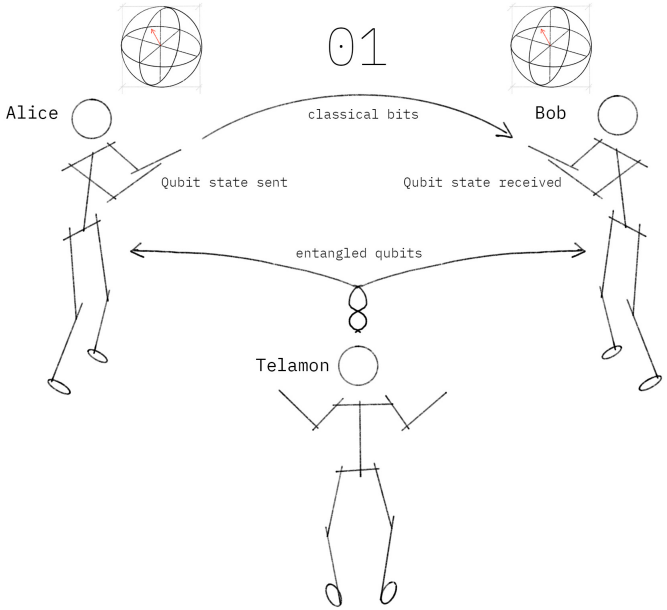
- Alice wants to send a qubit q_0 to Bob (more precisely the quantum state of the qubit q_0). However, the quantum non-cloning theorem prohibits this operation if the only parties involved are the sender (Alice) and the receiver (Bob).
- If $|\chi\rangle$ is any state of system A (for example a qubit), it is not possible to clone it, *i.e.* to copy it to a system B (for example another qubit).
- This result is known as "Quantum non-cloning theorem".

Quantum Teleportation & non-cloning theorem

- Alice wants to send a qubit q_0 to Bob (more precisely the quantum state of the qubit q_0). However, the quantum non-cloning theorem prohibits this operation if the only parties involved are the sender (Alice) and the receiver (Bob).
- If $|\chi\rangle$ is any state of system A (for example a qubit), it is not possible to clone it, *i.e.* to copy it to a system B (for example another qubit).
- This result is known as "Quantum non-cloning theorem".
- See Appendix 4 for proof.

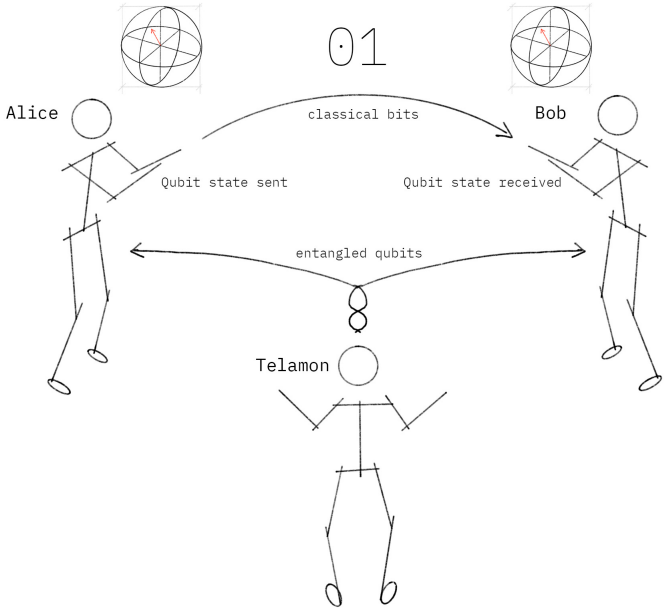
Teleportation protocol

- Alice and Bob call on a third partner (Telamon) who sends each a qubit that is part of a pair of entangled qubits (q_1 for Alice and q_2 for Bob).



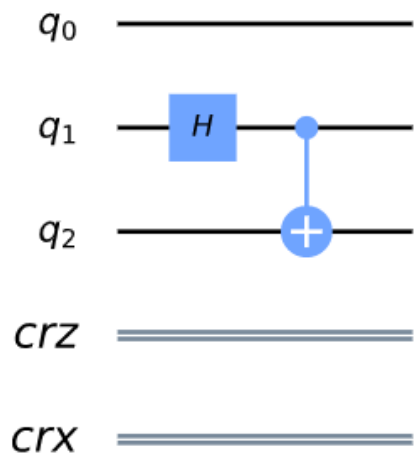
Teleportation protocol

- Alice and Bob call on a third partner (Telamon) who sends each a qubit that is part of a pair of entangled qubits (q_1 for Alice and q_2 for Bob).
- Telamon uses a special pair which is a Bell pair, in which both qubits are in a Bell entangled state.

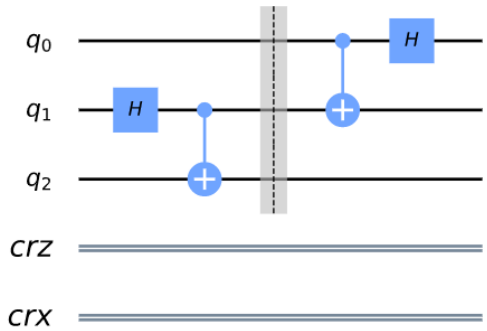


Teleportation protocol

- The translation in terms of quantum circuit of this preparation step is the first piece :
- The qubit q_0 passes a Hadamard gate which creates a $|+\rangle$ state. Then apply a $CNOT$ gate on the other qubit q_1 controlled by q_0.

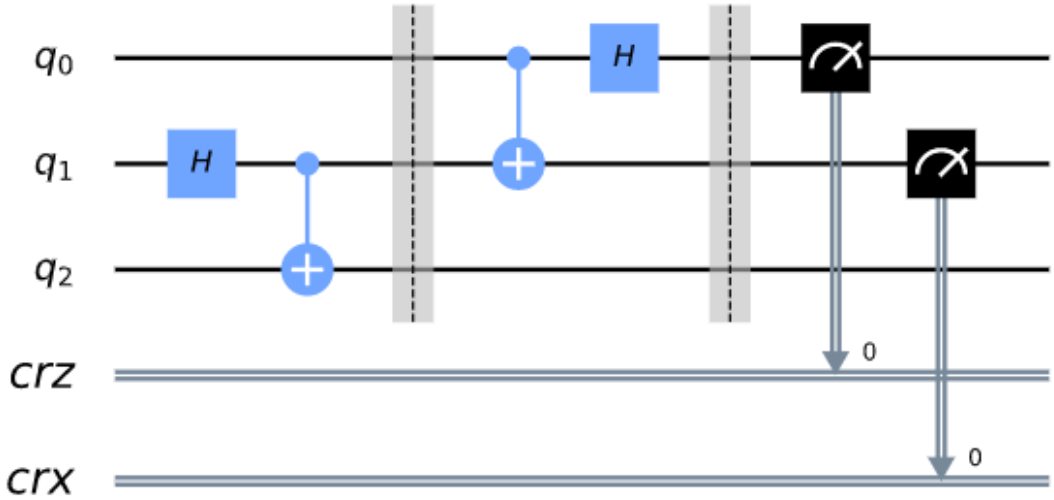


- Alice applies a $CNOT$ gate to q_1 controlled by q_0. Next, a Hadamard gate on q_0 that she wants to send to Bob.



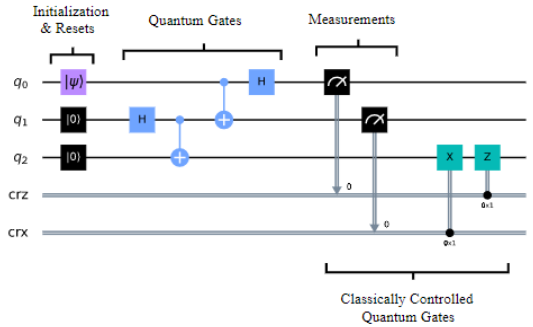
Teleportation protocol

Then, Alice measures the 2 qubits q_1 and q_0 and records the results in two standard bits. Then she sends these 2 classic bits to Bob through a classic channel.



Teleportation protocol

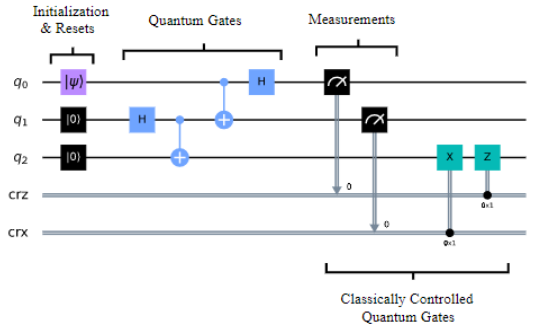
- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:



Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

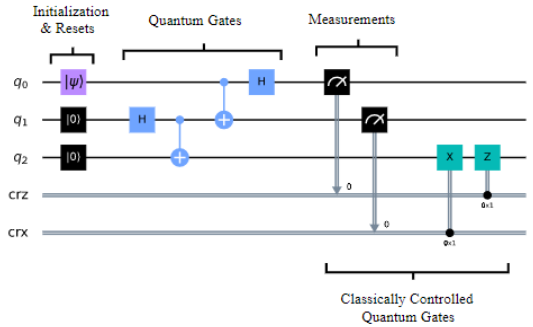
- $00 \longrightarrow$ Nothing to do



Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

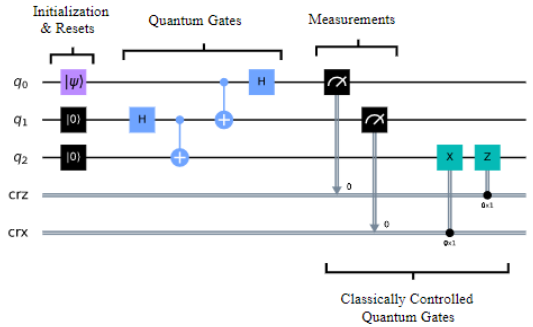
- 00 $\longrightarrow$ Nothing to do
- 01 $\longrightarrow$ Apply X gate



Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

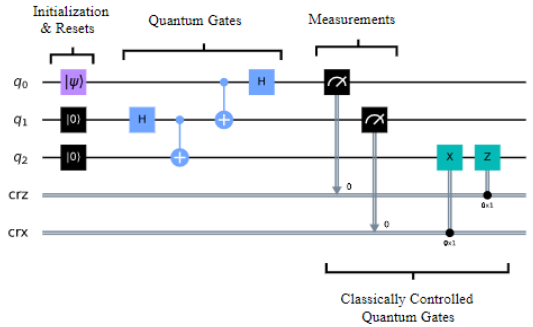
- 00 $\longrightarrow$ Nothing to do
- 01 $\longrightarrow$ Apply X gate
- 10 $\longrightarrow$ Apply Z gate



Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

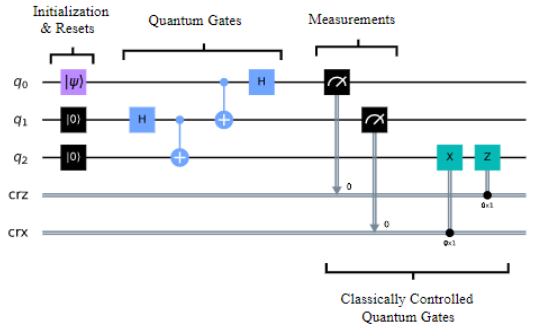
- $00 \longrightarrow$ Nothing to do
- $01 \longrightarrow$ Apply X gate
- $10 \longrightarrow$ Apply Z gate
- $11 \longrightarrow$ Apply ZX gate



Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

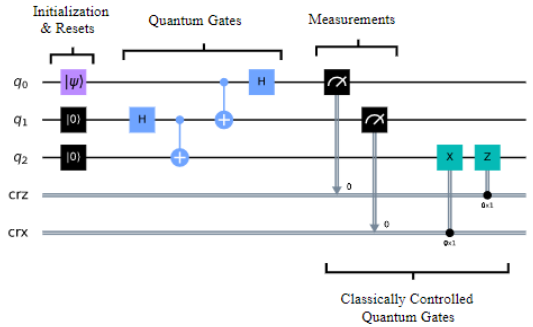
- $00 \longrightarrow$ Nothing to do
- $01 \longrightarrow$ Apply X gate
- $10 \longrightarrow$ Apply Z gate
- $11 \longrightarrow$ Apply ZX gate



Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

- $00 \longrightarrow$ Nothing to do
- $01 \longrightarrow$ Apply X gate
- $10 \longrightarrow$ Apply Z gate
- $11 \longrightarrow$ Apply ZX gate

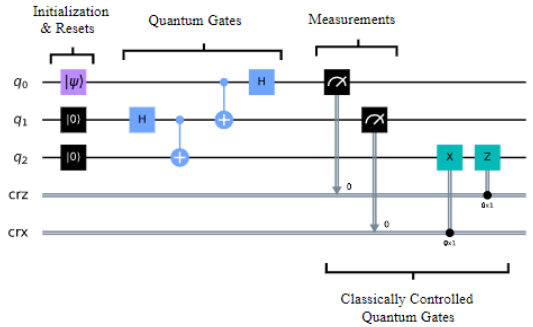


- Note here that this information transfer is purely classical.

Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

- $00 \longrightarrow$ Nothing to do
- $01 \longrightarrow$ Apply X gate
- $10 \longrightarrow$ Apply Z gate
- $11 \longrightarrow$ Apply ZX gate

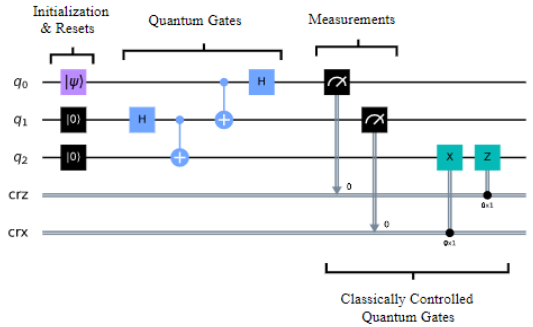


- Note here that this information transfer is purely classical.
- That's it ! At the end of the protocol, Alice's qubit q_0 was teleported to Bob. Let us insist on the fact that it is not the qubit itself which has been teleported, but a state of the qubit.

Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

- $00 \longrightarrow$ Nothing to do
- $01 \longrightarrow$ Apply X gate
- $10 \longrightarrow$ Apply Z gate
- $11 \longrightarrow$ Apply ZX gate

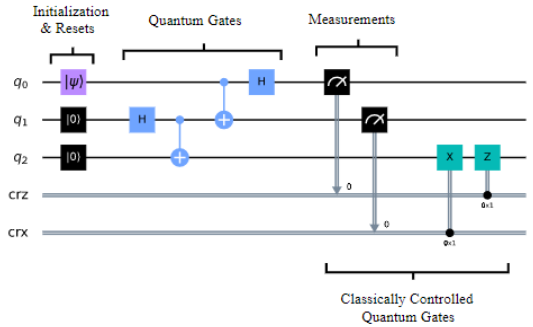


- Note here that this information transfer is purely classical.
- That's it ! At the end of the protocol, Alice's qubit q_0 was teleported to Bob. Let us insist on the fact that it is not the qubit itself which has been teleported, but a state of the qubit.
- Specifically, Bob reconstructed the quantum state that Alice sent him, thanks to the invaluable help of Telamon and his entangled qubits.

Teleportation protocol

- Bob, who had already received the qubit q_2 from Telamon, applies one of the following gates to it depending on the state of the classic bit sent by Alice:

- $00 \longrightarrow$ Nothing to do
- $01 \longrightarrow$ Apply X gate
- $10 \longrightarrow$ Apply Z gate
- $11 \longrightarrow$ Apply ZX gate



- Note here that this information transfer is purely classical.
- That's it ! At the end of the protocol, Alice's qubit q_0 was teleported to Bob. Let us insist on the fact that it is not the qubit itself which has been teleported, but a state of the qubit.
- Specifically, Bob reconstructed the quantum state that Alice sent him, thanks to the invaluable help of Telamon and his entangled qubits.
- So: No entanglement, no Quantum Teleportation!

Quantum Cryptography

- The objective of encryption is to secure communications between the sender (Alice) and the receiver (Bob) against the intrusions of a possible spy (Eve).

Quantum Cryptography

- The objective of encryption is to secure communications between the sender (Alice) and the receiver (Bob) against the intrusions of a possible spy (Eve).
- We have already studied the RSA protocol and seen how the difficulty of breaking the code comes from the virtual impossibility, with conventional computers, of finding the prime factors of the RSA number which was used for coding.

Quantum Cryptography

- The objective of encryption is to secure communications between the sender (Alice) and the receiver (Bob) against the intrusions of a possible spy (Eve).
- We have already studied the RSA protocol and seen how the difficulty of breaking the code comes from the virtual impossibility, with conventional computers, of finding the prime factors of the RSA number which was used for coding.
- The advent of quantum computing, and in particular the publication in 1994 of a quantum factorization algorithm by Peter Shor, raised the alarm on the possibility that very soon, a quantum computer could factorize RSA numbers in a very short time and undermine thus the building on which almost all the computer security of exchanges is based!

Quantum Cryptography

- The objective of encryption is to secure communications between the sender (Alice) and the receiver (Bob) against the intrusions of a possible spy (Eve).
- We have already studied the RSA protocol and seen how the difficulty of breaking the code comes from the virtual impossibility, with conventional computers, of finding the prime factors of the RSA number which was used for coding.
- The advent of quantum computing, and in particular the publication in 1994 of a quantum factorization algorithm by Peter Shor, raised the alarm on the possibility that very soon, a quantum computer could factorize RSA numbers in a very short time and undermine thus the building on which almost all the computer security of exchanges is based!
- At the same time, the idea germinated to use the quantum properties themselves (superposition / entanglement) to design quantum cryptography algorithms which would thus be almost inviolable.

Quantum cryptography

- Alice wants to send Bob confidential information (for example a password or the code of a bank card).

Quantum cryptography

- Alice wants to send Bob confidential information (for example a password or the code of a bank card).
- Unless she whispers the message in her ear, Alice is forced to go through a communication channel, to which possibly other people (eg Eve) have access.

Quantum cryptography

- Alice wants to send Bob confidential information (for example a password or the code of a bank card).
- Unless she whispers the message in her ear, Alice is forced to go through a communication channel, to which possibly other people (eg Eve) have access.
- If this channel is traditional (telephone line, messaging, ...), the confidentiality of the communication is based on an RSA type protocol or on the confidence that Alice and Bob have in Eve. Indeed if Eve decides to spy on this channel, neither Alice nor Bob would realize it.

Quantum cryptography

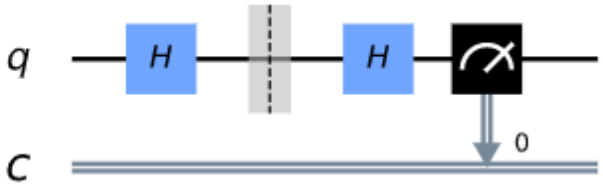
- Alice wants to send Bob confidential information (for example a password or the code of a bank card).
- Unless she whispers the message in her ear, Alice is forced to go through a communication channel, to which possibly other people (eg Eve) have access.
- If this channel is traditional (telephone line, messaging, ...), the confidentiality of the communication is based on an RSA type protocol or on the confidence that Alice and Bob have in Eve. Indeed if Eve decides to spy on this channel, neither Alice nor Bob would realize it.
- The idea is to use a quantum channel, so that if Eve dares to spy on the message sent by Alice, Bob will eventually find out, which should allow her to make further arrangements to secure this data. .

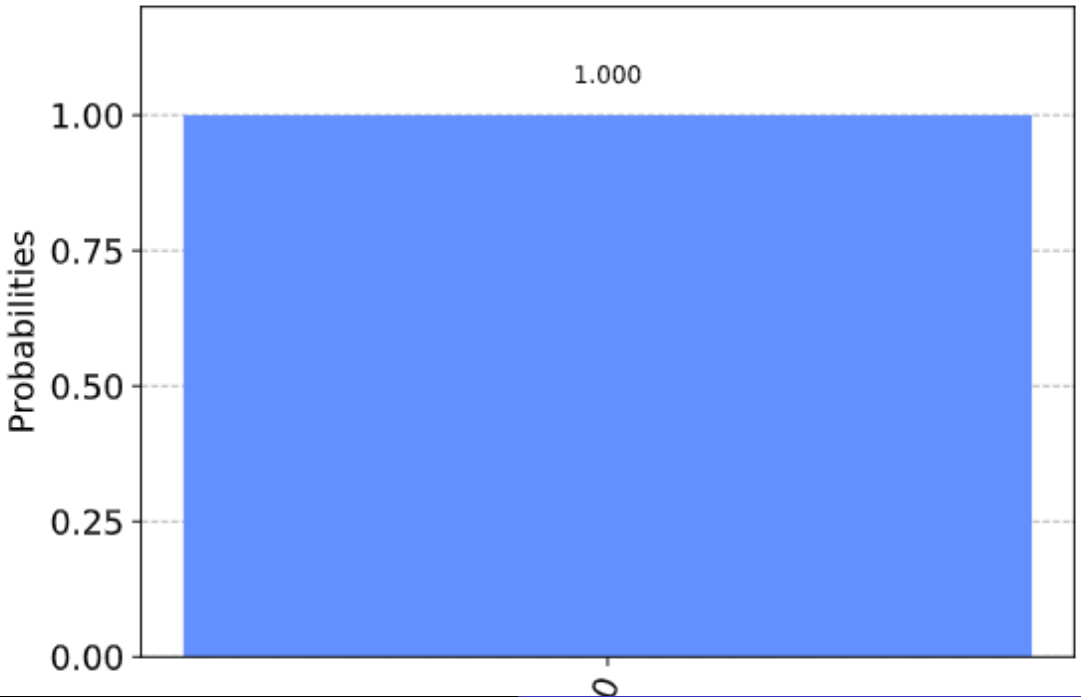
Quantum cryptography

- Alice wants to send Bob confidential information (for example a password or the code of a bank card).
- Unless she whispers the message in her ear, Alice is forced to go through a communication channel, to which possibly other people (eg Eve) have access.
- If this channel is traditional (telephone line, messaging, ...), the confidentiality of the communication is based on an RSA type protocol or on the confidence that Alice and Bob have in Eve. Indeed if Eve decides to spy on this channel, neither Alice nor Bob would realize it.
- The idea is to use a quantum channel, so that if Eve dares to spy on the message sent by Alice, Bob will eventually find out, which should allow her to make further arrangements to secure this data. .
- Schematically, this is based on the fact that on a quantum system, spying, which results in a measurement, alters the quantum state of the qubit, unlike a conventional channel and this alteration can be detected by Bob.

How does it work ?

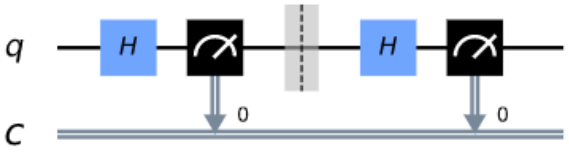
- If Alice prepares the qubit in the state $|+\rangle$, which is the eigenstate $|0\rangle$ of the gate X, and if Bob measures the state in the same base, he is certain always get the result $|0\rangle$ with a probability of 100 %.

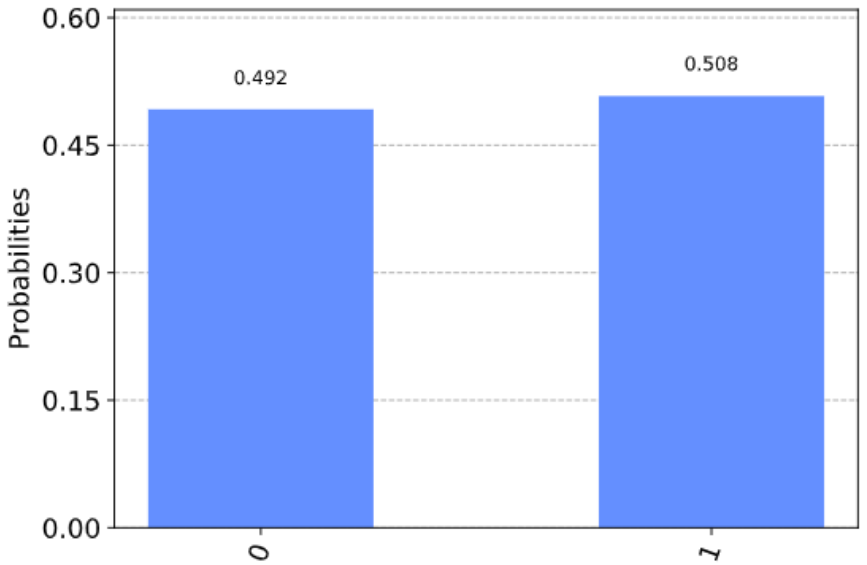




How it works ?

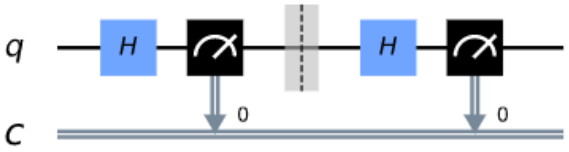
- But if Eve wants to intercept the message by measuring the state of the system by a gate Z (by default), she will project it on the state $|0\rangle$ or $|1\rangle$ of X with a probability of 50% each.

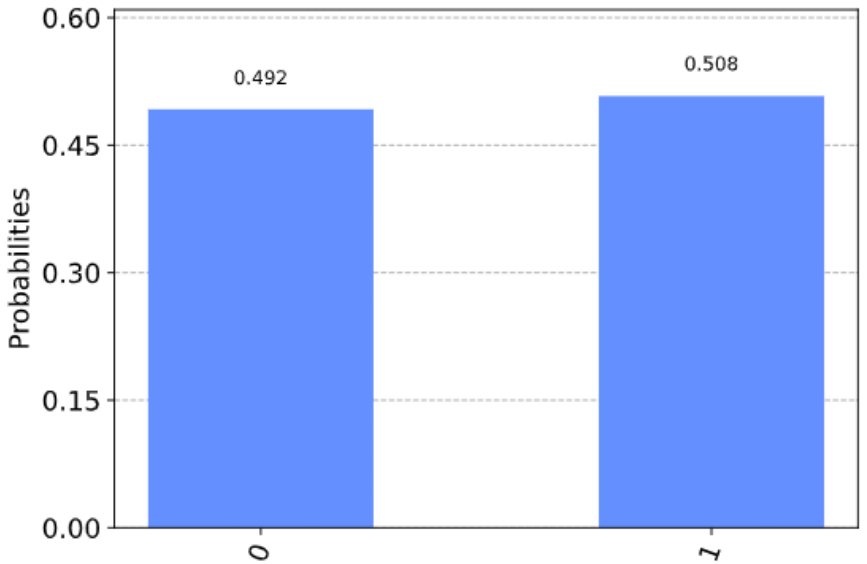




How it works ?

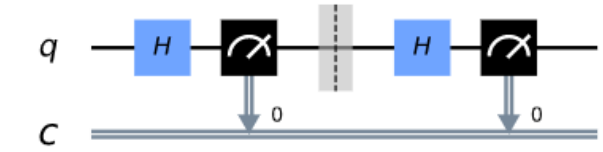
- But if Eve wants to intercept the message by measuring the state of the system by a gate Z (by default), she will project it on the state $|0\rangle$ or $|1\rangle$ of X with a probability of 50% each.
- Subsequently, If Bob measures the state with a gate X, he can no longer find the state $|0\rangle$ with certainty!

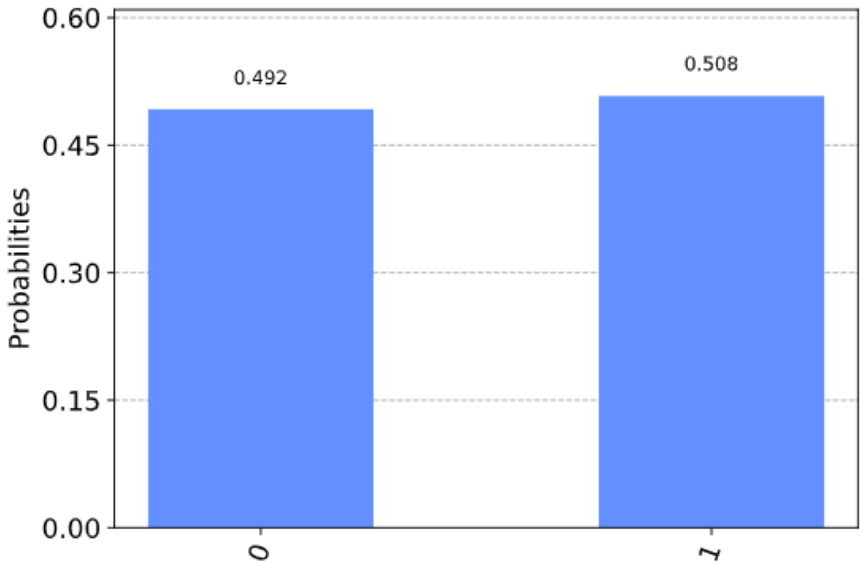




How it works ?

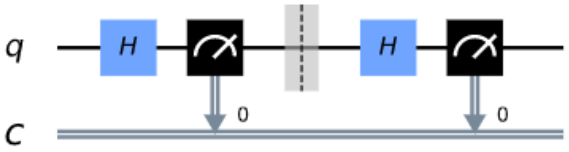
- But if Eve wants to intercept the message by measuring the state of the system by a gate Z (by default), she will project it on the state $|0\rangle$ or $|1\rangle$ of X with a probability of 50% each.
- Subsequently, If Bob measures the state with a gate X, he can no longer find the state $|0\rangle$ with certainty!
  - We see that Bob in this case has a 50% chance of measuring 0 (or 1), so Alice and Bob realize the interception of the message.

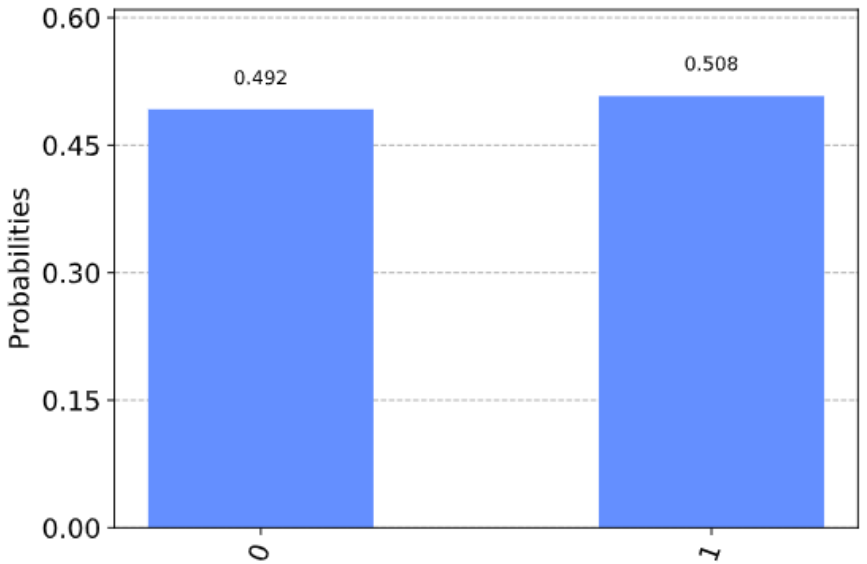




How it works ?

- But if Eve wants to intercept the message by measuring the state of the system by a gate Z (by default), she will project it on the state $|0\rangle$ or $|1\rangle$ of X with a probability of 50% each.
- Subsequently, If Bob measures the state with a gate X, he can no longer find the state $|0\rangle$ with certainty!





  - We see that Bob in this case has a 50% chance of measuring 0 (or 1), so Alice and Bob realize the interception of the message.
  - The quantum key distribution protocol relies on repeating this process enough times that Eve has virtually no chance of making her interception undetectable.

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:

    1000101011010100

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:

    $$1000101011010100$$

  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:

    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:
    $$1000101011010100$$
  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:
    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$
  - Alice makes a random choice of bases (or gates) for each bit, for example:
    $$ZZXZXXXZXZXXXXXX$$

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:
    $$1000101011010100$$
  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:
    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$
  - Alice makes a random choice of bases (or gates) for each bit, for example:
    $$ZZXZXXXZXZXXXXXX$$
  - Alice keeps these 2 pieces of information private to herself.

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:
    $$1000101011010100$$
  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:
    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$
  - Alice makes a random choice of bases (or gates) for each bit, for example:
    $$ZZXZXXXZXZXXXXXX$$
  - Alice keeps these 2 pieces of information private to herself.
- Second step :

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:
    $$1000101011010100$$
  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:
    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$
  - Alice makes a random choice of bases (or gates) for each bit, for example:
    $$ZZXZXXXZXZXXXXXX$$
  - Alice keeps these 2 pieces of information private to herself.
- Second step :
  - Alice applies the gates to each qubit, whose initial state is defined by the value of the corresponding bit

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:
    $$1000101011010100$$
  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:
    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$
  - Alice makes a random choice of bases (or gates) for each bit, for example:
    $$ZZXZXXXZXZXXXXXX$$
  - Alice keeps these 2 pieces of information private to herself.
- Second step :
  - Alice applies the gates to each qubit, whose initial state is defined by the value of the corresponding bit
  - In the example chosen, this gives:
    $$|1\rangle|0\rangle|+\rangle|1\rangle|-\rangle|+\rangle|-\rangle|0\rangle|-\rangle|1\rangle|+\rangle|-\rangle|+\rangle|-\rangle|+\rangle|+\rangle$$

Quantum key distribution protocol

The quantum key distribution protocol takes place in 5 steps.

- First stage :
  - Alice chooses a string of random bits, for example a 16-bit register:
    $$1000101011010100$$
  - Alice prepares the initial state of the qubit string according to the values of the corresponding classic bits:
    $$|1\rangle|0\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle|0\rangle$$
  - Alice makes a random choice of bases (or gates) for each bit, for example:
    $$ZZXZXXXZXZXXXXXX$$
  - Alice keeps these 2 pieces of information private to herself.
- Second step :
  - Alice applies the gates to each qubit, whose initial state is defined by the value of the corresponding bit
  - In the example chosen, this gives:
    $$|1\rangle|0\rangle|+\rangle|1\rangle|-\rangle|+\rangle|-\rangle|0\rangle|-\rangle|1\rangle|+\rangle|-\rangle|+\rangle|-\rangle|+\rangle|+\rangle$$
  - This is the message Alice sends to Bob.

Protocol (continued)

- Third step :

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.
- Fourth step :

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.
- Fourth step :
  - Bob and Alice publicly exchange the bases (or gates) that each has used for each qubit (16 in all for each of them).

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.
- Fourth step :
  - Bob and Alice publicly exchange the bases (or gates) that each has used for each qubit (16 in all for each of them).
  - If Bob used the same basis for measurement as Alice for state preparation for a given qubit of the sequence, he retains it as part of their secret key, otherwise he discards the information for this qubit.

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.
- Fourth step :
  - Bob and Alice publicly exchange the bases (or gates) that each has used for each qubit (16 in all for each of them).
  - If Bob used the same basis for measurement as Alice for state preparation for a given qubit of the sequence, he retains it as part of their secret key, otherwise he discards the information for this qubit.
- Fifth step :

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.
- Fourth step :
  - Bob and Alice publicly exchange the bases (or gates) that each has used for each qubit (16 in all for each of them).
  - If Bob used the same basis for measurement as Alice for state preparation for a given qubit of the sequence, he retains it as part of their secret key, otherwise he discards the information for this qubit.
- Fifth step :
  - Eventually, Bob and Alice publicly share a sample of their keys.

Protocol (continued)

- Third step :
  - Bob measures the state of each qubit randomly using a series of gates, for example:

    XZZZXZXZXZXZZZXZ

    and this of course without prior knowledge of the bases chosen by Alice.
  - Bob keeps the results of the measurements and does not disseminate them.
- Fourth step :
  - Bob and Alice publicly exchange the bases (or gates) that each has used for each qubit (16 in all for each of them).
  - If Bob used the same basis for measurement as Alice for state preparation for a given qubit of the sequence, he retains it as part of their secret key, otherwise he discards the information for this qubit.
- Fifth step :
  - Eventually, Bob and Alice publicly share a sample of their keys.
  - If the keys match, they can be sure (with a small margin of error though) that the transmission is successful and secure.

Post-Quantum era

THE NATIONAL LAW REVIEW

July 30, 2021
Volume XI, Number 211

65
NEW ARTICLES

Preparing for the Post-Quantum Migration: A Race to Save the Internet

Thursday, July 29, 2021

Most people don't know or care to know, about cryptography. Without cryptography, the internet privacy that we all rely on for transmitting virtually all forms of digital communication would be insecure from attackers. Our current encryption methods are threatened by the breakthrough in quantum computing. Unless proactive steps are taken to mitigate this threat, large-scale quantum computers will tear down the backbone of the internet, secure communications.

Article By

Robert M. Botkin

Womble Bond Dickinson (US) LLP
HeyDataData

WOMBLE BOND DICKINSON

Conclusion of lecture 3

- Review of Quantum gates (1-qubit and n-qubits gates)

Conclusion of lecture 3

- Review of Quantum gates (1-qubit and n-qubits gates)
- First example of Quantm circuit : Half-adder

Conclusion of lecture 3

- Review of Quantum gates (1-qubit and n-qubits gates)
- First example of Quantm circuit : Half-adder
- Review of main Quantum algorithims

Conclusion of lecture 3

- Review of Quantum gates (1-qubit and n-qubits gates)
- First example of Quantm circuit : Half-adder
- Review of main Quantum algorithims
- Applications: Teleportation and Quantum cryptography

General conclusion

- In this series of lectures we have briefly reviewed :

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation
- We did not address several important issues :

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation
- We did not address several important issues :
  - Quantum algorithms (QFT, QPE, Grover, Shor, ...)

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation
- We did not address several important issues :
  - Quantum algorithms (QFT, QPE, Grover, Shor, ...)
  - Quantum code error corrections

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation
- We did not address several important issues :
  - Quantum algorithms (QFT, QPE, Grover, Shor, ...)
  - Quantum code error corrections
  - Other fundamental and practical issues

General conclusion

- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation
- We did not address several important issues :
  - Quantum algorithms (QFT, QPE, Grover, Shor, ...)
  - Quantum code error corrections
  - Other fundamental and practical issues
- Several platforms are available for intersted people to get introduced to Quantum computing, e.g., IBM : www.qiskit.org

General conclusion

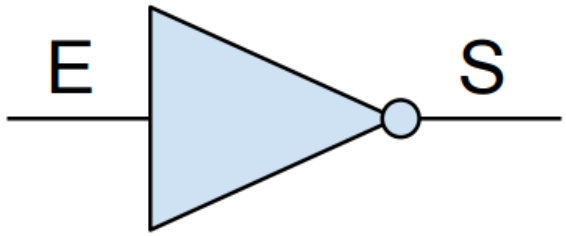
- In this series of lectures we have briefly reviewed :
  - Shannon information theory
  - Quantum mechanics tools for quantum information
  - Quantum information main features including examples of quantum cryptography and teleportation
- We did not address several important issues :
  - Quantum algorithms (QFT, QPE, Grover, Shor, ...)
  - Quantum code error corrections
  - Other fundamental and practical issues
- Several platforms are available for intersted people to get introduced to Quantum computing, e.g., IBM : www.qiskit.org
- You are most welcome to join the African Quantum community through various initiatives : OneQuantum Africa, ASFAP, QWorld branches, ...

Quantum Africa

Quantum Africa

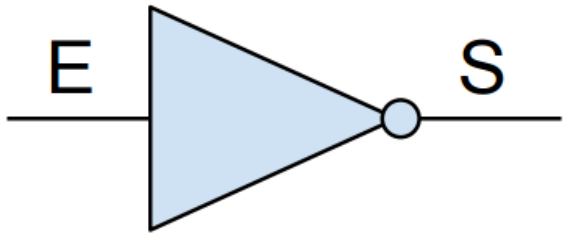
Appendix 1 : classical logic gates, NOT gate

- The NOT gate takes an input E and gives an output S. Its symbol is:



Appendix 1 : classical logic gates, NOT gate

- The NOT gate takes an input E and gives an output S. Its symbol is:

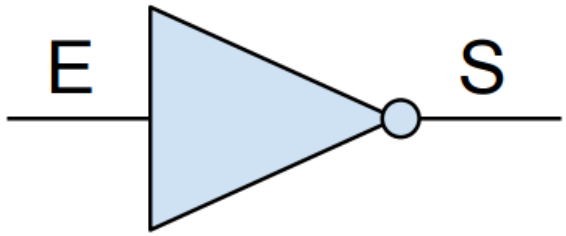


- The truth table is written:

E	S
0	1
1	0

Appendix 1 : classical logic gates, NOT gate

- The NOT gate takes an input E and gives an output S. Its symbol is:



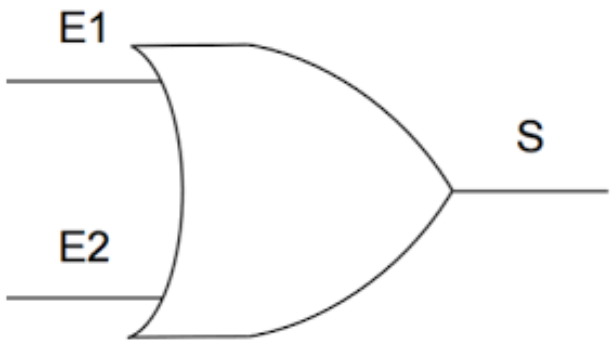
- The truth table is written:

E	S
0	1
1	0

- This gate is also called an inverter because it inverts the values of bits 0 and 1.

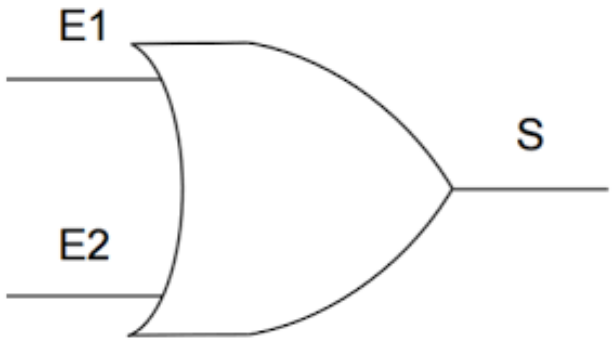
Appendix 1 : OR gate

- The OR gate takes 2 inputs E_1 and E_2 and gives an output S. Its symbol is:



Appendix 1 : OR gate

- The OR gate takes 2 inputs E_1 and E_2 and gives an output S. Its symbol is:

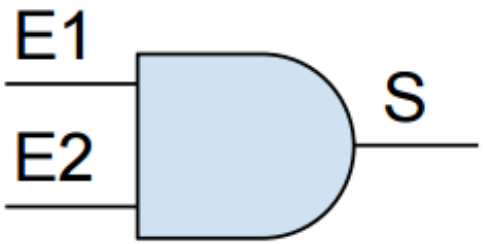


- The truth table is written:

E_1	E_2	S
0	0	0
0	1	1
1	0	1
1	1	1

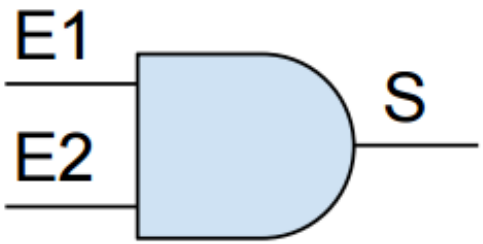
Appendix 1 : AND gate

- The AND gate takes 2 inputs E_1 and E_2 and gives an output S. Its symbol is:



Appendix 1 : AND gate

- The AND gate takes 2 inputs E_1 and E_2 and gives an output S. Its symbol is:



- The truth table is written :

E_1	E_2	S
0	0	0
0	1	0
1	0	0
1	1	1

Appendix 1 : Composite logic gates

- By combining the 3 simple gates NOT, OR and AND, we define the composite gates NAND, NOR, XOR and XNOR

Appendix 1 : Composite logic gates

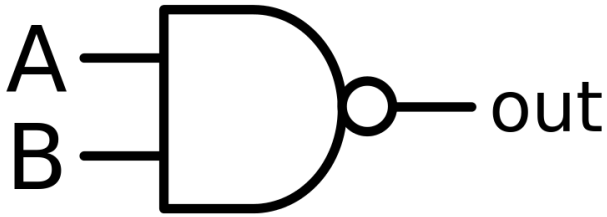
- By combining the 3 simple gates NOT, OR and AND, we define the composite gates NAND, NOR, XOR and XNOR
- Each of these gates takes 2 inputs E_1 and E_2 and gives an output S, characterized by a specific truth table.

Appendix 1 : NAND gate

- The NAND gate combines the AND and NOT gates. The name NAND is a contraction of NOT-AND.

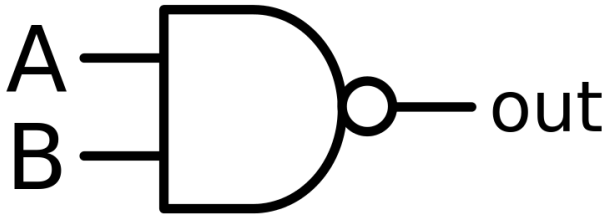
Appendix 1 : NAND gate

- The NAND gate combines the AND and NOT gates. The name NAND is a contraction of NOT-AND.
- Its symbol is:



Appendix 1 : NAND gate

- The NAND gate combines the AND and NOT gates. The name NAND is a contraction of NOT-AND.
- Its symbol is:



- The truth table is :

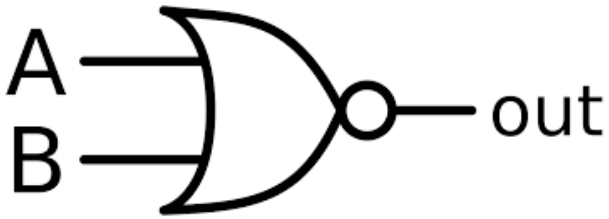
E_1	E_2	S
0	0	1
0	1	1
1	0	1
1	1	0

Appendix 1 : NOR gate

- The NOR gate combines the OR and NOT gates. The name NAND is a contraction of NOT-OR.

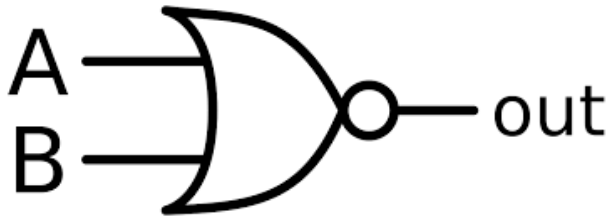
Appendix 1 : NOR gate

- The NOR gate combines the OR and NOT gates. The name NAND is a contraction of NOT-OR.
- Its symbol is:



Appendix 1 : NOR gate

- The NOR gate combines the OR and NOT gates. The name NAND is a contraction of NOT-OR.
- Its symbol is:



- The truth table is :

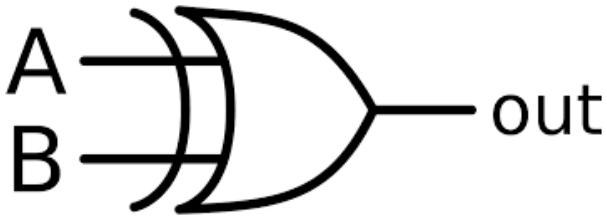
E_1	E_2	S
0	0	1
0	1	0
1	0	0
1	1	0

Appendix 1 : XOR gate

- The XOR gate is also called exclusive OR

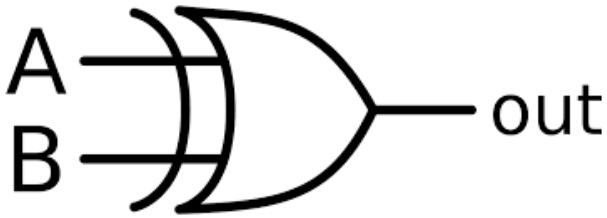
Appendix 1 : XOR gate

- The XOR gate is also called exclusive OR
- Its symbol is:



Appendix 1 : XOR gate

- The XOR gate is also called exclusive OR
- Its symbol is:



- The truth table is :

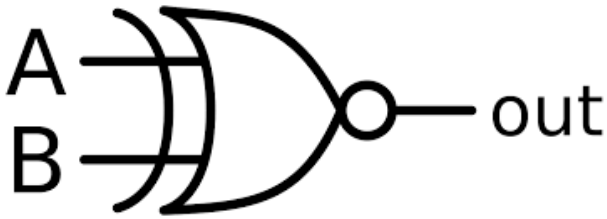
E_1	E_2	S
0	0	0
0	1	1
1	0	1
1	1	0

Appendix 1 : XNOR gate

- The XNOR gate is also called exclusive NOR

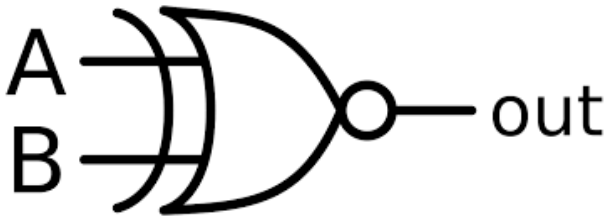
Appendix 1 : XNOR gate

- The XNOR gate is also called exclusive NOR
- Its symbol is:



Appendix 1 : XNOR gate

- The XNOR gate is also called exclusive NOR
- Its symbol is:



- The truth table is :

E_1	E_2	S
0	0	1
0	1	0
1	0	0
1	1	1

Appendix 2 : More 1-qubit Quantum gates, Gate R_ϕ

- The gate R_ϕ is represented by the matrix:

$$R_\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

where ϕ is a real number.

Appendix 2 : More 1-qubit Quantum gates, Gate R_ϕ

- The gate R_ϕ is represented by the matrix:

$$R_\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

  where ϕ is a real number.
- We can notice that for $\phi = \pi$, we find the gate Z.

Appendix 2 : More 1-qubit Quantum gates, Gate R_ϕ

- The gate R_ϕ is represented by the matrix:

$$R_\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

  where ϕ is a real number.
- We can notice that for $\phi = \pi$, we find the gate Z.
- We will see later that the gates S and T are also special cases of the gate R_ϕ

Gates I, S and T

- The I gate is the identity gate :

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

It does not change the state of the qubit.

Gates I, S and T

- The I gate is the identity gate :

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

It does not change the state of the qubit.

- The S gate is a R_ϕ gate for $\phi = -\pi/2$:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{2}} \end{bmatrix}$$

The gate S is also known as the gate $\sqrt{Z}$, because we have $S^2 = Z$.

Gates I, S and T

- The I gate is the identity gate :

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

  It does not change the state of the qubit.

- The S gate is a R_ϕ gate for $\phi = -\pi/2$:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{2}} \end{bmatrix}$$

  The gate S is also known as the gate $\sqrt{Z}$, because we have $S^2 = Z$.

- The gate T is also a gate R_ϕ for $\phi = -\pi/4$:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{bmatrix}$$

General gate U_3

- The U_3 gate is the most general of all 1 qubit gates.

General gate U_3

- The U_3 gate is the most general of all 1 qubit gates.
- Its matrix representation involves the angles θ and ϕ, defined on the Bloch sphere, as well as a parameter denoted λ:

$$U_3(\theta,\phi,\lambda) = \begin{bmatrix} \cos(\frac{\theta}{2}) & e^{-i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\phi}\sin(\frac{\theta}{2}) & e^{i(\lambda+\phi)}\cos(\frac{\theta}{2}) \end{bmatrix}$$

General gate U_3

- The U_3 gate is the most general of all 1 qubit gates.
- Its matrix representation involves the angles θ and ϕ, defined on the Bloch sphere, as well as a parameter denoted λ:

$$U_3(\theta, \phi, \lambda) = \begin{bmatrix} \cos(\frac{\theta}{2}) & e^{-i\lambda} \sin(\frac{\theta}{2}) \\ e^{i\phi} \sin(\frac{\theta}{2}) & e^{i(\lambda+\phi)} \cos(\frac{\theta}{2}) \end{bmatrix}$$

- All the gates we have just listed are special cases of the gate $U_3(\theta, \phi, \lambda)$.

General gate U_3

- The U_3 gate is the most general of all 1 qubit gates.
- Its matrix representation involves the angles θ and ϕ, defined on the Bloch sphere, as well as a parameter denoted λ:

$$U_3(\theta, \phi, \lambda) = \begin{bmatrix} \cos(\frac{\theta}{2}) & e^{-i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\phi}\sin(\frac{\theta}{2}) & e^{i(\lambda+\phi)}\cos(\frac{\theta}{2}) \end{bmatrix}$$

- All the gates we have just listed are special cases of the gate $U_3(\theta, \phi, \lambda)$.
- We also define the gates U_1 and U_2, which correspond to the cases $(\theta = \phi = 0)$ and $(\theta = \pi/2)$ respectively.

General gate U_3

- The U_3 gate is the most general of all 1 qubit gates.
- Its matrix representation involves the angles θ and ϕ, defined on the Bloch sphere, as well as a parameter denoted λ:

$$U_3(\theta, \phi, \lambda) = \begin{bmatrix} \cos(\frac{\theta}{2}) & e^{-i\lambda} \sin(\frac{\theta}{2}) \\ e^{i\phi} \sin(\frac{\theta}{2}) & e^{i(\lambda+\phi)} \cos(\frac{\theta}{2}) \end{bmatrix}$$

- All the gates we have just listed are special cases of the gate $U_3(\theta, \phi, \lambda)$.
- We also define the gates U_1 and U_2, which correspond to the cases $(\theta = \phi = 0)$ and $(\theta = \pi/2)$ respectively.
- We can also notice that the gate U_1 is nothing more than a gate R_ϕ $(\phi = \lambda)$. Indeed :

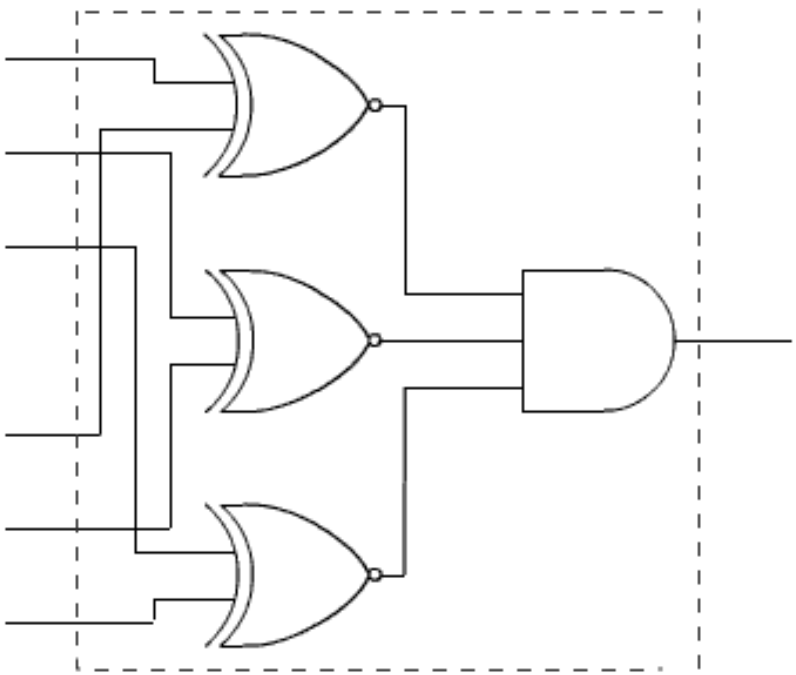
$$U_1 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{bmatrix}$$

Appendix 3 : Comparator circuit

- The comparator is a circuit which compares two words of n bits. At the output, a bit indicates the result of the comparison: 1 if there is equality between the two codes present at the input, 0 if these codes are different.

Appendix 3 : Comparator circuit

- The comparator is a circuit which compares two words of n bits. At the output, a bit indicates the result of the comparison: 1 if there is equality between the two codes present at the input, 0 if these codes are different.
- It is formed by n XNOR gates connected in parallel and an AND gate with n inputs (below is the circuit diagram for $n = 3$).



Appendix 3 : Full-adder circuit

- Take the example of the addition operation $1 + 3 = 4$ with 4-bit registers.

Appendix 3 : Full-adder circuit

- Take the example of the addition operation $1 + 3 = 4$ with 4-bit registers.
- In binary code, the addition is written:

$$\begin{array}{cccccc} & & 0 & 1 & 1 & \\ & & 0 & 0 & 0 & 1 \\ + & & & & & \\ & & 0 & 0 & 1 & 1 \\ \hline & & 0 & 1 & 0 & 0 \end{array}$$

Appendix 3 : Full-adder circuit

- Take the example of the addition operation $1 + 3 = 4$ with 4-bit registers.
- In binary code, the addition is written:

$$\begin{array}{cccccc} & & 0 & 1 & 1 & \\ & & 0 & 0 & 0 & 1 \\ + & & & & & \\ \hline & & 0 & 0 & 1 & 1 \\ \hline & & 0 & 1 & 0 & 0 \end{array}$$

- The addition of the right-hand bits is an addition of two bits, it can be done with the half-adder. In the example above, the output will give a sum $S_1 = 0$ and a carry $R_1 = 1$.

Appendix 3 : Full-adder circuit

- Take the example of the addition operation $1 + 3 = 4$ with 4-bit registers.
- In binary code, the addition is written:

$$\begin{array}{cccccc} & & 0 & 1 & 1 & \\ & & 0 & 0 & 0 & 1 \\ + & & & & & \\ & & 0 & 0 & 1 & 1 \\ \hline & & 0 & 1 & 0 & 0 \end{array}$$

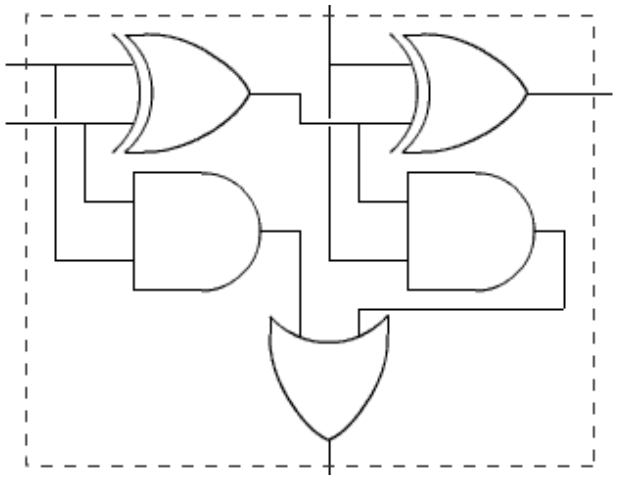
- The addition of the right-hand bits is an addition of two bits, it can be done with the half-adder. In the example above, the output will give a sum $S_1 = 0$ and a carry $R_1 = 1$.
- The sum of the next two bits requires the carryover to be taken into account (indicated at the top in red), which amounts to performing 2 additions instead of just one for the first pair of bits ($1 + 0 + 1 = 0$) with a carryover of 1 for the next column.

Appendix 3 : Full-adder circuit

- To carry out the addition, we chain a first addition without prior carry-over, and a series of additions with carry-over (3 in our example)

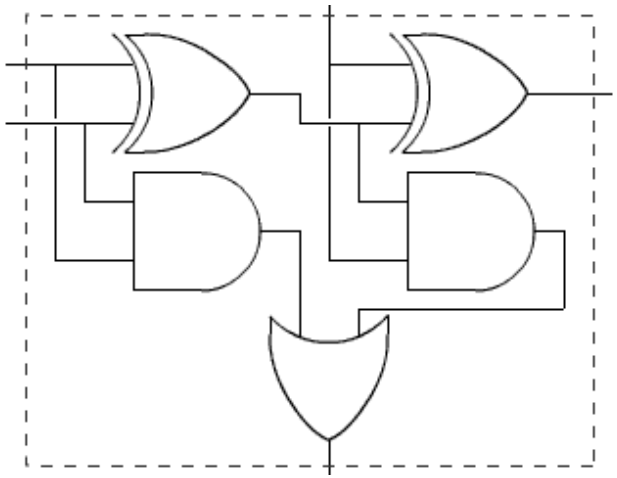
Appendix 3 : Full-adder circuit

- To carry out the addition, we chain a first addition without prior carry-over, and a series of additions with carry-over (3 in our example)
- The adder circuit must take as input 3 bits, the inputs A and B and the carry R from the previous operation. It will output the sum S and the carryforward for the next operation.



Appendix 3 : Full-adder circuit

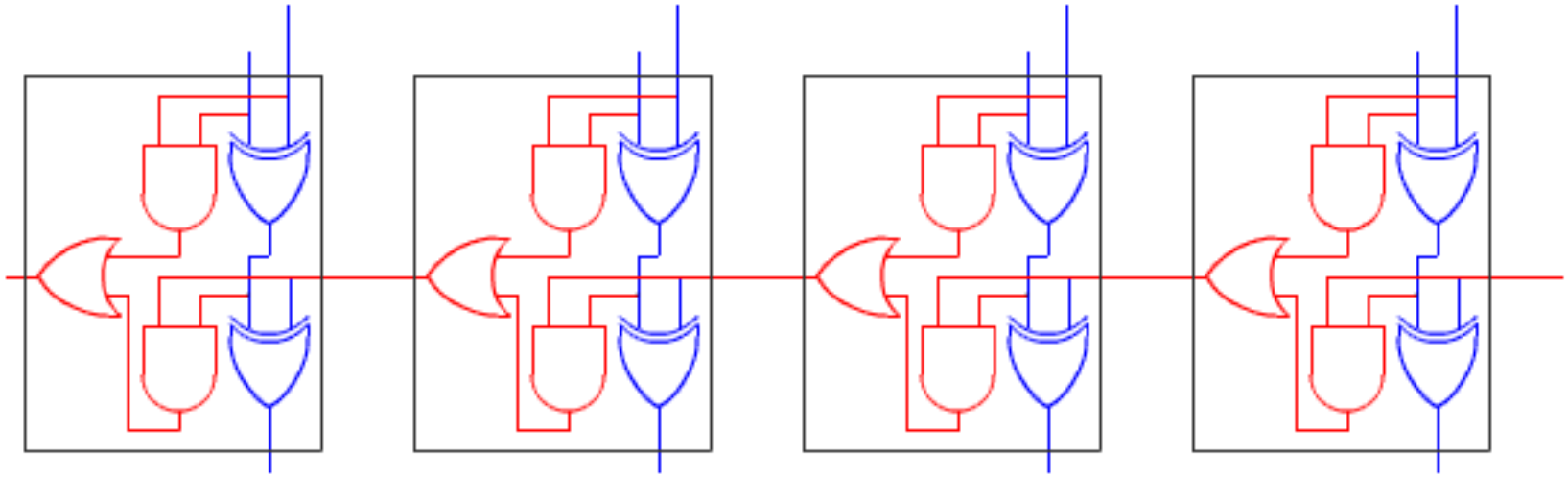
- To carry out the addition, we chain a first addition without prior carry-over, and a series of additions with carry-over (3 in our example)
- The adder circuit must take as input 3 bits, the inputs A and B and the carry R from the previous operation. It will output the sum S and the carryforward for the next operation.



- The circuit which will realize the total addition will be a cascade of full-adder circuits.

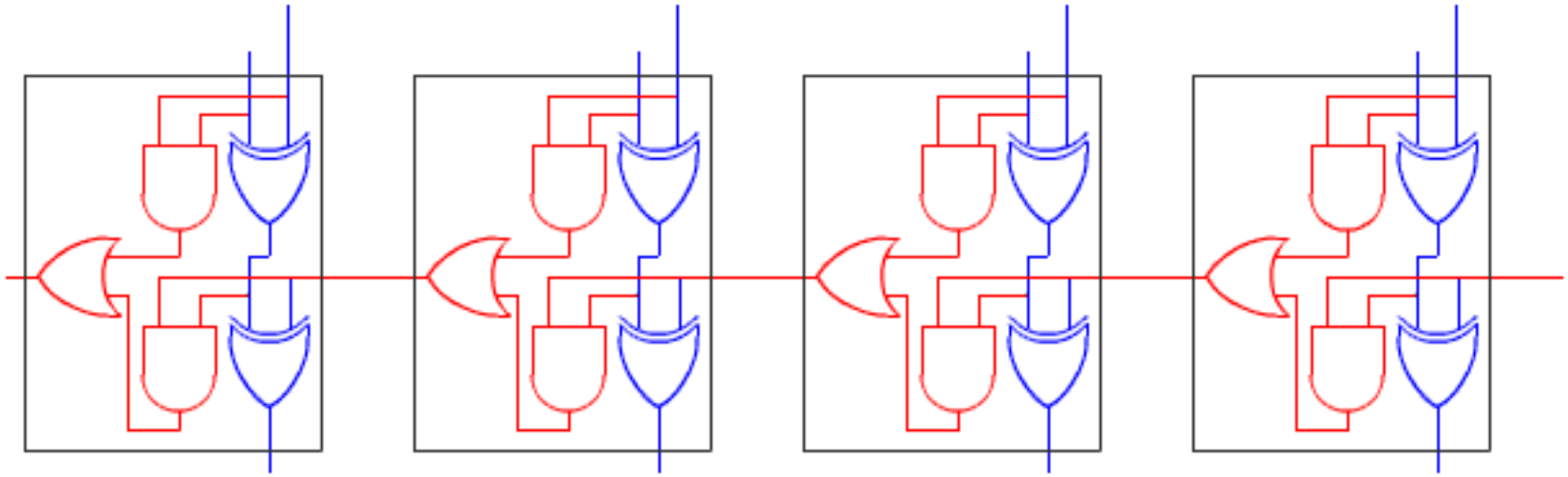
Appendix 3 : Full-adder circuit

- Cascading of 4 adders for the addition of two 4-bit numbers.



Appendix 3 : Full-adder circuit

- Cascading of 4 adders for the addition of two 4-bit numbers.



- Exercise: Check the correct implementation of the 4-bit addition given as an example above.

Appendix 4 : Quantum non-cloning theorem

- This theorem addresses the following question: Is it possible to duplicate (copy / clone) the quantum state of a system?

Appendix 4 : Quantum non-cloning theorem

- This theorem addresses the following question: Is it possible to duplicate (copy / clone) the quantum state of a system?
- To answer this question, we suppose the system A in the state $|\chi_A\rangle$ and we want to copy this state in a system B, previously in a state $|\phi_B\rangle$.

Appendix 4 : Quantum non-cloning theorem

- This theorem addresses the following question: Is it possible to duplicate (copy / clone) the quantum state of a system?
- To answer this question, we suppose the system A in the state $|\chi_A\rangle$ and we want to copy this state in a system B, previously in a state $|\phi_B\rangle$.
- For this, we consider the system AB including the two parts A and B. If the cloning operation is possible, then there exists a unit transformation (quantum gate) which transforms the state $|\chi_A \otimes \phi_B\rangle$ into the state $|\chi_A \otimes \chi_B\rangle$.

$$U : |\chi_A \otimes \phi_B\rangle \longrightarrow |\chi_A \otimes \chi_B\rangle$$

Appendix 4 : Quantum non-cloning theorem

- This theorem addresses the following question: Is it possible to duplicate (copy / clone) the quantum state of a system?
- To answer this question, we suppose the system A in the state $|\chi_A\rangle$ and we want to copy this state in a system B, previously in a state $|\phi_B\rangle$.
- For this, we consider the system AB including the two parts A and B. If the cloning operation is possible, then there exists a unit transformation (quantum gate) which transforms the state $|\chi_A \otimes \phi_B\rangle$ into the state $|\chi_A \otimes \chi_B\rangle$.

$$U : |\chi_A \otimes \phi_B\rangle \longrightarrow |\chi_A \otimes \chi_B\rangle$$

- If such a gate exists, then it must be able to copy any state from A to B, *i.e.* for 2 states χ_{1A} and χ_{2A} :

$$U|\chi_{1A} \otimes \phi_B\rangle = |\chi_{1A} \otimes \chi_{1B}\rangle$$
$$U|\chi_{2A} \otimes \phi_B\rangle = |\chi_{2A} \otimes \chi_{2B}\rangle$$

Appendix 4 : Quantum non-cloning theorem

- Let us calculate the quantity X scalar product of the left (then right) members of the previous equality:

Appendix 4 : Quantum non-cloning theorem

- Let us calculate the quantity X scalar product of the left (then right) members of the previous equality:
  - On the one hand we have

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \phi_B | U^\dagger U | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} \otimes \phi_B | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \phi_B | \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \end{aligned}$$

  because U is unitary and $\langle \phi_B | \phi_B \rangle = 1$.

Appendix 4 : Quantum non-cloning theorem

- Let us calculate the quantity X scalar product of the left (then right) members of the previous equality:
  - On the one hand we have

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \phi_B | U^\dagger U | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} \otimes \phi_B | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \phi_B | \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \end{aligned}$$

    because U is unitary and $\langle \phi_B | \phi_B \rangle = 1$.
  - On the other hand :

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \chi_{1B} | \chi_{2A} \otimes \chi_{2B} \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \chi_{1B} | \chi_{2B} \rangle \end{aligned}$$

Appendix 4 : Quantum non-cloning theorem

- Let us calculate the quantity X scalar product of the left (then right) members of the previous equality:
  - On the one hand we have

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \phi_B | U^\dagger U | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} \otimes \phi_B | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \phi_B | \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \end{aligned}$$

    because U is unitary and $\langle \phi_B | \phi_B \rangle = 1$.
  - On the other hand :

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \chi_{1B} | \chi_{2A} \otimes \chi_{2B} \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \chi_{1B} | \chi_{2B} \rangle \end{aligned}$$

- Since $\langle \chi_{1A} | \chi_{2A} \rangle = \langle \chi_{1B} | \chi_{2B} \rangle$, on déduit que $X = X^2$. There are therefore 2 cases:

Appendix 4 : Quantum non-cloning theorem

- Let us calculate the quantity X scalar product of the left (then right) members of the previous equality:
  - On the one hand we have

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \phi_B | U^\dagger U | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} \otimes \phi_B | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \phi_B | \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \end{aligned}$$

    because U is unitary and $\langle \phi_B | \phi_B \rangle = 1$.
  - On the other hand :

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \chi_{1B} | \chi_{2A} \otimes \chi_{2B} \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \chi_{1B} | \chi_{2B} \rangle \end{aligned}$$

- Since $\langle \chi_{1A} | \chi_{2A} \rangle = \langle \chi_{1B} | \chi_{2B} \rangle$, on déduit que $X = X^2$. There are therefore 2 cases:
  - $X = 1 \Rightarrow |\chi_1\rangle = |\chi_2\rangle$.

Appendix 4 : Quantum non-cloning theorem

- Let us calculate the quantity X scalar product of the left (then right) members of the previous equality:
  - On the one hand we have

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \phi_B | U^\dagger U | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} \otimes \phi_B | \chi_{2A} \otimes \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \phi_B | \phi_B \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \end{aligned}$$

    because U is unitary and $\langle \phi_B | \phi_B \rangle = 1$.
  - On the other hand :

$$\begin{aligned} X &= \langle \chi_{1A} \otimes \chi_{1B} | \chi_{2A} \otimes \chi_{2B} \rangle \\ &= \langle \chi_{1A} | \chi_{2A} \rangle \langle \chi_{1B} | \chi_{2B} \rangle \end{aligned}$$

- Since $\langle \chi_{1A} | \chi_{2A} \rangle = \langle \chi_{1B} | \chi_{2B} \rangle$, on déduit que $X = X^2$. There are therefore 2 cases:
  - $X = 1 \Rightarrow |\chi_1\rangle = |\chi_2\rangle$.
  - $X = 0 \Rightarrow |\chi_1\rangle \perp |\chi_2\rangle$.