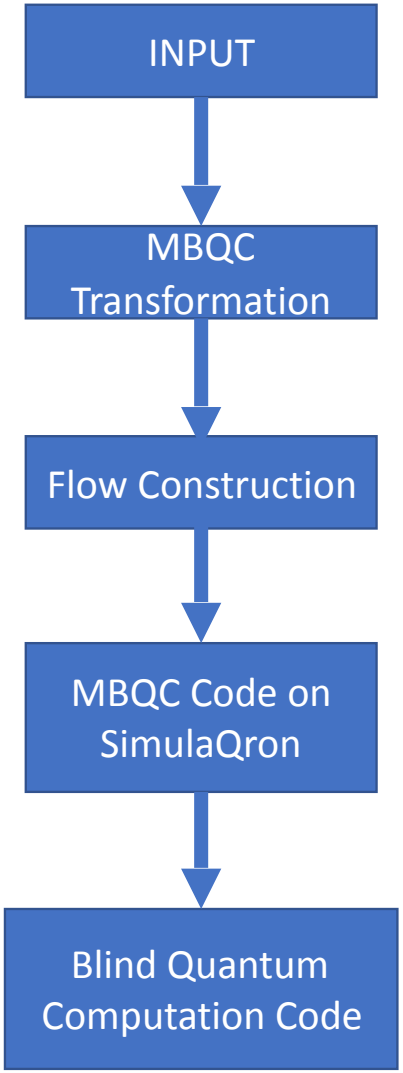
TEAM aMBiQuiCy

Team Members:

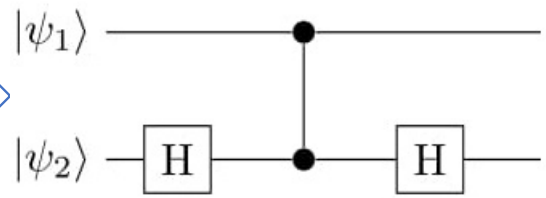
Andrey
Anne
Cristopher
Georg
Marc
Shraddha
Yao

Project: MBQC subroutine for SimulaQron
Implementation: Blind Quantum Computation

WORK FLOW:

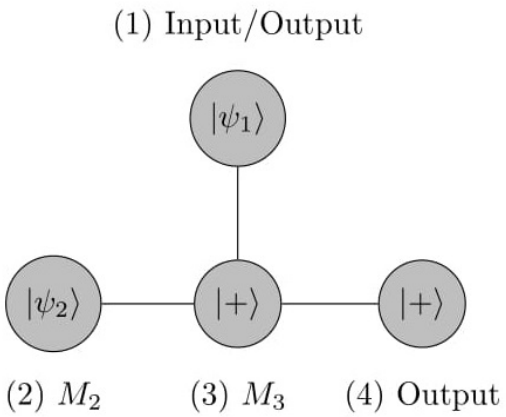

INPUT
MBQC Transformation
Flow Construction
MBQC Code on SimulaQron
Blind Quantum Computation Code

Example: C-NOT



MBQC transformation:
(Includes only measurement and entanglement)

INPUT: $H_2E_{12}H_2$

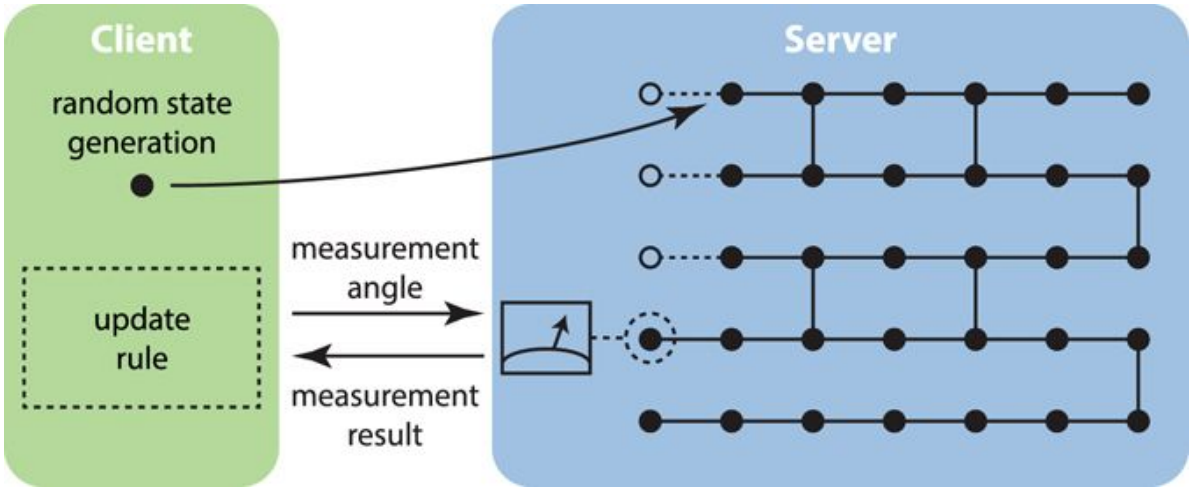


SimulaQron

$X_4^{s_3} Z_4^{s_2} Z_1^{s_2} M_3^x M_2^x E_{13} E_{234}$

3.) Flow Construction

Qubits: 1,2,3,4
Outcomes: s_1, s_2, s_3, s_4
Circuit Operation: $X_4^{s_3} M_3^x E_{34} E_{13} X_3^{s_2} M_2^x E_{23}$.



BLIND QUANTUM COMPUTATION

1.) Client generates **random** Qubits

2.) Client sends qubits to Server and **entanglement information**

3.)Server entangles the received qubits accordingly

4.) Client computes **measurement angles** for qubits using **update rule** and sends it to the Server

5.) Server measures and communicates the **measurement result** to the Client

6.) Client uses the received **result** to recover correct outcome of computation.

DEMO

https://giant.gfycat.com/EarnestImperturbableAbalone.webm

EXTENSION

- Current Blind Quantum Computation protocol incorporates only classical input/output case but MBQC subroutine is designed for quantum and classical input/output . Protocol can be extended to the quantum input/ output case by adding following steps
    1. quantum one time pad of input/ output states during generation of qubits
    2. output correction of output qubits in the end.

- Use universal resource states for MBQC for better security

Thanks!