CS981 Assignment 1

CS981: Advanced Topics on Cryptography

Indian Institute of Technology Kanpur

Instruction We encouraged discussions but you should write your answer and honorably acknowledge the sources if any. Make sure you have not copied from others (or internet resources) and do not share your solution with others. For such circumstances, you may have been heavily penalized. Dishonest behaviour and cheating in the assignment will be penalized with extreme measures.

See: https://www.cse.iitk.ac.in/pages/AntiCheatingPolicy.html.

Kindly submit a ZIP folder to the ipearl portal (do not email). Your name of the folder should be ROLLNO.zip, eg 21111261.zip. This folder should contain your answer.

Question 1

i. Implement Controlled Controlled NOT Gate using basic quantum gates.

ii. Implement a quantum oracle that takes $|x>$ and $|y>$ as input and produces $|x>$ and $|y \oplus f(x)>$ as output where $f(x)$ is defined as follows: $f(x) = x_0 \oplus x_1.x_2$.

iii. Comment whether the function $f(x)$ is balanced or constant.

iv. Draw the Quantum circuit that can detect whether this function is balanced or constant. Justify your answer.

v. Consider a boolean function $f(x) = sx \ mod \ 2$ where x is a 5-bit value and $s = 10101$.

- Construct a quantum oracle circuit that will take x and y as inputs and will produce x and $y \bigoplus f(x)$ as output.
- Construct a quantum circuit that will use the aforementioned quantum oracle to determine the s value with a single query.