



1. Supón que Alice quiere mandar el estado $|\varphi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ a Bob. Realiza el protocolo de tele portación documentando paso por paso como se va modificando el estado. (Asume que cuando Alice mide sus qubits obtiene 01).

Consideremos 3 qubits: q_0 (estado desconocido de Alice), q_1 (mitad de Alice del par EPR) y q_2 (mitad de Bob del par EPR).

Donde el estado a enviar es $|\varphi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$ y el estado inicial del par compartido (EPR) es: $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ en (q_1, q_2) .

El total es: $|\Psi_0\rangle = |\varphi\rangle_{q_0} \otimes |\beta_{00}\rangle_{q_1 q_2} = \frac{1}{2}(|0\rangle+|1\rangle) \otimes (|00\rangle+|11\rangle) = \frac{1}{2}(|000\rangle+|011\rangle+|100\rangle+|111\rangle)$

Se aplica CNOT con control q_0 y blanco q_1 :

$$|\Psi_1\rangle = (CNOT(q_0, q_1) \otimes I) \frac{1}{2}(|000\rangle+|011\rangle+|100\rangle+|111\rangle) = \frac{1}{2}(|000\rangle+|011\rangle+|110\rangle+|101\rangle)$$

Aplicamos Hadamard H en q_0 , recordando que $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ y $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$:

$$\begin{aligned} |\Psi_2\rangle &= (H \otimes I \otimes I) \frac{1}{2}(|000\rangle+|011\rangle+|110\rangle+|101\rangle) \\ &= \frac{1}{2} \left[\frac{|000\rangle+|100\rangle}{\sqrt{2}} + \frac{|011\rangle+|111\rangle}{\sqrt{2}} + \frac{|011\rangle-|110\rangle}{\sqrt{2}} + \frac{|101\rangle-|101\rangle}{\sqrt{2}} \right] \\ &= \frac{1}{2\sqrt{2}} [|000\rangle+|100\rangle+|011\rangle+|111\rangle+|010\rangle-|110\rangle+|001\rangle-|101\rangle] \\ &= \frac{1}{2\sqrt{2}} [(|000\rangle+|001\rangle)+(|011\rangle+|010\rangle)+(|100\rangle-|101\rangle)+(-|110\rangle+|111\rangle)] \\ &= \frac{1}{2\sqrt{2}} [|00\rangle(|0\rangle+|1\rangle)+|01\rangle(|1\rangle+|0\rangle)+|10\rangle(|0\rangle-|1\rangle)+|11\rangle(-|0\rangle+|1\rangle)] \\ &= \frac{1}{2} [|00\rangle|+\rangle+|01\rangle|+\rangle+|10\rangle|-\rangle+|11\rangle|-\rangle] \end{aligned}$$

Por tanto, la forma canónica (en términos de Pauli sobre $|+\rangle$) es: $|\Psi_2\rangle = \frac{1}{2} [|00\rangle I |+\rangle + |01\rangle X |+\rangle + |10\rangle Z |+\rangle + |11\rangle XZ |+\rangle]$

Ya que: $I|+\rangle = |+\rangle$, $X|+\rangle = |+\rangle$, $Z|+\rangle = |-\rangle$, $XZ|+\rangle = X|-\rangle = -|-\rangle$.

Alice mide sus dos qubits $(q_0, q_1) \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, el estado colapsado es:

$$|\Psi_m\rangle = \frac{|m\rangle \otimes (O_m |\varphi\rangle)}{\sqrt{p_m}}, \quad p_m = \text{amplitud asociada a } m \|^2, \quad m \in \{00, 01, 10, 11\}, \quad O_m \in \{I, X, Z, XZ\}$$

El problema indica quedarnos la rama de Alice obtuvo 01.

$$|\Psi_{01}\rangle = \frac{P_{01} |\Psi_2\rangle}{\sqrt{p_{01}}} = \frac{1}{2} \frac{|01\rangle \otimes (X|+\rangle)}{\sqrt{1/4}} = \frac{1}{2} \frac{|01\rangle \otimes X|+\rangle}{1/2} = |01\rangle \otimes X|\varphi\rangle = \frac{|010\rangle+|011\rangle}{\sqrt{2}}$$

Una vez que Alice colapso sus 2 qubits y el estado total colapso a lo anterior, significa que estos 2 qubits quedan fijos, sin embargo, el qubit de Bob queda en $X|\varphi\rangle$, lo cual es igual a $|\varphi\rangle$, por lo que Bob ya tiene el estado que se deseaba enviar. En el protocolo se establece que si Alice mide $m_1 m_2$, Bob debe aplicar la corrección $X^{m_2} Z^{m_1}$, esto nos lleva a que Bob debe aplicar X a su qubit:

$$X(X|\varphi\rangle) = |\varphi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}.$$

2. (Obligatorio) Supón que Alice quiere mandar el estado base $|\varphi\rangle = |01\rangle$ a Bob. Realiza el protocolo de codificación superdensa documentando paso por paso como se va modificando el estado.

Partamos de $|00\rangle_{AB}$, apliquemos Hadamard a A:

$$(H \otimes I)|00\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

Ahora apliquemos CNOT con control A y objetivo B:

$$CNOT \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Ya tenemos preparado el entrelazamiento, ahora hay que codificar el mensaje 01, apliquemos X en A:

$$(X \otimes I) \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

Hay que recordar que compuerta debemos aplicar a $|00\rangle_{AB}$, dependiendo de que queremos que Bob mida:

$$|00\rangle \rightarrow I \div 00, \quad |01\rangle \rightarrow X \div 00, \quad |10\rangle \rightarrow Z \div 00, \quad |11\rangle \rightarrow ZX \div 00$$

Ahora Alicia envía el qubit A a Bob. Considerando un canal cuántico donde el estado no cambie durante él envió.

Para decodificar el mensaje de Bob, hay que aplicar CNOT con control A y objetivo B, para luego aplicar la Hadamard en A.

$$\begin{aligned} (H \otimes I)CNOT \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\ (H \otimes I) \frac{|11\rangle + |01\rangle}{\sqrt{2}} &= \frac{1}{\sqrt{2}} [H|1\rangle + H|0\rangle \otimes |1\rangle + |1\rangle] = \frac{1}{\sqrt{2}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} + \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle + |1\rangle \right] \\ &= \frac{1}{\sqrt{2}} \left[\frac{|0\rangle - |1\rangle + |0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle + |1\rangle \right] = \frac{1}{\sqrt{2}} \left[\frac{2|0\rangle}{\sqrt{2}} \otimes 2|1\rangle \right] = \frac{2}{2} [|0\rangle \otimes |1\rangle] = |01\rangle \end{aligned}$$

Entonces Bob mide $|q_A q_B\rangle = |01\rangle$ midiendo 01 con probabilidad 1.

3. Escribe las diferencias entre los dos protocolos de envió de datos, incluyendo sus precondiciones.

	Codificación superdensa	Teleportación cuántica
Propósito	Enviar dos bits clásicos por uso.	Transferir el estado cuántico de un qubit.
Dato final en Bob	Dos bits clásicos exactos.	El mismo estado cuántico que tenía Alice.
Recurso previo	Par de Bell compartido.	Par de Bell compartido.
Comunicación enviada	1 qubit físico, 0 bits clásicos.	0 qubits físicos, 2 bits clásicos.
Acciones de Alice	Aplica $(Z^{b_1} X^{b_0})$ a su qubit y lo envía.	Acopla, aplica H, mide 2 qubits y envía 2 bits.
Acciones de Bob	CNOT (A→B) + H; mide para leer los 2 bits.	Correcciones condicionadas $(X^{b_0} Z^{b_1})$; no necesita medir para reconstruir.
Canal clásico	No requerido para el mensaje.	Requerido (2 bits).
Mediciones	Solo Bob, al final.	Solo Alice, para generar los 2 bits.
Uso típico	Maximizar envió de datos clásicos por qubit enviado.	Enviar estados cuánticos a distancia sin enviar el qubit.

4. (Obligatorio) Usando la implementación de funciones, define las compuertas cuánticas correspondientes a la implicación lógica (U_{\rightarrow}) y la función $pot(x) = x^2$ con x un estado de dos bits (U_{pot}).

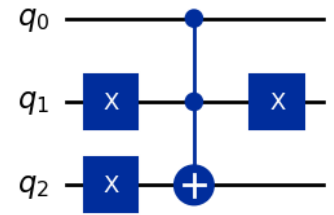
a) U_{\rightarrow}

Definición: $a, b \in \{0,1\} \Rightarrow f_{\rightarrow}(a, b) = (a \Rightarrow b) = \neg a \vee b = (a \wedge \neg b)$

a	b	$(a \wedge \neg b)$
0	0	1
0	1	1
1	0	0
1	1	1

Para la tabla cuántica: $y' = y \oplus f_{\rightarrow}(a, b)$

a	b	y	y'
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0



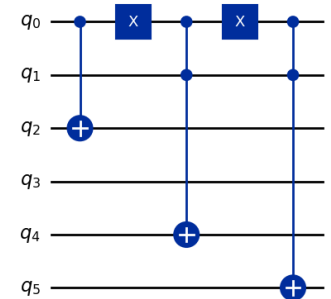
Veamos que podemos usar $U_{\rightarrow}|q_1q_2q_3\rangle = (I \otimes X \otimes I)CCX_{1,2 \rightarrow 3}(I \otimes X \otimes I)(I \otimes I \otimes X)|q_1q_2q_3\rangle$

b) $pot(x) = x^2$

Definición: $x_1, x_0 \in \{0,1\}$, con $x = 2x_1 + x_0$. Definimos: $f_{pot}(x_1, x_2) = x^2$

x_1	x_0	x	x^2	$y_3y_2y_1y_0$
0	0	0	0	0000
0	1	1	1	0001
1	0	2	4	0100
1	1	3	9	1001

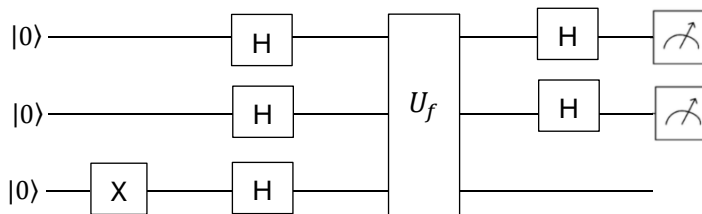
Usamos un registro de 6 qubits: $|q_1q_2q_3q_4q_5q_6\rangle = |x_0, x_1, y_0, y_1, y_2, y_3\rangle$, usando estado inicial $y = 0000$



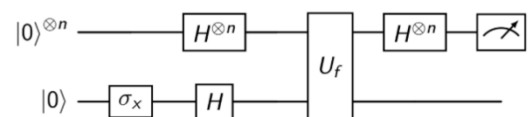
x_1	x_0	Estado	y
0	0	$ 000000\rangle$	0000
0	1	$ 010000\rangle$	0001
1	0	$ 100000\rangle$	0100
1	1	$ 110000\rangle$	1001

Veamos que podemos usar $U_{pot}|q_1q_2q_3q_4q_5q_6\rangle = CCX_{2,1 \rightarrow 6}(X_1CCX_{2,1 \rightarrow 5}X_1)CX_{2,1 \rightarrow 3}|q_1q_2q_3q_4q_5q_6\rangle$

5. Dibuja el circuito del algoritmo de Deutsch-Jozsa para una función $f: \{0,1\}^2 \rightarrow \{0,1\}$.



Es la generalización del algoritmo de Deutsch tomando a $f: \{0,1\}^n \rightarrow \{0,1\}$.



6. (Obligatorio) Aplica el algoritmo de Deutsch-Jozsa para la función f definida como sigue: $f(00) = 0$, $f(01) = 1$, $f(10) = 0$, $f(11) = 1$

Estado inicial: $|\psi_0\rangle = |000\rangle$, aplicando el primer paso: $I \otimes I \otimes X |\psi_0\rangle = |001\rangle$, luego aplicamos las Hadamards: $H^{\otimes 3} |001\rangle = |001\rangle$

Por lo tanto:

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

Ahora se aplica el oráculo U_f ($U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$) y phase kick-back: $U_f(|x\rangle |-\rangle) = |x\rangle (-1)^{f(x)} |-\rangle$.

$$|\psi_1\rangle = \frac{1}{2} \sum_{x_1, x_2 \in \{0,1\}} |x_1 x_2\rangle \otimes |-\rangle \Rightarrow |\psi_2\rangle = U_f |\psi_1\rangle$$

Por linealidad podemos ver cada base $|x_1 x_2\rangle \otimes |-\rangle$:

$$U_f \left(|x_1 x_2\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x_1 x_2\rangle \otimes (-1)^{f(x_1 x_2)} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

a) $x_1 = 0$ y $x_2 = 0$

$$\Rightarrow |00\rangle \otimes (-1)^{f(00)} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |00\rangle \otimes (-1)^0 \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} (|000\rangle - |001\rangle) = |00\rangle \otimes |-\rangle$$

b) $x_1 = 0$ y $x_2 = 1$

$$\Rightarrow |01\rangle \otimes (-1)^{f(01)} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |01\rangle \otimes (-1)^1 \frac{|0\rangle - |1\rangle}{\sqrt{2}} = -\frac{1}{\sqrt{2}} (|010\rangle - |011\rangle) = -|01\rangle \otimes |-\rangle$$

c) $x_1 = 1$ y $x_2 = 0$

$$\Rightarrow |10\rangle \otimes (-1)^{f(10)} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |10\rangle \otimes (-1)^0 \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} (|100\rangle - |101\rangle) = |10\rangle \otimes |-\rangle$$

d) $x_1 = 1$ y $x_2 = 1$

$$\Rightarrow |11\rangle \otimes (-1)^{f(11)} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |11\rangle \otimes (-1)^1 \frac{|0\rangle - |1\rangle}{\sqrt{2}} = -\frac{1}{\sqrt{2}} (|110\rangle - |111\rangle) = -|11\rangle \otimes |-\rangle$$

Por lo tanto:

$$\begin{aligned} |\psi_2\rangle &= U_f |\psi_1\rangle = \frac{1}{2} [(|00\rangle \otimes |-\rangle) + (-|01\rangle \otimes |-\rangle) + (|10\rangle \otimes |-\rangle) + (-|11\rangle \otimes |-\rangle)] \\ &= \frac{1}{2} [(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \otimes |-\rangle] \\ &= \frac{1}{2} [(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)] \otimes |-\rangle \\ &= \frac{1}{2} [2|+\rangle \otimes |-\rangle] \otimes |-\rangle \\ &= |+\rangle \otimes |-\rangle \otimes |-\rangle \end{aligned}$$

Ahora aplicamos los Hadamards finales en x_1 y x_2 :

$$|\psi_3\rangle = (H \otimes H \otimes I) (|+\rangle \otimes |-\rangle \otimes |-\rangle) = H|+\rangle \otimes H|-\rangle \otimes I|-\rangle = |0\rangle \otimes |1\rangle \otimes |-\rangle = |01\rangle \otimes |-\rangle$$

Solo falta realizar la medición del registro de entrada (x_1, x_2) la cual vemos que siempre obtiene $|01\rangle$ con probabilidad 1, los otros 3 estados no son posibles, así que nos queda el qubit ansilla $|-\rangle$. Como el resultado no es 00...0, la función f es balanceada.

7. (Obligatorio) Desglosa la siguiente notación para llegar al estado concreto, asumiendo que $|\bar{x}\rangle = |100\rangle$,

$$|\varphi\rangle = \frac{1}{\sqrt{2^3}} \sum_{\bar{z} \in \{0,1\}^3} (-1)^{\bar{x}\bar{z}} |\bar{z}\rangle$$

$\{0,1\}^3$: significa el conjunto de todas la cadenas binarias de longitud 3, i. e.: $\{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$

Lo que nos lleva a la notación $\bar{z} = z_1 z_2 z_3$ con $z_i = \{0, 1\}$.

Por otro lado, tenemos $\bar{x} = 100$, lo cual en otras palabras es: $x_1 = 1, x_2 = 0, x_3 = 0$.

De modo que el producto punto binario es:

$$\bar{x}\bar{z} = (x_1 z_1 + x_2 z_2 + x_3 z_3) \bmod(2) = (1z_1 + 0z_2 + 0z_3) \bmod(2) = z_1 \bmod(2) = \begin{cases} 0, & \text{si } z_1 = 0 \\ 1, & \text{si } z_1 = 1 \end{cases}$$

Por lo tanto, el signo de $(-1)^{\bar{x}\bar{z}}$ depende solo del primer bit de z : $(-1)^{\bar{x}\bar{z}} = (-1)^{z_1} = \begin{cases} 1, & \text{si } z_1 = 0 \\ -1, & \text{si } z_1 = 1 \end{cases}$

Tenemos 3 casos para cada rama: $\begin{cases} z_1 = 0, \bar{z} = 000, 001, 010, 011 \Rightarrow (-1)^{\bar{x}\bar{z}} = 1 \\ z_1 = 1, \bar{z} = 100, 101, 110, 111 \Rightarrow (-1)^{\bar{x}\bar{z}} = -1 \end{cases}$, por equiprobabilidad nuestro estado es:

$$\begin{aligned} |\varphi\rangle &= \frac{1}{\sqrt{8}} [1|000\rangle + 1|001\rangle + 1|010\rangle + 1|011\rangle - 1|100\rangle - 1|101\rangle - 1|110\rangle - 1|111\rangle] \\ &= \frac{1}{\sqrt{8}} [|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle] \end{aligned}$$

8. El estado al que llegaste en la pregunta anterior ¿a que es equivalente con respecto al estado $|\bar{x}\rangle$.

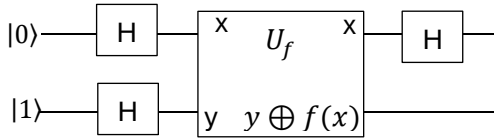
$$\begin{aligned} |\varphi\rangle &= \frac{1}{\sqrt{8}} [|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle] \\ &= \frac{1}{\sqrt{8}} [|0\rangle(|00\rangle + |01\rangle + |10\rangle + |11\rangle) - |1\rangle(|00\rangle + |01\rangle + |10\rangle + |11\rangle)] \\ &= \frac{1}{\sqrt{8}} [|0\rangle \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle) - |1\rangle \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle)] \\ &= \frac{1}{\sqrt{8}} [(|0\rangle - |1\rangle) \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle)] \\ &= \frac{1}{\sqrt{8}} [(|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)] \\ &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= |-\rangle \otimes |+\rangle \otimes |+\rangle \end{aligned}$$

Entonces, $H^{\otimes 3}|\varphi\rangle = H|-\rangle \otimes H|+\rangle \otimes H|+\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle = |100\rangle = |\bar{x}\rangle$.

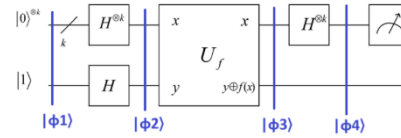
Por lo tanto, tenemos que (por definición):

$$|\varphi\rangle = \frac{1}{\sqrt{2^3}} \sum_{\bar{z} \in \{0,1\}^3} (-1)^{\bar{x}\bar{z}} |\bar{z}\rangle = H^{\otimes 3}|\bar{x}\rangle, \quad \text{equivalentemente,} \quad |\bar{x}\rangle = H^{\otimes 3}|\varphi\rangle$$

9. Dibuja el circuito de Bernstein-Vazirani para la función f de un qubit.



Primero demostraremos el algoritmo con un qubit, así $k=1$.



10. (Obligatorio) Aplica el algoritmo de Bernstein-Vazirani para la función $f(x) = 1 \cdot x$. Escribe paso por paso como se va modificando el estado con respecto al circuito y enfatiza donde se ocupa el phase kick-back.

En B-V el núm. de qubits de entrada es n , igual a la longitud del bit secreto s . El enunciado dice $f(x) = 1 \cdot x$ con x un solo bit, entonces $s = 1$ y $n = 1$, obvio no se considera el qubit ancilla.

Nuestro oráculo U_f , actúa como:

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

El estado inicial es $|\psi_0\rangle = |0\rangle_{q_0}|0\rangle_{q_1}$, por lo que necesitamos $|1\rangle$ en nuestro qubit ancilla q_1 :

$$(I \otimes X)|\psi_0\rangle = |0\rangle|1\rangle = |\psi_1\rangle$$

Aplicamos las compuertas Hadamard:

$$(H \otimes H)|\psi_1\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|-\rangle + |1\rangle|-\rangle) = |\psi_2\rangle$$

Aplicando el oráculo y phase kick-back:

$$|\psi_3\rangle = (U_f \otimes I)|\psi_2\rangle = \frac{1}{\sqrt{2}}(U_f|0\rangle|-\rangle + U_f|1\rangle|-\rangle)$$

Qubit 1:

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

Qubit 2:

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

Por lo tanto:

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle|-\rangle - |1\rangle|-\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |-\rangle = |-\rangle \otimes |-\rangle$$

Aplicamos H al qubit de entrada:

$$(H \otimes I)|\psi_3\rangle = H|-\rangle \otimes |-\rangle = |1\rangle_{\text{entrada}(s)} \otimes |-\rangle_{\text{ancilla}} = \frac{|10\rangle - |11\rangle}{\sqrt{2}} = |\psi_4\rangle$$

Al medir la entrada tenemos una probabilidad de medir 1 de un 100%, así que el secreto $s = 1$.