Introducción a la Computación Cuántica y Fundamentos de Lenguajes de Programación

Primer encuentro

Alejandro Díaz-Caro

LCC – FCEIA – UNR – 18 y 19 de octubre de 2016

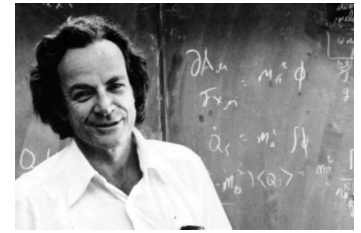
Un poco de historia

Richard Feynman

First Conference on the Physics of Computation, MIT, 1981

Simulación

- Física clásica $\Longrightarrow$ computación clásica
- Física cuántica $\Longrightarrow$ ¿computación clásica?



Necesidad de una computadora cuántica para simular física cuántica

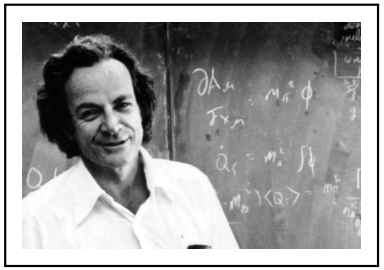
Un poco de historia

Richard Feynman

First Conference on the Physics of Computation, MIT, 1981

Simulación

- Física clásica $\Longrightarrow$ computación clásica
- Física cuántica $\Longrightarrow$ ¿computación clásica?



Necesidad de una computadora cuántica para simular física cuántica

Entre tanto en Rusia...

R. P. Poplavskii

Uspekhi Fizicheskikh Nauk, 115:3, 465–501, 1975

- Inviabilidad computacional de simular sistemas cuánticos (debido al ppio de superposición)

Yuri I. Manin

Moscow, Sovetskoye Radio, 1980

- Uso del número exponencial de estados de base
- Propuesta de teoría de computación cuántica

Un poco de historia (continuación)

Paul Benioff

Journal of Statistical Physics 29 (3):515–546, 1982

- Primer framework teórico para computación cuántica

Charles Bennett y Gilles Brassard

Int. Conference on Computers, Systems and Signal Processing, EE.UU., 1984

- BB84: Método de distribuciónd de claves para criptografía

David Deutsch

Proceedings of the Royal Society A 400 (1818):97–117, 1985

- Máquina de Turing Cuántica: máquina cuántica universal

. . . Varios hitos históricos omitidos . . .

Peter Shor

35th Annual Symposium on Foundations of Computer Science, EE.UU., 1994

- Algoritmo cuántico para factorizar números primos

Lov Grover

28th Annual ACM Symposium on the Theory of Computing, EE.UU., 1996

- Algoritmo de búsqueda (con ganancia cuadrática)

En el pizarrón

- Espacio de Hilbert
- Producto tensorial
- Notación bra-ket

Bits cuánticos

Un qubit es...

(para un físico)

...un sistema cuántico con dos niveles de energía y que puede ser manipulado arbitrariamente

Bits cuánticos

Un qubit es...

(para un físico)

...un sistema cuántico con dos niveles de energía y que puede ser manipulado arbitrariamente

pero nosotros no somos físicos...

(para un matemático o informático)

...un vector normalizado del espacio de Hilbert $\mathbb{C}^2$

Bits cuánticos

Un qubit es...

(para un físico)

...un sistema cuántico con dos niveles de energía y que puede ser manipulado arbitrariamente

pero nosotros no somos físicos...

(para un matemático o informático)

...un vector normalizado del espacio de Hilbert $\mathbb{C}^2$

n-qubits: un vector de $\bigotimes_{i=1}^{n} \mathbb{C}^2 = \mathbb{C}^{2^n}$

Operadores

En el pizarrón

- Operador
- Adjunto y propiedades
- Proyector
- Operador hermítico
- Operador unitario
- Operador de medición
- Compuertas cuánticas
- Evolución

Compuertas más comunes y operadores de Pauli

Hadamard

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

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

Identidad

$$I|0\rangle = |0\rangle$$
$$I|1\rangle = |1\rangle$$

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

Negación

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

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

Cambio de fase

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

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

No-controlada

$$CNOT|0x\rangle = |0x\rangle$$
$$CNOT|1x\rangle = |1\rangle \otimes X|x\rangle$$

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$

Matrices de Pauli

$$I \qquad X$$
$$iXZ \qquad Z$$

Teorema de no-clonado

Teorema (No clonado)

No existe ninguna compuerta cuántica U tal que para algún $|\phi\rangle \in \mathbb{C}^N$ y para todo $|\psi\rangle \in \mathbb{C}^N$ se cumpla

$$U|\psi\phi\rangle = |\psi\psi\rangle$$

Es decir...

No existe una máquina universal de clonado

Teorema de no-clonado

Teorema (No clonado)

No existe ninguna compuerta cuántica U tal que para algún $|\phi\rangle \in \mathbb{C}^N$ y para todo $|\psi\rangle \in \mathbb{C}^N$ se cumpla

$$U|\psi\phi\rangle = |\psi\psi\rangle$$

Es decir...

No existe una máquina universal de clonado

o más simplemente

No se puede copiar un qubit desconocido

Teorema de no-clonado

Teorema (No clonado)

No existe ninguna compuerta cuántica U tal que para algún $|\phi\rangle \in \mathbb{C}^N$ y para todo $|\psi\rangle \in \mathbb{C}^N$ se cumpla

$$U|\psi\phi\rangle = |\psi\psi\rangle$$

Es decir...

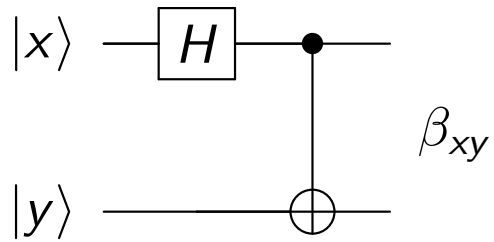
No existe una máquina universal de clonado

o más simplemente

No se puede copiar un qubit desconocido

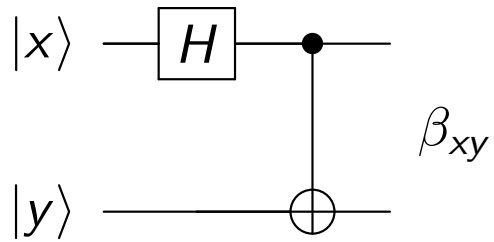
Demostración en el pizarrón

Estados de Bell



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

Estados de Bell



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

Ejemplo:

$$M = \left\{ \begin{array}{lcl} M_0 & = & |0\rangle\langle 0| \\ M_1 & = & |1\rangle\langle 1| \end{array} \right\}$$

Entonces

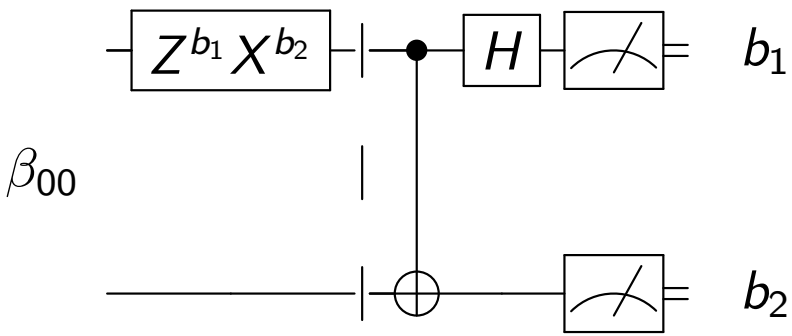
$$(M \otimes I)\beta_{00} \nearrow |00\rangle \quad \searrow |11\rangle$$

Codificación superdensa

Objetivo:
Transmitir 2 bits clásicos enviando tan sólo 1 qubit

Codificación superdensa

Objetivo:
Transmitir 2 bits clásicos enviando tan sólo 1 qubit



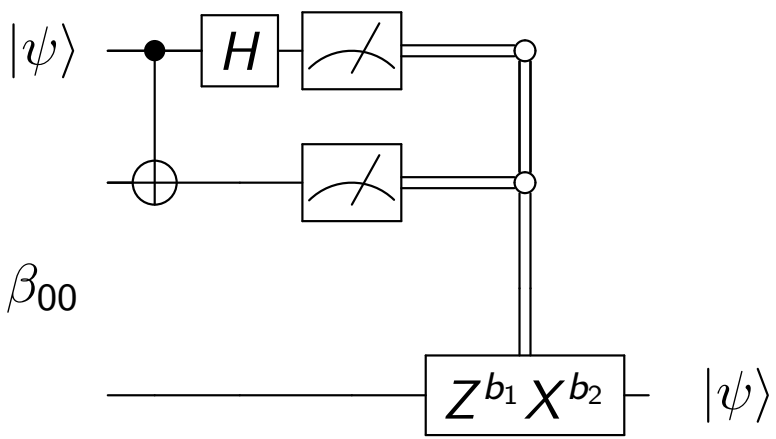
1. A y B preparan β_{00}
2. Se llevan cada uno un qubit
3. A aplica $Z^{b_1}X^{b_2}$ a su qubit
4. A envía su qubit a B
5. B aplica *CNOT* y *H* a ambos
6. B mide

Teleportación cuántica

Objetivo:
Transmitir 1 qubit enviando 2 bits clásicos

Teleportación cuántica

Objetivo:
Transmitir 1 qubit enviando 2 bits clásicos



1. A y B preparan β_{00}
2. Se llevan cada uno un qubit
3. A aplica *CNOT* y *H* al qubit a transmitir y el suyo del par
4. A mide y envía el resultado a B
5. B aplica $Z^{b_1}X^{b_2}$ (b_1 y b_2 de A)

Paralelismo cuántico

Primera intuición

$$f : \{0, 1\} \to \{0, 1\}$$

Resultados posibles: 2
Cantidad de evaluaciones para obtenerlos: 2

Paralelismo cuántico

Primera intuición

$$f : \{0,1\} \to \{0,1\}$$

Resultados posibles: 2
Cantidad de evaluaciones para obtenerlos: 2

Supongamos que existe la siguiente compuerta:

$$U_f|x,0\rangle = |x,f(x)\rangle$$

Paralelismo cuántico

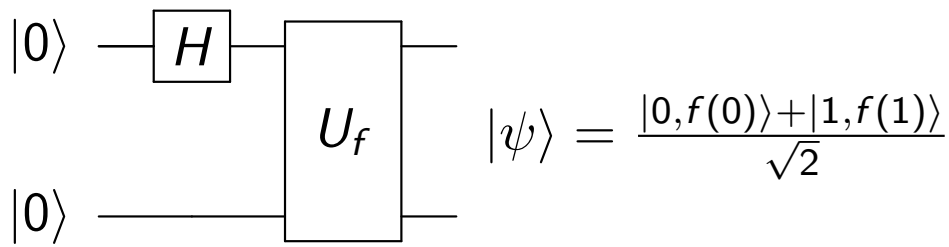
Primera intuición

$$f : \{0,1\} \to \{0,1\}$$

Resultados posibles: 2
Cantidad de evaluaciones para obtenerlos: 2

Supongamos que existe la siguiente compuerta:

$$U_f|x,0\rangle = |x, f(x)\rangle$$



Es decir:

$$|00\rangle \xrightarrow{H(1)} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}}(|0,f(0)\rangle+|1,f(1)\rangle)$$

Cantidad de evaluaciones de U_f para obtener los dos resultados: 1

Algoritmo de Deutsch

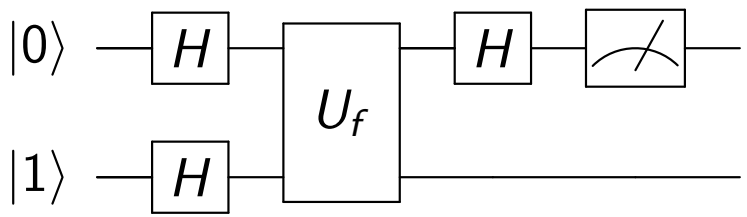
Objetivo:
Dado un "oráculo" U_f que implementa la función
$f : \{0,1\} \to \{0,1\}$, **determinar si f es constante o no**

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$

Algoritmo de Deutsch

Objetivo:
Dado un "oráculo" U_f que implementa la función
$f : \{0,1\} \to \{0,1\}$, **determinar si f es constante o no**

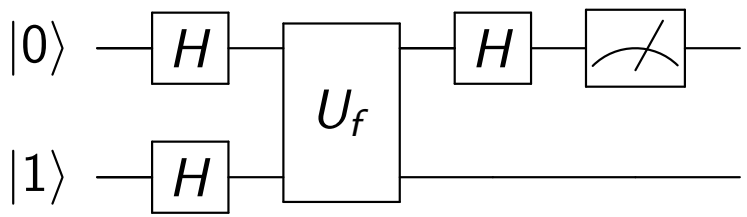
$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$



Algoritmo de Deutsch

Objetivo:
Dado un "oráculo" U_f que implementa la función
$f : \{0,1\} \to \{0,1\}$, **determinar si f es constante o no**

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$

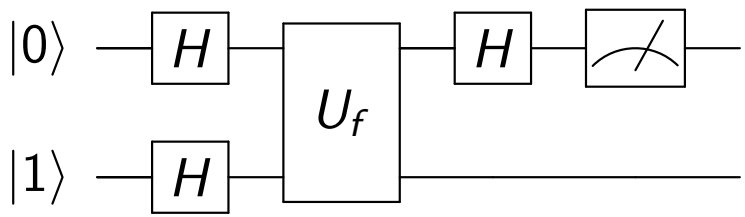


$$|01\rangle \xrightarrow{\text{Deustch alg.}} \cdots \to$$

Algoritmo de Deutsch

Objetivo:
Dado un "oráculo" U_f que implementa la función
$f : \{0,1\} \to \{0,1\}$, **determinar si f es constante o no**

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$



$$|01\rangle \xrightarrow{\text{Deustch alg.}} \pm\,|f(0)\oplus f(1)\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \begin{cases} \xrightarrow{\text{Si es constante}} \pm|0\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \\ \xrightarrow{\text{Sino}} \pm|1\rangle \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \end{cases}$$

Algoritmo de Deutsch-Jotza

Objetivo:

Dado un "oráculo" U_f que implementa la función

$f : \{0,1\}^n \to \{0,1\}$, **determinar si f es constante o balanceada**

$$U_f|\overline{x}, y\rangle = |\overline{x}, y \oplus f(\overline{x})\rangle$$

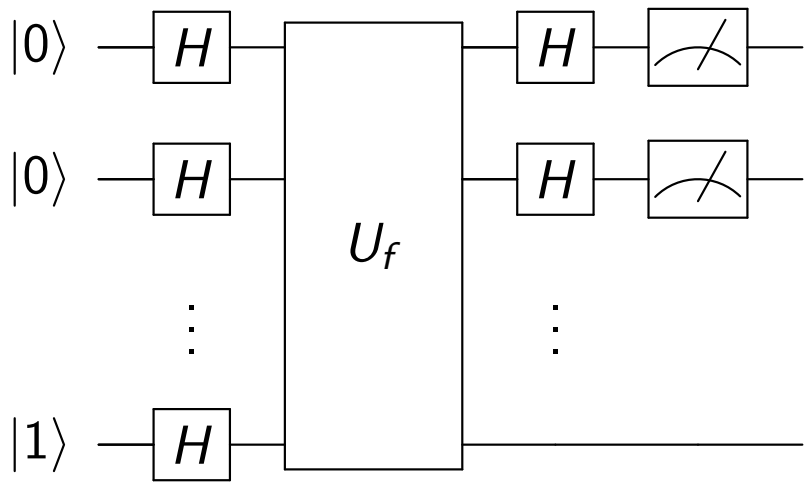
Algoritmo de Deutsch-Jotza

Objetivo:

Dado un "oráculo" U_f que implementa la función

$f : \{0,1\}^n \to \{0,1\}$, **determinar si f es constante o balanceada**

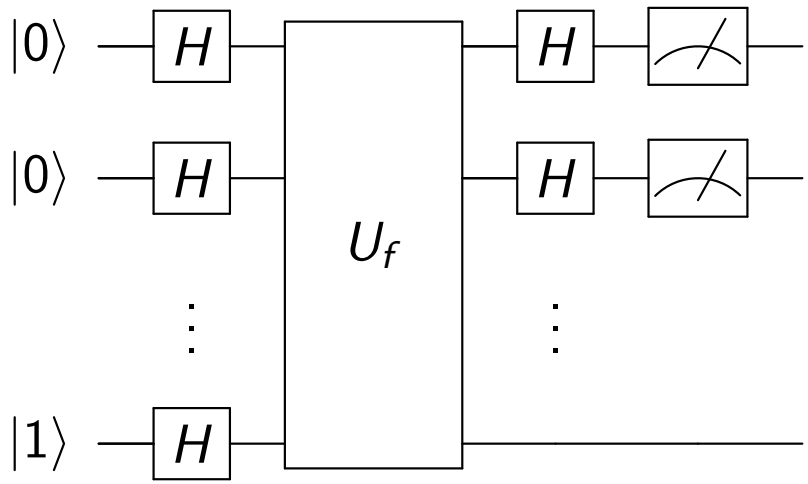
$$U_f|\overline{x}, y\rangle = |\overline{x}, y \oplus f(\overline{x})\rangle$$



Algoritmo de Deutsch-Jotza

Objetivo:
Dado un "oráculo" U_f que implementa la función
$f : \{0,1\}^n \to \{0,1\}$, **determinar si f es constante o balanceada**

$$U_f|\overline{x}, y\rangle = |\overline{x}, y \oplus f(\overline{x})\rangle$$

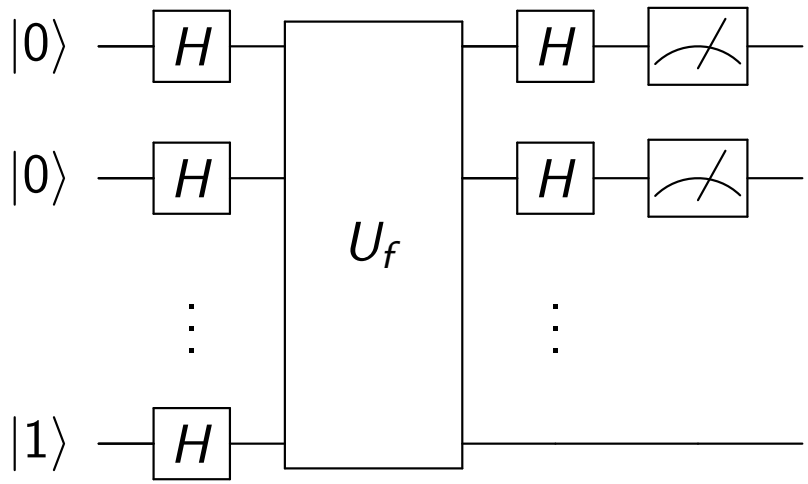


$$|0\rangle^{\otimes n}|1\rangle \xrightarrow{\text{D–J alg.}} \cdots \to$$

Algoritmo de Deutsch-Jotza

Objetivo:
Dado un "oráculo" U_f que implementa la función
$f : \{0,1\}^n \to \{0,1\}$, **determinar si f es constante o balanceada**

$$U_f|\overline{x}, y\rangle = |\overline{x}, y \oplus f(\overline{x})\rangle$$



$$|0\rangle^{\otimes n}|1\rangle \xrightarrow{\text{D–J alg.}} \cdots \rightarrow \begin{cases} \xrightarrow{\text{Si es constante}} \pm|0\rangle^{\otimes n}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \\ \xrightarrow{\text{Si es balanceada}} \pm|\psi\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \end{cases}$$

donde $|\psi\rangle$ no incluye $|0\rangle^{\otimes n}$

Algoritmo de búsqueda de Grover

Preliminares: Oráculo

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$

Tomar $y = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ entonces

$$\begin{aligned} U_f|x,y\rangle &= U_f\left(|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}\left(U_f|x,0\rangle - U_f|x,1\rangle\right) \\ &= \frac{1}{\sqrt{2}}(|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle) = |x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= (-1)^{f(x)}|x,y\rangle \end{aligned}$$

Algoritmo de búsqueda de Grover

Preliminares: Oráculo

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$

Tomar $y = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ entonces

$$\begin{aligned} U_f|x,y\rangle &= U_f\left(|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}\left(U_f|x,0\rangle - U_f|x,1\rangle\right) \\ &= \frac{1}{\sqrt{2}}(|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle) = |x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= (-1)^{f(x)}|x,y\rangle \end{aligned}$$

U_f no modifica y... lo omitimos

Oráculo

$$U|x\rangle = (-1)^{f(x)}|x\rangle$$

Algoritmo de búsqueda de Grover

Preliminares: Inversión sobre el promedio

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\overline{x} \in \{0,1\}^n} |\overline{x}\rangle$$

Algoritmo de búsqueda de Grover

Preliminares: Inversión sobre el promedio

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\overline{x} \in \{0,1\}^n} |\overline{x}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2^n}} \\ \vdots \\ \frac{1}{\sqrt{2^n}} \end{pmatrix}_{2^n}$$

Algoritmo de búsqueda de Grover

Preliminares: Inversión sobre el promedio

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\overline{x}\in\{0,1\}^n} |\overline{x}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2^n}} \\ \vdots \\ \frac{1}{\sqrt{2^n}} \end{pmatrix}_{2^n}$$

Inversión sobre el promedio

$$G = 2|\phi\rangle\langle\phi| - I$$

$$\begin{pmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{pmatrix}_{2^n \times 2^n}$$

Algoritmo de búsqueda de Grover

Preliminares: Inversión sobre el promedio

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\overline{x}\in\{0,1\}^n} |\overline{x}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2^n}} \\ \vdots \\ \frac{1}{\sqrt{2^n}} \end{pmatrix}_{2^n}$$

Inversión sobre el promedio

$$G = 2|\phi\rangle\langle\phi| - I$$

$$\begin{pmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{pmatrix}_{2^n \times 2^n}$$

$$G\left(\sum_{\overline{x}\in\{0,1\}^n} a_{\overline{x}}|\overline{x}\rangle\right) = \sum_{\overline{x}\in\{0,1\}^n} (2A - a_{\overline{x}})|\overline{x}\rangle$$

donde A es el promedio de los $a_{\overline{x}}$

Algoritmo de búsqueda de Grover

El algoritmo

Objetivo:
Localizar el $\overline{x}_0$ tal que $f(\overline{x}_0) = 1$

1. Aplicar Hadamard a $|0\rangle^{\otimes n}$
2. Aplicar el oráculo U
3. Aplicar la inversión sobre el promedio G
4. Repetir pasos 2 y 3 durante $\left\lfloor \frac{\pi}{4\text{arcsen}(\sqrt{\frac{1}{2^n}})} \right\rfloor$ iteraciones

   (cálculo del número óptimo de iteraciones, en el apunte, sección 2.3.4)

Explicación paso a paso en el pizarrón (y ejemplo)

Aplicación criptográfica

One-time pad, un método clásico infalible...

b_1	b_2	$b_1 \oplus b_2$
1	1	0
1	0	1
0	1	1
0	0	0

Aplicación criptográfica

One-time pad, un método clásico infalible...

b_1	b_2	$b_1 \oplus b_2$
1	1	0
1	0	1
0	1	1
0	0	0

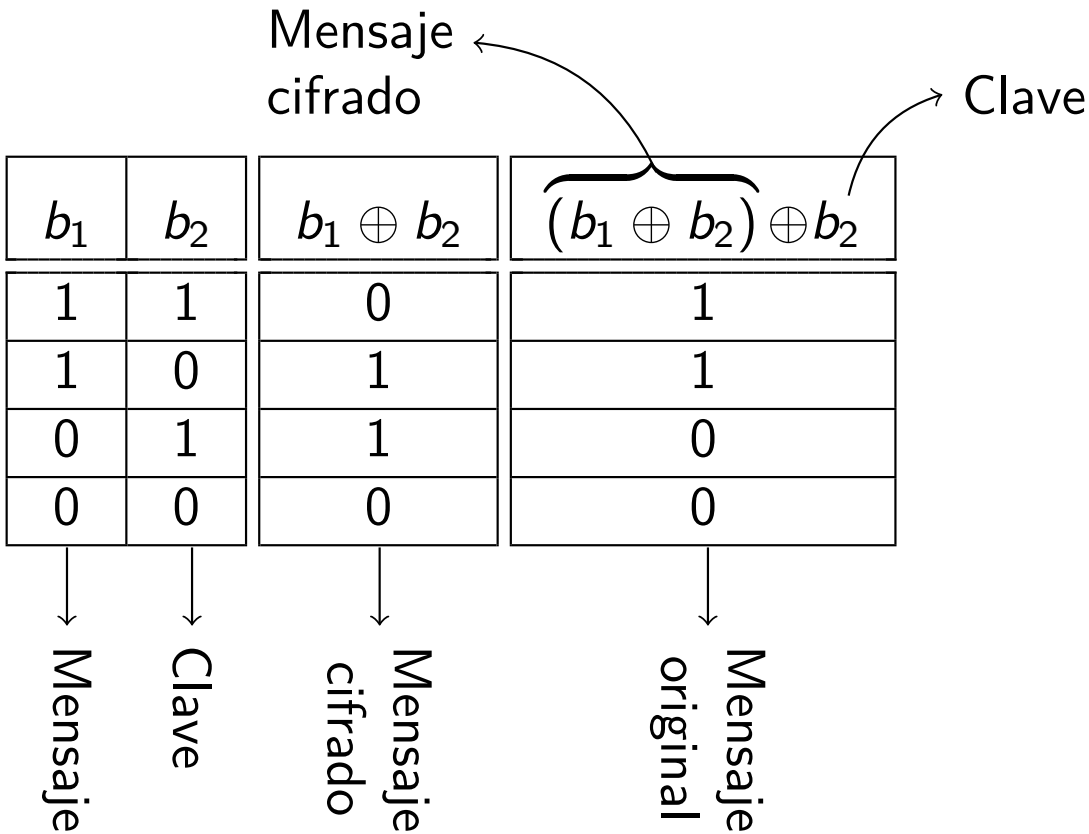
↓ Mensaje

↓ Clave

↓ Mensaje cifrado

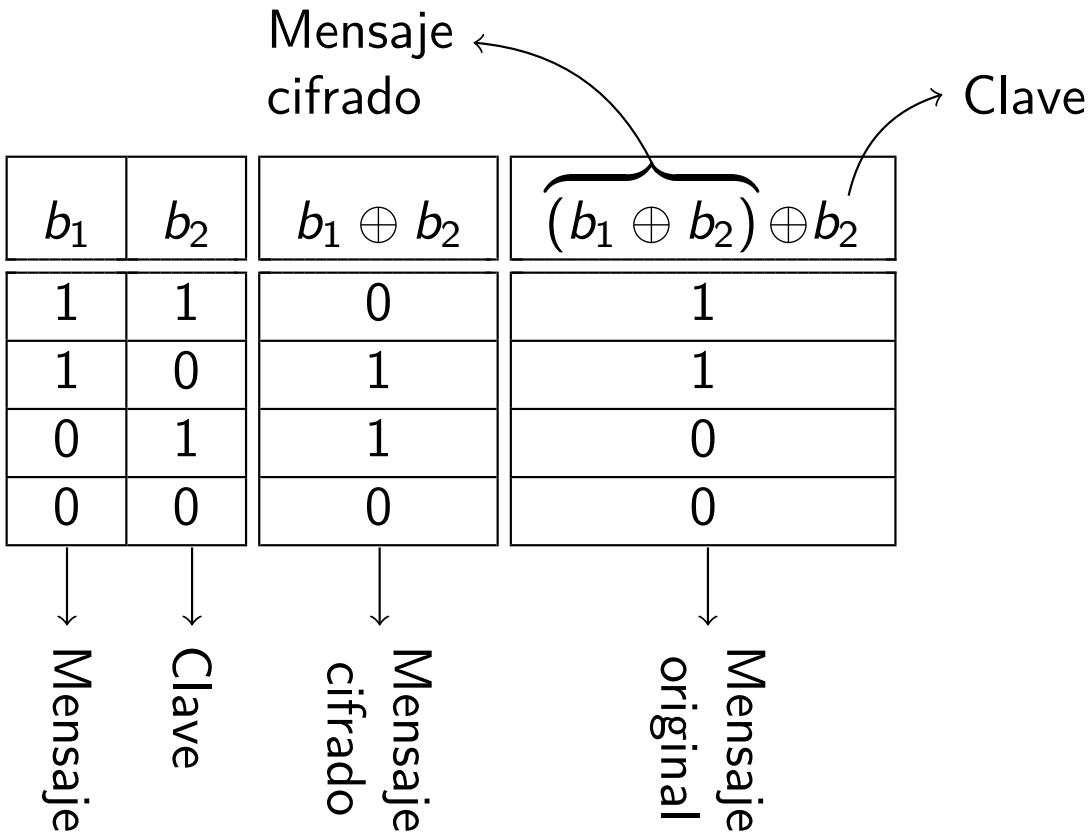
Aplicación criptográfica

One-time pad, un método clásico infalible...



Aplicación criptográfica

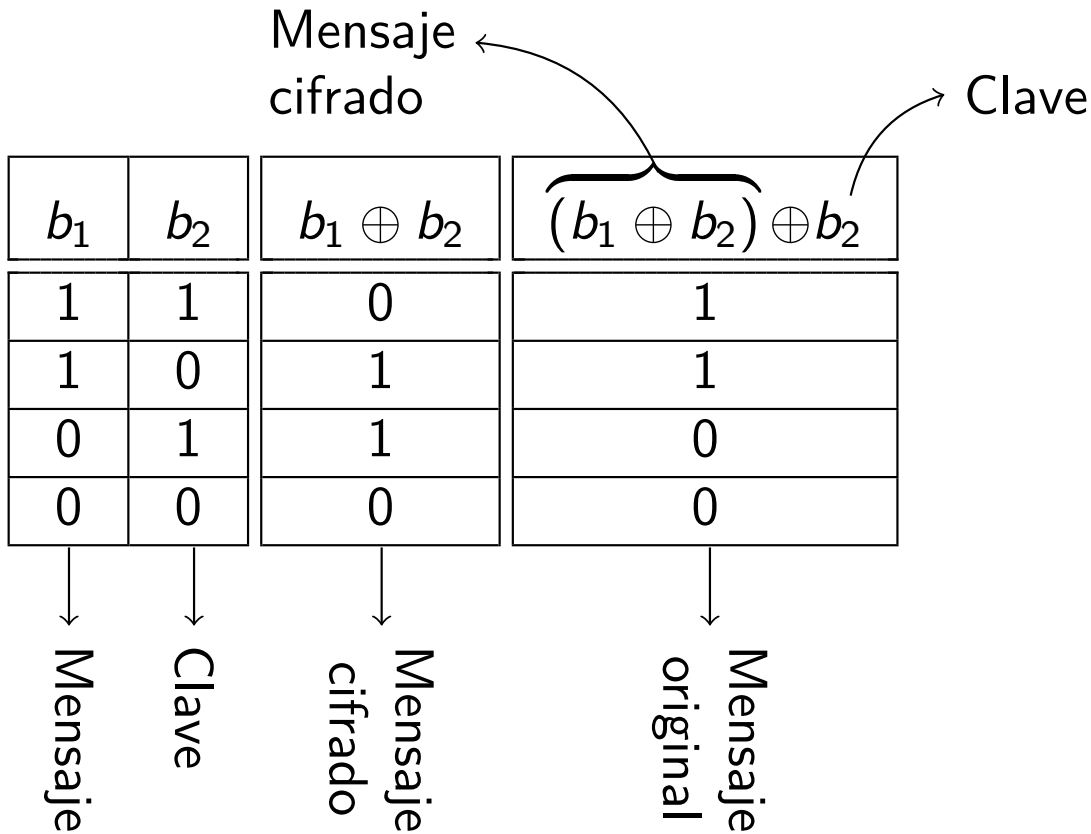
One-time pad, un método clásico infalible...



Probabilidad de adivinar el mensaje original a partir del cifrado: $\frac{1}{2^n}$

Aplicación criptográfica

One-time pad, un método clásico infalible...



Probabilidad de adivinar el mensaje original a partir del cifrado: $\frac{1}{2^n}$

¡Igual que la posibilidad de adivinar el mensaje original sin ninguna información extra!

Aplicación criptográfica

One-time pad, un método clásico infalible...

Entonces, si es tan simple y seguro... ¿porqué no es utilizado?

Aplicación criptográfica

One-time pad, un método clásico infalible...

Entonces, si es tan simple y seguro... ¿porqué no es utilizado?

- Largo del mensaje = largo de la clave (para 100 % de seguridad)
- Clave de encriptación y desencriptación iguales (y secretas)
  - Dificultad para distribuir las claves

Aplicación criptográfica

One-time pad, un método clásico infalible...

Entonces, si es tan simple y seguro... ¿porqué no es utilizado?

- Largo del mensaje = largo de la clave (para 100 % de seguridad)
- Clave de encriptación y desencriptación iguales (y secretas)
  - Dificultad para distribuir las claves

Ahí entra el método BB84: es un método de *distribución* de claves de manera segura.

Aplicación criptográfica

QKD–BB84

Objetivo: Crear y transmitir una clave de manera segura

Esquema	$+$	$\times$
Base	$\{\|0\rangle, \|1\rangle\}$	$\{\|+\rangle, \|-\rangle\}$
Codif.	$0 = \|0\rangle$ $1 = \|1\rangle$	$0 = \|-\rangle$ $1 = \|+\rangle$

1. A: secuencia aleatoria de 0s o 1s y elección aleatoria de esquemas para c/bit
2. B: elección aleatoria del esquema de medición para cada bit recibido
3. A: transmite la sucesión de esquemas empleada
4. B: informa en qué casos coincidieron
5. La clave queda definida por los bits donde se usaron los mismos esquemas
6. Intercambio de hashes para verificación

Aplicación criptográfica

QKD–BB84: Ejemplo

$$+: \quad 0 = |0\rangle, \quad 1 = |1\rangle \qquad\qquad \times: \quad 0 = |-\rangle, \quad 1 = |+\rangle$$

1. A: secuencia aleatoria de 0s o 1s y elección aleatoria de esquemas para c/bit
2. B: elección aleatoria del esquema de medición para cada bit recibido
3. A: transmite la sucesión de esquemas empleada
4. B: informa en qué casos coincidieron
5. La clave queda definida por los bits donde se usaron los mismos esquemas
6. Intercambio de hashes para verificación

Bits de A	1	0	0	1	0	0	0	1
Esquemas de A	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$
Valores de A	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$
Esquemas de B	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$
Valores de B	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$

Aplicación criptográfica

QKD–BB84: Ejemplo

$$+: \quad 0 = |0\rangle, \quad 1 = |1\rangle \qquad\qquad \times: \quad 0 = |-\rangle, \quad 1 = |+\rangle$$

1. A: secuencia aleatoria de 0s o 1s y elección aleatoria de esquemas para c/bit
2. B: elección aleatoria del esquema de medición para cada bit recibido
3. A: transmite la sucesión de esquemas empleada
4. B: informa en qué casos coincidieron
5. La clave queda definida por los bits donde se usaron los mismos esquemas
6. Intercambio de hashes para verificación

Bits de A	1	0	0	1	0	0	0	1
Esquemas de A	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$
Valores de A	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$
Esquemas de B	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$
Valores de B	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
Coincidencias			$\surd$	$\surd$		$\surd$	$\surd$	

Aplicación criptográfica

QKD–BB84: Ejemplo

$$+: \quad 0 = |0\rangle, \quad 1 = |1\rangle \qquad\qquad \times: \quad 0 = |-\rangle, \quad 1 = |+\rangle$$

1. A: secuencia aleatoria de 0s o 1s y elección aleatoria de esquemas para c/bit
2. B: elección aleatoria del esquema de medición para cada bit recibido
3. A: transmite la sucesión de esquemas empleada
4. B: informa en qué casos coincidieron
5. La clave queda definida por los bits donde se usaron los mismos esquemas
6. Intercambio de hashes para verificación

Bits de A	1	0	0	1	0	0	0	1
Esquemas de A	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$
Valores de A	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$
Esquemas de B	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$
Valores de B	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
Coincidencias			$\surd$	$\surd$		$\surd$	$\surd$	
Clave			0	1		0	0	

Aplicación criptográfica

QKD–BB84: Inviolabilidad (teórica)

Agregamos un espía: C

Aplicación criptográfica

QKD–BB84: Inviolabilidad (teórica)

Agregamos un espía: C

- A envía 0 con esquema $\times$: $|-\rangle$

Aplicación criptográfica

QKD–BB84: Inviolabilidad (teórica)

Agregamos un espía: C

- A envía 0 con esquema $\times$: $|-\rangle$
- Si C usa esquema $+$, el estado pasa a $|0\rangle$ o $|1\rangle$

Aplicación criptográfica

QKD–BB84: Inviolabilidad (teórica)

Agregamos un espía: C

- A envía 0 con esquema $\times$: $|-\rangle$
- Si C usa esquema $+$, el estado pasa a $|0\rangle$ o $|1\rangle$
- Si B usa esquema $\times$, obtiene $|-\rangle$ con probabilidad $\frac{1}{2}$ y $|+\rangle$ con probabilidad $\frac{1}{2}$

Aplicación criptográfica

QKD–BB84: Inviolabilidad (teórica)

Agregamos un espía: C

- A envía 0 con esquema $\times$: $|-\rangle$
- Si C usa esquema $+$, el estado pasa a $|0\rangle$ o $|1\rangle$
- Si B usa esquema $\times$, obtiene $|-\rangle$ con probabilidad $\frac{1}{2}$ y $|+\rangle$ con probabilidad $\frac{1}{2}$
- Mientras más bits se envían, la probabilidad de no detectar a C decrece exponencialmente:

Bits	Probabilidad
1 bit	$3/4 = 0{,}75$
8 bits	$(3/4)^8 = 0{,}10011$
128 bits	$(3/4)^{128} = 1{,}018 \times 10^{-16}$
1Mb	$(3/4)^{1024} = 1{,}155 \times 10^{-128}$
1MB	$(3/4)^{8192} = 3{,}17 \times 10^{-1024}$

Aplicación criptográfica

QKD–BB84 en la vida real