CS981: Advanced Topics On Cryptography

Name: Mohammed Jawed

StudentID: 23356 00 19

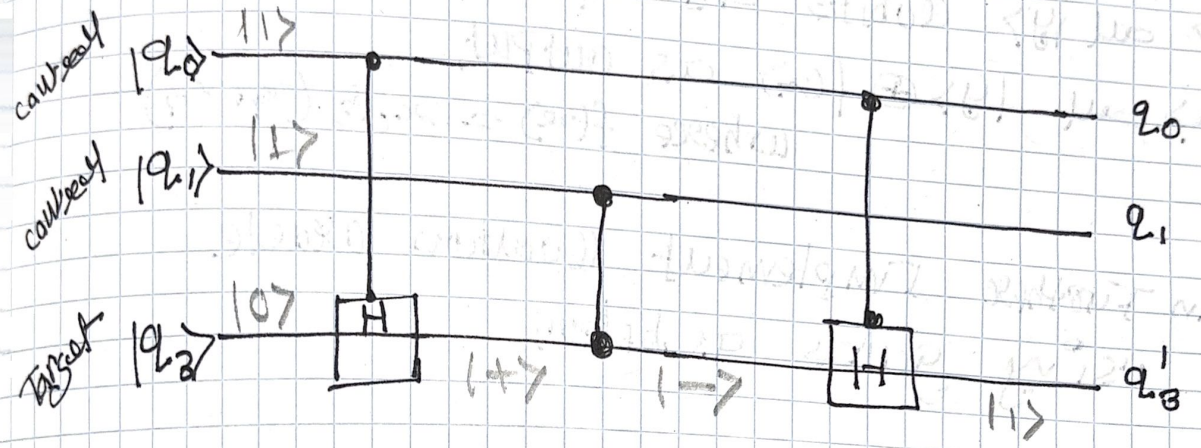
CS981 Assignment I

Mohammed Jawed
Student ID - 23376019

---

(1) controlled controlled Not Gate is also called as "Toffoli Gate".

using Basic quantum Gates:



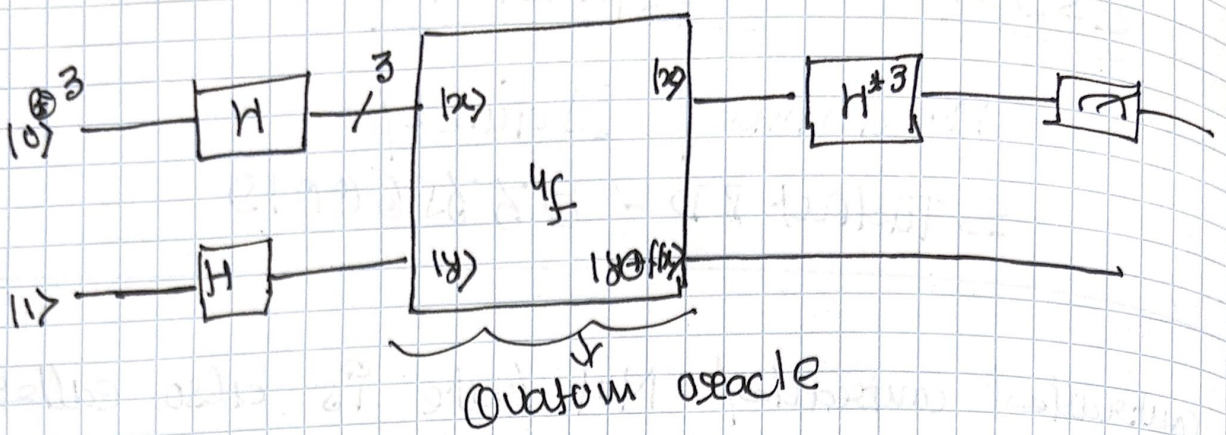
CCNOT gate is type of CNOT gate with two control qubits and one Target qubit ($|q_2\rangle$).

The target qubit ($|q_2\rangle$) will be inverted if the first ($|q_0\rangle$) and second ($|q_1\rangle$) qubits are both 1.

Truth Table

I/P			O/P			
q_0	q_1	q_2	q_0	q_1	q'_2	← target
0	0	0	0	0	0	
0	0	1	0	0	1	
0	1	0	0	1	0	
0	1	1	0	1	1	
1	0	0	1	0	0	
1	0	1	1	0	1	
1	1	0	1	1	1	← target qubit flipped (inverted)
1	1	1	1	1	0	

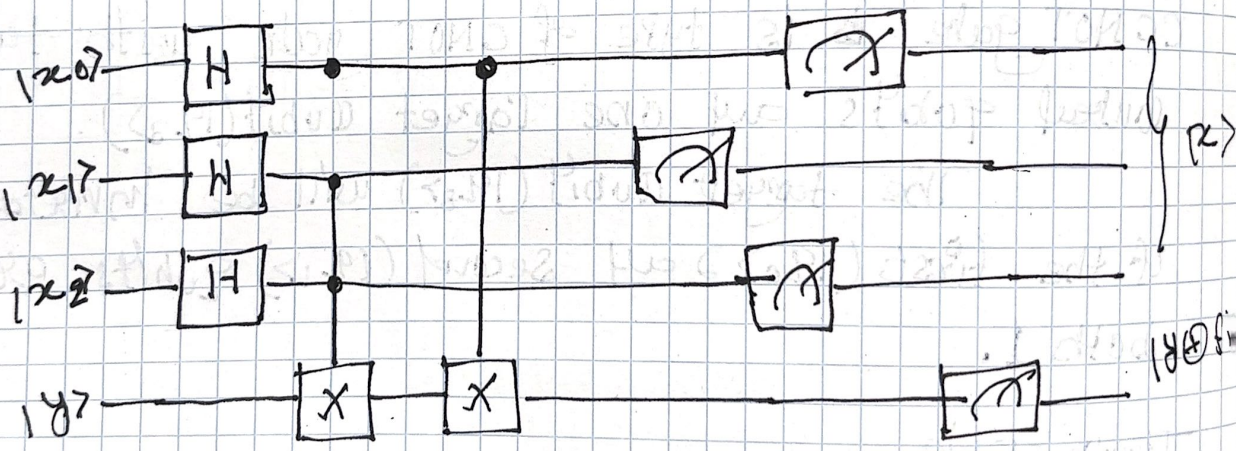
i)



the above black box (Quatum oracle) will takes $|x\rangle$ and $|y\rangle$ qubits as input and produces $|x\rangle$ and $|y\rangle \oplus f(x)$ as output,

where $f(x) = x_0 \oplus (x_1 \cdot x_2)$

we can further implement Quatum oracle using gates as below,



1) x_0, x_1, x_2 are in superposition using Hadamard gates. this will testing all combination in 1 execution
2) the X gate compute $(x_1 \cdot x_2)$ and stores the result in qubit y.
3) A CNOT gate compute $x_0 \oplus (x_1 \cdot x_2)$, finalizing $f(x)$ in qubit y.

iii) To comment whether function $f(x) = x_0 \oplus x_1 \cdot x_2$ is balanced or constant.

- A function $f(x)$ (boolean) is balanced if it returns 0's for exactly half of all inputs and 1's for the other half.
- On other hand if boolean function $f(x)$ is constant function then returns all 0's or all 1's for any Input.

Now, let's Analyze function $f(x) = x_0 \oplus x_1 \cdot x_2$ behaviour to comment,

$$f(x) = x_0 \oplus x_1 \cdot x_2$$

We will use truth table to Analyze it.

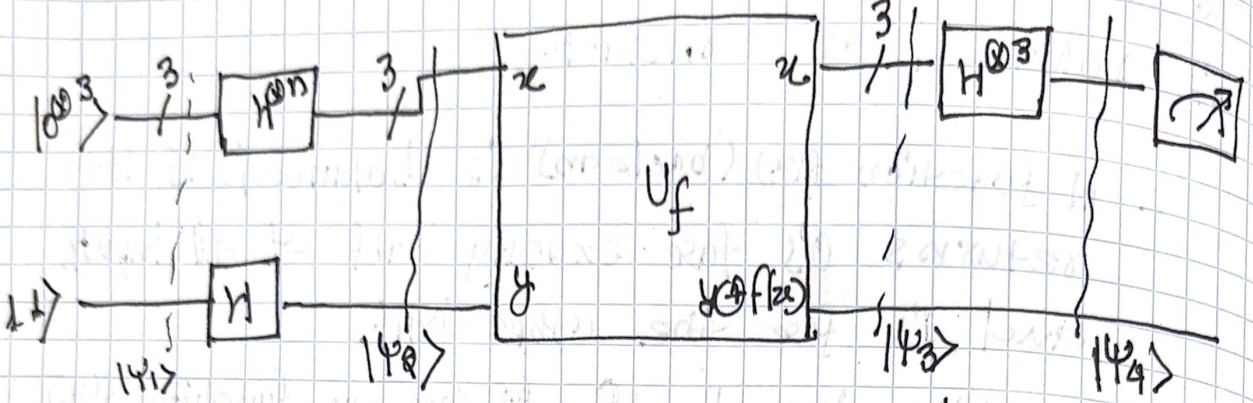
For 3 i/ps qubits (x_0, x_1, x_2), total $2^3 = 8$ Possible I/P combinations.

x_0	x_1	x_2	$x_1 \cdot x_2$	$f(x) = x_0 \oplus x_1 \cdot x_2$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	0

As we can observe from above truth table O/P $(f(x)$ has 4 0's and 4 1's

therefore, boolean function $f(x)$ is balanced* as it produces an equal number of 0s and 1s for all possible I/P combination.

iv) Quantum circuit diagram



We can use Deutsch-Jozsa Algorithm, to efficiently detect whether provided function is balanced or constant by leveraging quantum superposition and Interference.

Above drawn quantum circuit can detect for Balanced or constant.

Let's justify my claim,

as we know, $f(x) = x_0 \oplus x_1 \cdot x_2$.

Here, $n = 3$.

x	f(x)
0 0 0	0
0 0 1	0
0 1 0	0
0 1 1	1
1 0 0	1
1 0 1	1
1 1 0	1
1 1 1	0

from Generalize formula, final o/p,

$$|\psi_4\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} |y\rangle$$ where $n =$

and from truth table and stated in Q. iii) the function f(x) is balanced.

It means,

$\sum_{x \in (0,1)^n} (-1)^{f(x)} = 0$, then we will never measure $|0\rangle^{\otimes 3}$.

Balanced

$M \neq |0^3\rangle$

Solution of Algorithm

① $|\psi_1\rangle = |0\rangle^{\otimes 3} |1\rangle$

② Apply a Hadamard gate to each qubits:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}} \sum_{x=0}^{2^3-1} |x\rangle (|0\rangle - |1\rangle)$$

③ Apply the quatum oracle $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^4}} \sum_{x=0}^{2^3-1} |x\rangle (|f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$= \frac{1}{\sqrt{2^4}} \sum_{x=0}^{2^3-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

each $x, f(x)$ is either 0 or 1

④ Let this state ignored second register.

Apply a Hadmard gate to each qubit in 1st register.

$$|\psi_4\rangle = \frac{1}{2^3} \sum_{x=0}^{2^3-1} (-1)^{f(x)} \left[\sum_{y=0}^{2^3-1} (-1)^{x \cdot y} |y\rangle \right]$$

$$= \frac{1}{2^3} \sum_{y=0}^{7} \left[\sum_{x=0}^{7} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle$$

$$\boxed{|\psi_4\rangle = \frac{1}{8} \sum_{y \in \{0,1\}^3} \sum_{x \in \{0,1\}^3} (-1)^{f(x)+x \cdot y} |y\rangle}$$

lets check:

$|\psi_1\rangle = |000\rangle |-\rangle$

$|\psi_2\rangle = H^{\otimes 3} |000\rangle \; H|-\rangle$

$|\psi_2\rangle = \frac{1}{2\sqrt{2}} \Big[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle \Big] |-\rangle$

$|\psi_3\rangle = U_f |\psi_2\rangle$

$= \frac{1}{2\sqrt{2}} \Big[|000\rangle + |001\rangle + |010\rangle - |011\rangle - |100\rangle - |101\rangle - |110\rangle + |111\rangle \Big] |-\rangle$

$|\psi_4\rangle$ = Apply Hadamard gate to 1st register

$|\psi_4\rangle = \frac{1}{2\sqrt{2}} \Big[H|000\rangle + H|001\rangle + H|010\rangle - H|011\rangle - H|100\rangle - H|101\rangle - H|110\rangle + H|111\rangle \Big] |-\rangle$

$|\psi_4\rangle = \frac{1}{8} \Big[4|100\rangle + 4|101\rangle + 4|110\rangle - 2|111\rangle \Big] |-\rangle$

$|\psi_4\rangle = \Big(\frac{1}{2}|100\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|110\rangle - \frac{1}{4}|111\rangle \Big) |-\rangle$

Now, Sum of probabilities $\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{16} = \frac{3}{4}$.

this indicate partial destructive interference.

therefore,

- destructive interference for the state $|000\rangle$, indicate / consistent with a balanced function.
- and Non-Zero amplitudes for multiple steps also indicate a balanced function.

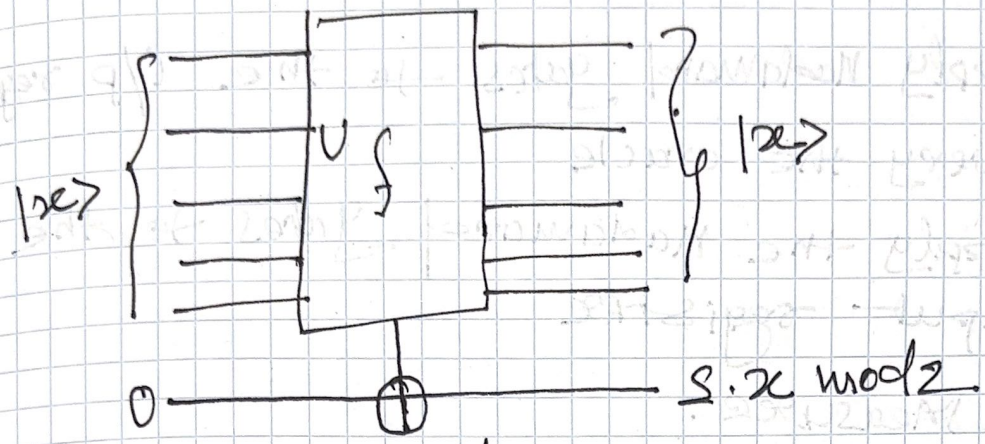
Hence, this Quantum circuit for given $f(x)$ could be able to indicate for balanced / constant Function.

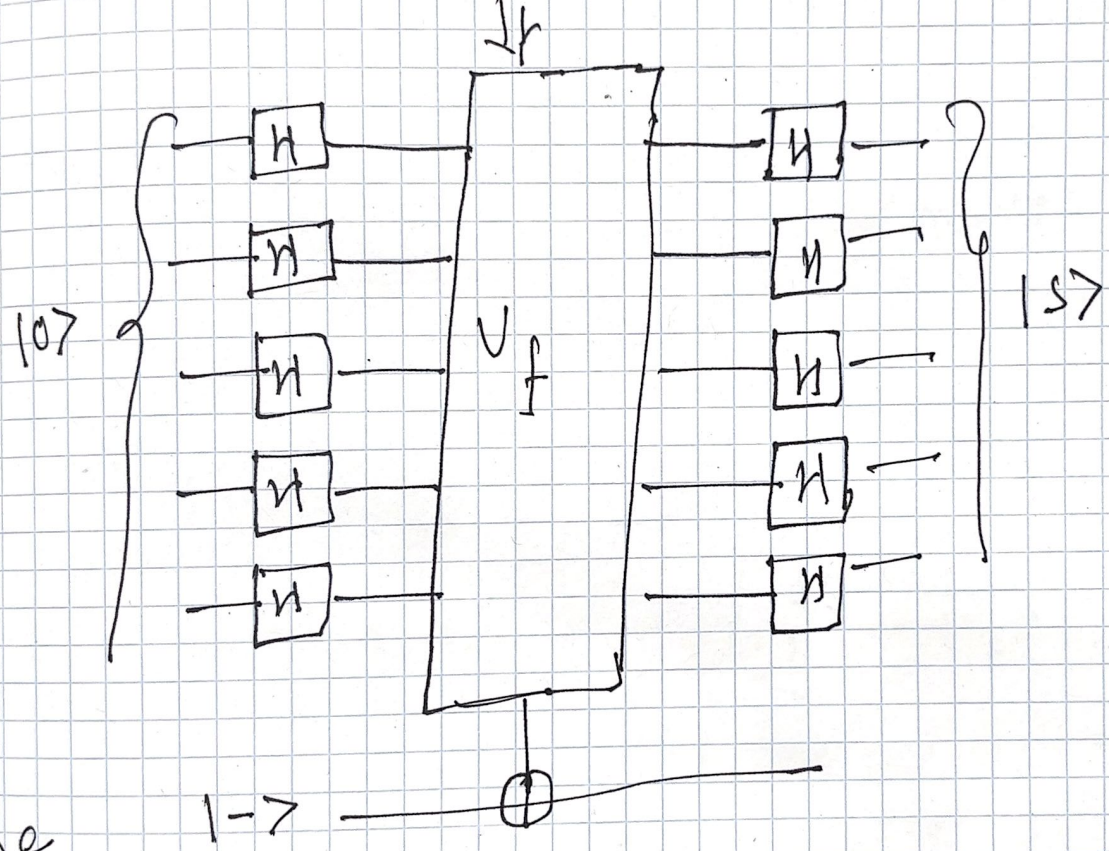
v)

$f(x) = s \cdot x \bmod 2$

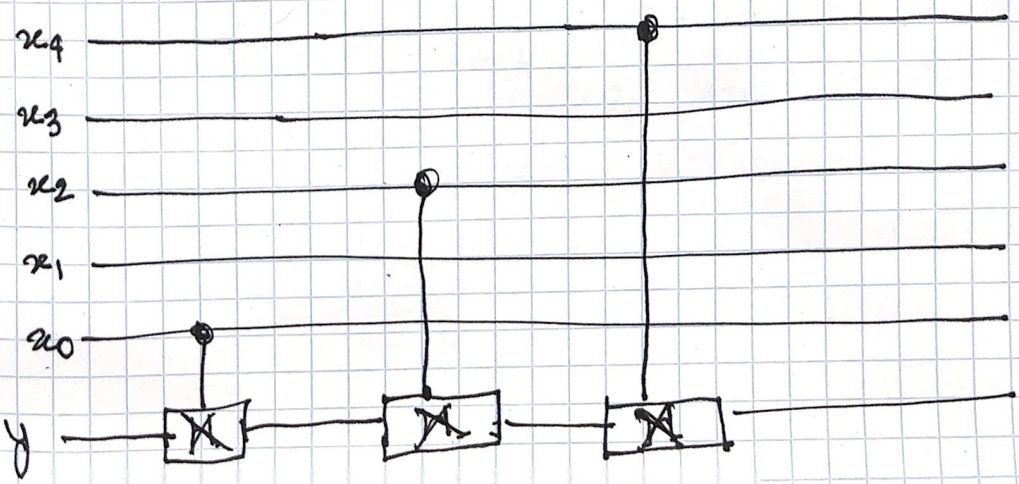
$x = 5$ b.t

ou $s = 10101$.





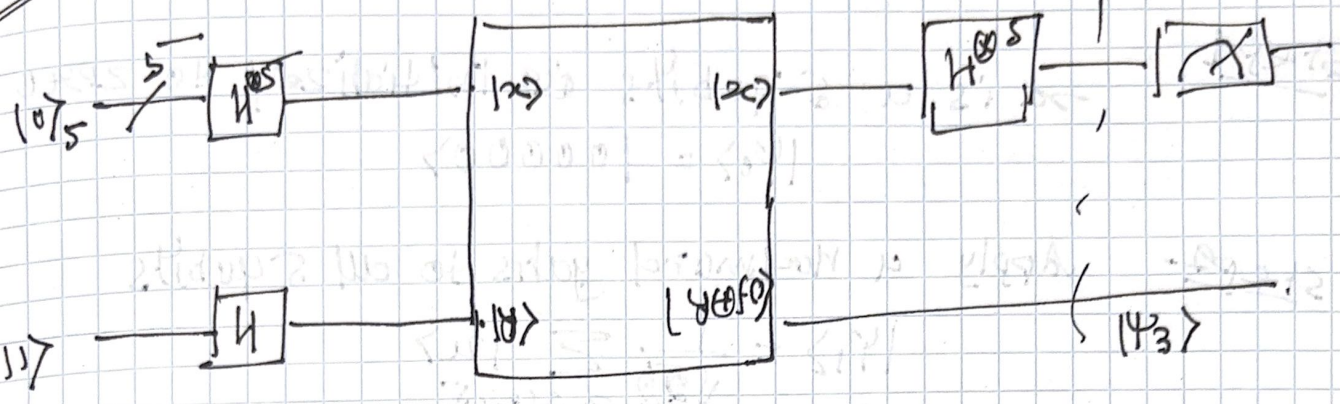
oracle



The Quatum Solution (reference to Part I of Q V.)

1. Initialize the inputs qubits to the $|0\rangle^{\otimes 5}$ state, and output qubit to $|-\rangle$
2. Apply Hadamard gates to the i/p register
3. Query the oracle
4. Apply the Hadamard gates to the input register
5. Measure.

Part-II



we already know,

$$|\psi_3\rangle = \frac{1}{2^5} \sum_{(x,y)\{0,1\}^5} (-1)^{f(x)+x\cdot y} |y\rangle$$

let's consider (measurement) only 1st register

$$|\psi_3\rangle = \frac{1}{2^5} \sum_{(x\in)\{0,1\}^5} (-1)^{f(x)+x\cdot y}$$

Given, $f(x) = s \cdot x \bmod 2$.

$$|\psi_3\rangle = \frac{1}{2^5} \sum_{x\{0,1\}^5} (-1)^{x\cdot s + x\cdot y}$$

$$|\psi_3\rangle = \frac{1}{2^5} \sum_{x\{0,1\}^5} (-1)^{x(s\oplus y)}$$

Further can be written as

$$|\psi_3\rangle = \frac{1}{2^5} \bigotimes_{j=0}^{4} \left[\sum_{x_j=0}^{1} (-1)^{(s_j \oplus y_j) x_j} \right]$$

If $s = y$ then above value is 1.

If $s \neq y$, then there exist j such that $s_j \oplus y_j = 1$. So the o/p in the case will be $|0\rangle$

So the final o/p will be

$$|s\rangle \otimes |1\rangle.$$

P.T.O

Explanation to determine the s value. (wordy)

Step 1 → is a 5 qubits are initialized to zero

$$|\psi_0\rangle = |00000\rangle$$

Step 2 Apply a Hadamard gates to all 5 qubits

$$|\psi_1\rangle = \frac{1}{\sqrt{32}} \sum_{x\in\{0,1\}^5} |x\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{32}} (|00000\rangle + |00001\rangle + |00010\rangle + \cdots + |11111\rangle)$$

Step 3: Oracle Transformation for $s = 1010$

the oracle applies the phase $(-1)^{s.x}$ to each basis state.

$$s.x = s_4x_4 \oplus s_3x_3 \oplus s_2x_2 \oplus s_1x_1 \oplus s_0x_0$$

Here, $s_4 = 1$, $s_3 = 0$, $s_2 = 1$, $s_1 = 0$ & $s_0 = 1$.

→ therefore, the oracle flips the phase of a basis state $|x\rangle$ if $x_4 \oplus x_2 \oplus x_0 = 1$

$$|\psi_2\rangle = \frac{1}{\sqrt{32}} \sum_{x\in\{0,1\}^5} (-1)^{s.x} |x\rangle$$

| if $s.x = 0$, phase +1
| $s.x = 1$, phase −1

$$|\psi_2\rangle = \frac{1}{\sqrt{32}} (|00000\rangle - |00001\rangle - |00010\rangle + |00011\rangle - |00100\rangle + |00101\rangle + |00110\rangle - |00111\rangle + \cdots + |11111\rangle)$$

Step 4: Applying Hadamard gate to all qubits.

$$|\psi_3\rangle = H^{\otimes 5} |\psi_2\rangle = H^{\otimes 5} \left(\frac{1}{\sqrt{32}} \sum_{x\in\{0,1\}^5} (-1)^{s.x} |x\rangle \right)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{32}} \sum_{x \in \{0,1\}^5} (-1)^{s \cdot x} \cdot H^{\otimes 5} |x\rangle$$

$$H^{\otimes 5} |x\rangle = \frac{1}{\sqrt{32}} \sum_{z \in \{0,1\}^5} (-1)^{x \cdot z} |z\rangle$$

Now, $$|\psi_3\rangle = \frac{1}{32} \sum_{z \in \{0,1\}^5} \left(\sum_{x \in \{0,1\}^5} (-1)^{s \cdot x + x \cdot z} \right) |z\rangle$$

on simplification,

$$|\psi_3\rangle = |s\rangle = |10101\rangle$$

Thus in single query the designed Quatum circuit is able to give Secret $s = 10101$