Quantum Computing Hackathon July 2023
on

Noise Model Simulation of QKD Protocols using QSim

Organized by IIIT Roorkee and CDAC Hyderabad

Submitted by
Team
Noise Model Simulations of QKD Protocols using QSim

Participants
of
Quantum Computing using Indigenous Quantum Simulator QSim

Dr. Ajanta Das
Amity University Kolkata,
Newtown, Kolkata 700135

Email: ajanta.desarkar@gmail.com

Varsha Chakraborty
University of Engineering & Management
Newtown, Kolkata 700160

Email: chakrabortyvarsha1@gmail.com

Introduction

- Quantum Key Distribution (QKD) protocols provide secured Quantum communication
- QKD uses classical channel and quantum channel
- Interference or noise may occur in quantum circuit
- Quantum systems are highly sensitive to disturbances from the environment
- A security interface between the classical and quantum network is necessary

Motivation

- From literature, it is evident that analysis of noise models of QKD protocols is essential for fault tolerant quantum communication
- Quantum computers are expensive and difficult to access
- Programming in Quantum computers are different than that in classical computers
- Crucial to evaluate the QKD protocol in real platform of quantum computer
- Quantum simulators – QASM and QSim are chosen for analysis and modeling

Objective

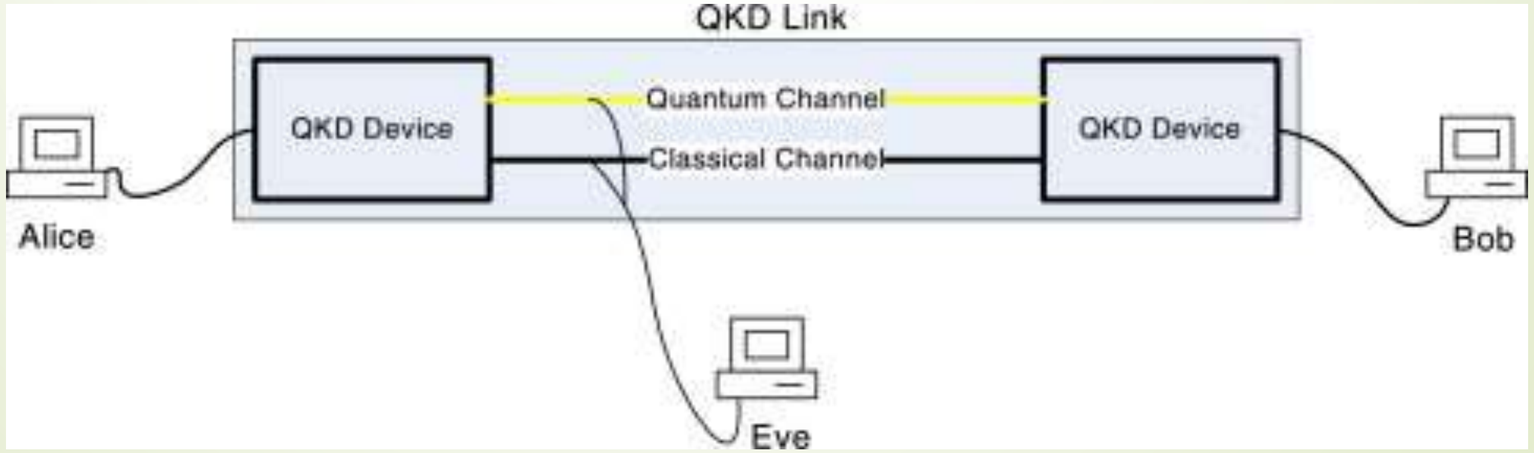
1. Study and Implementation of QKD protocols
   - BB84, the first QKD protocol
   - Differential Phase Shift (DPS)
2. Chosen Quantum Simulators
   - IBM Quantum assembly language, QASM
   - Qsim built by IISc Bangalore and IIT Roorkee and C-DAC
3. Execution of Noise models of the QKD Protocols in simulators
   - Circuit Noise, Bit Flip
   - Channel Noise, Depolarization

Quantum Key Distribution

Quantum Key Distribution

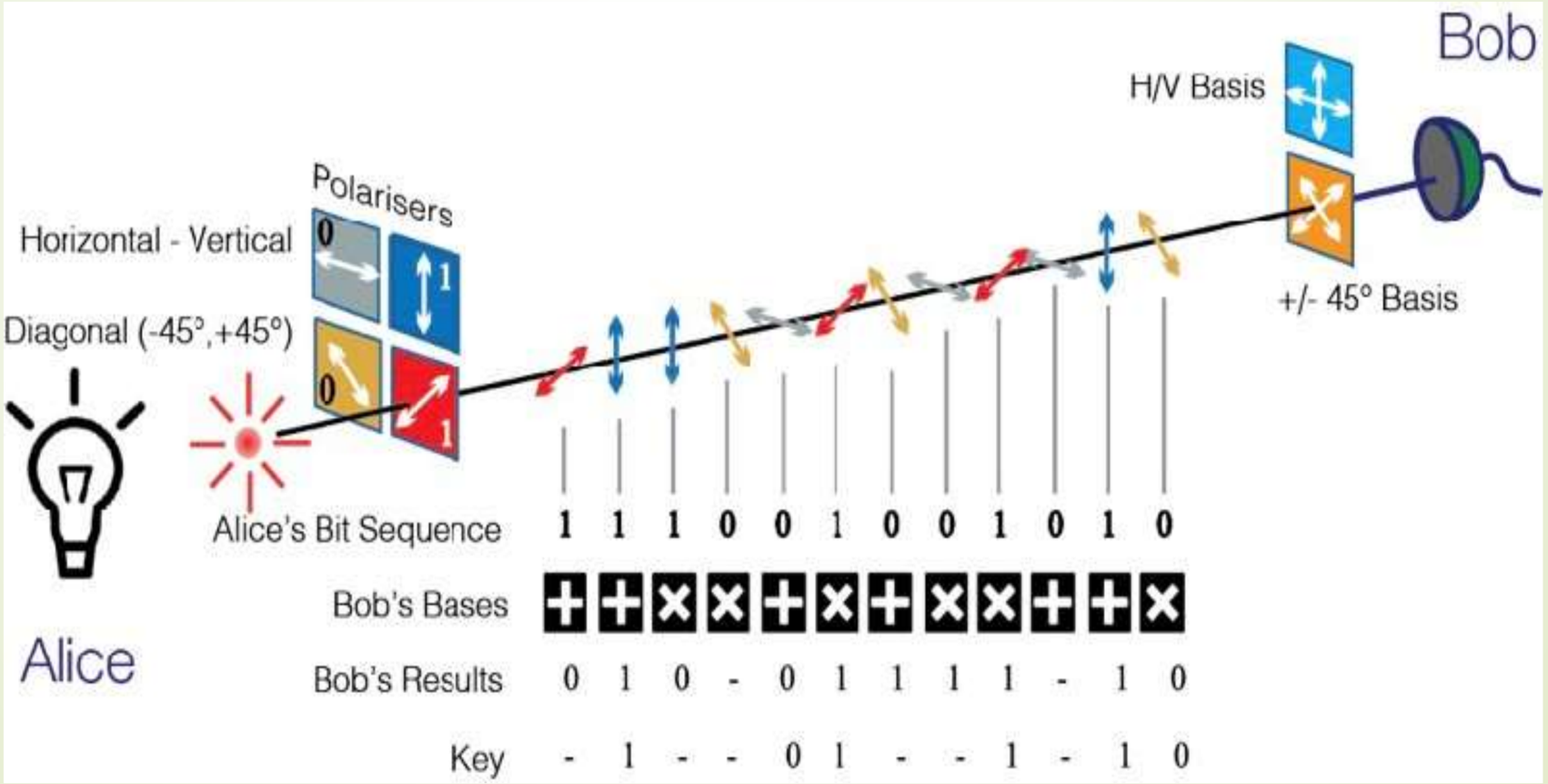
- uses a series of photons to transmit data over a fiber optic
- to guarantee a secure key agreement

- Alice and Bob generate a secret key by sending qubits
- Utilizes classical channel and quantum channel
- Eavesdropping may happen by Eve

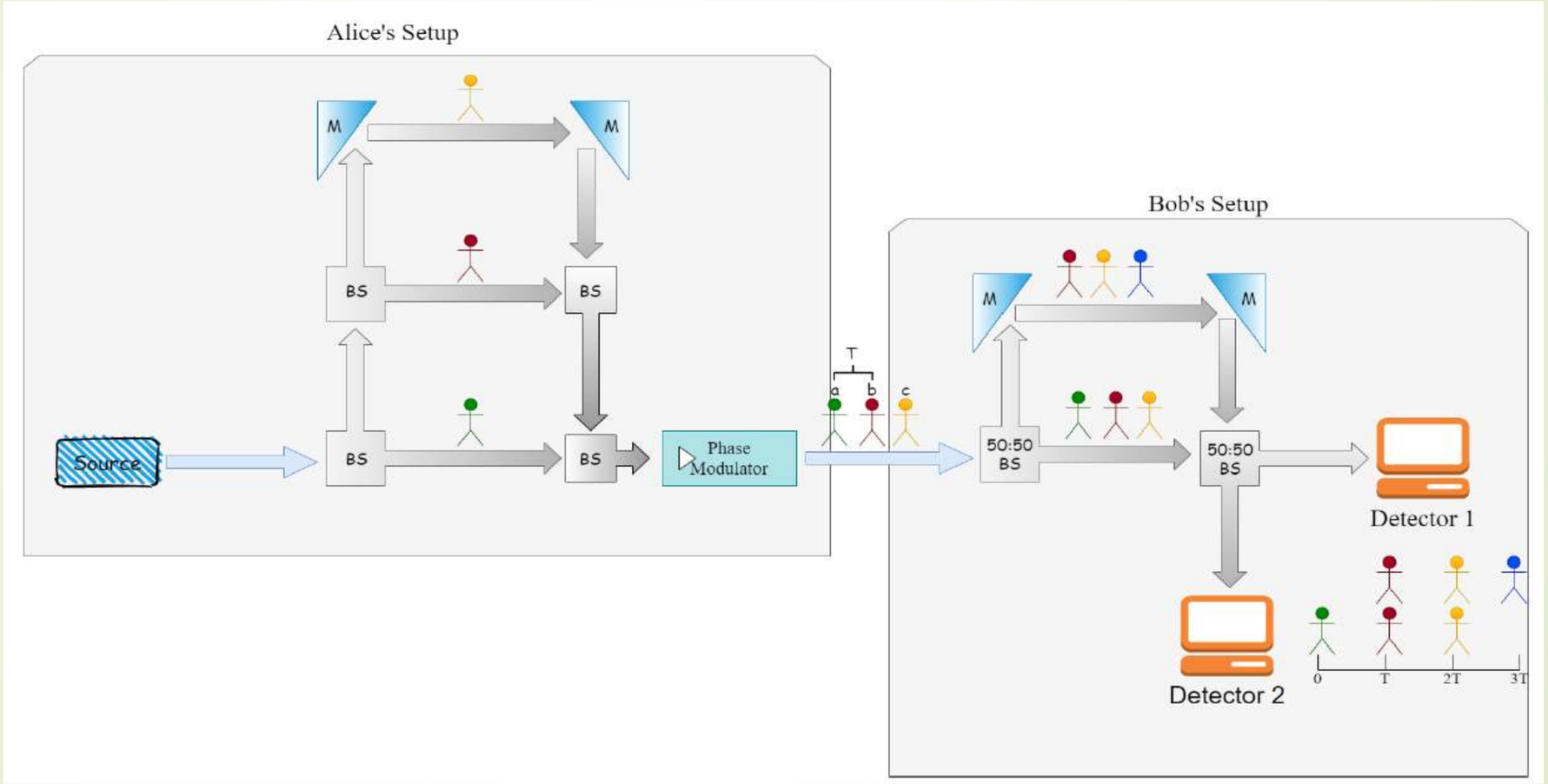


BB84 Protocol

- First quantum cryptography protocol, proposed by Charles Bennett and Gilles Brassard in 1984
- based on Quantum Key Distribution, polarization and no cloning theorem



DPS Protocol



Noise in Quantum Communication

- Circuit Noise
  - Bit Flip - flipping the bit values to 1 from 0 or vice versa; X gate is used
  - Phase Flip – phase changes due to physical parameters and superposition; Z gate is used
- Channel Noise
  - Depolarization – due to hardware infidelity; X, Y, Z and I gates are used
  - Amplitude Damping – energy dissipation or loss of photon
  - Phase Damping – loss of information
  - Decoherence - due to thermal relaxation, decoherence occurs

QASM Vs QSim

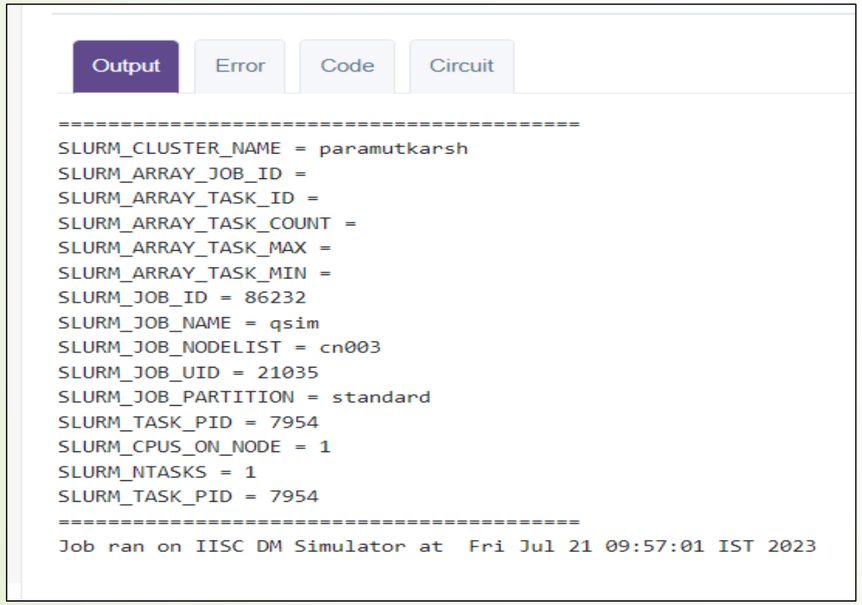
- ✓ QASM, developed by IBM Quantum Composer in 2020
- ✓ Drag and drop and prepare the quantum circuit
- ✓ Prototyping 32 qubits qubits quantum circuits, algorithms and noise models
- ✓ In India, the first initiative of Govt. of India to propose QSim in 2020-2021
- ✓ QSim is proficient by C-DAC, IISc Bangalore and IIT Roorkee
- ✓ Provides a graphical user interface to easily explore quantum computing with 10 qubits

QASM Environments

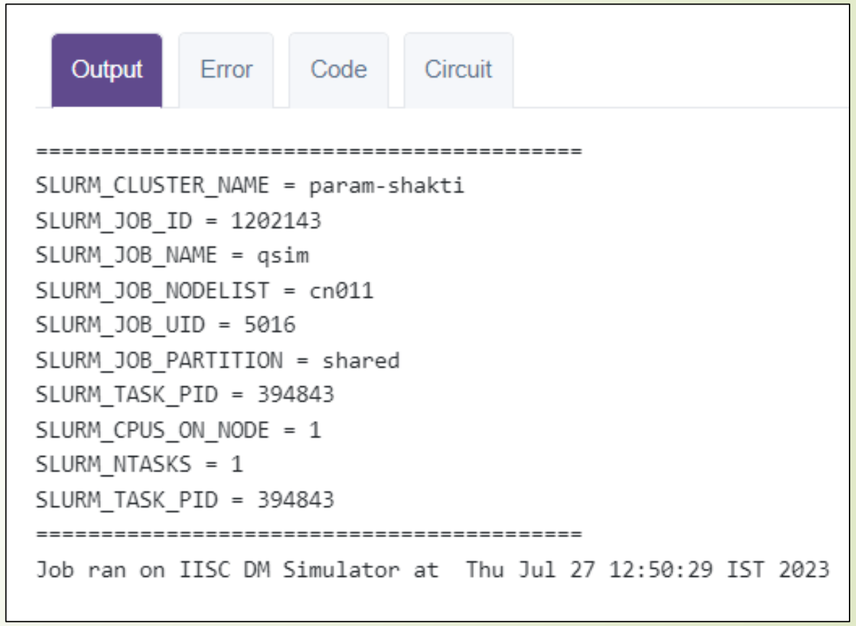
Provider	***qiskit-ibmq-provider0.19.1***
Simulator	*qiskit-aer0.10.4*
Languages	*qiskit0.36.2; Python version 3.8.12*
Compiler	*Python compiler GCC 9.4.0*
Operating System	*Linux*
CPU	*2*
Memory	*(Gb)6.783603668212891*

Qsim Environements

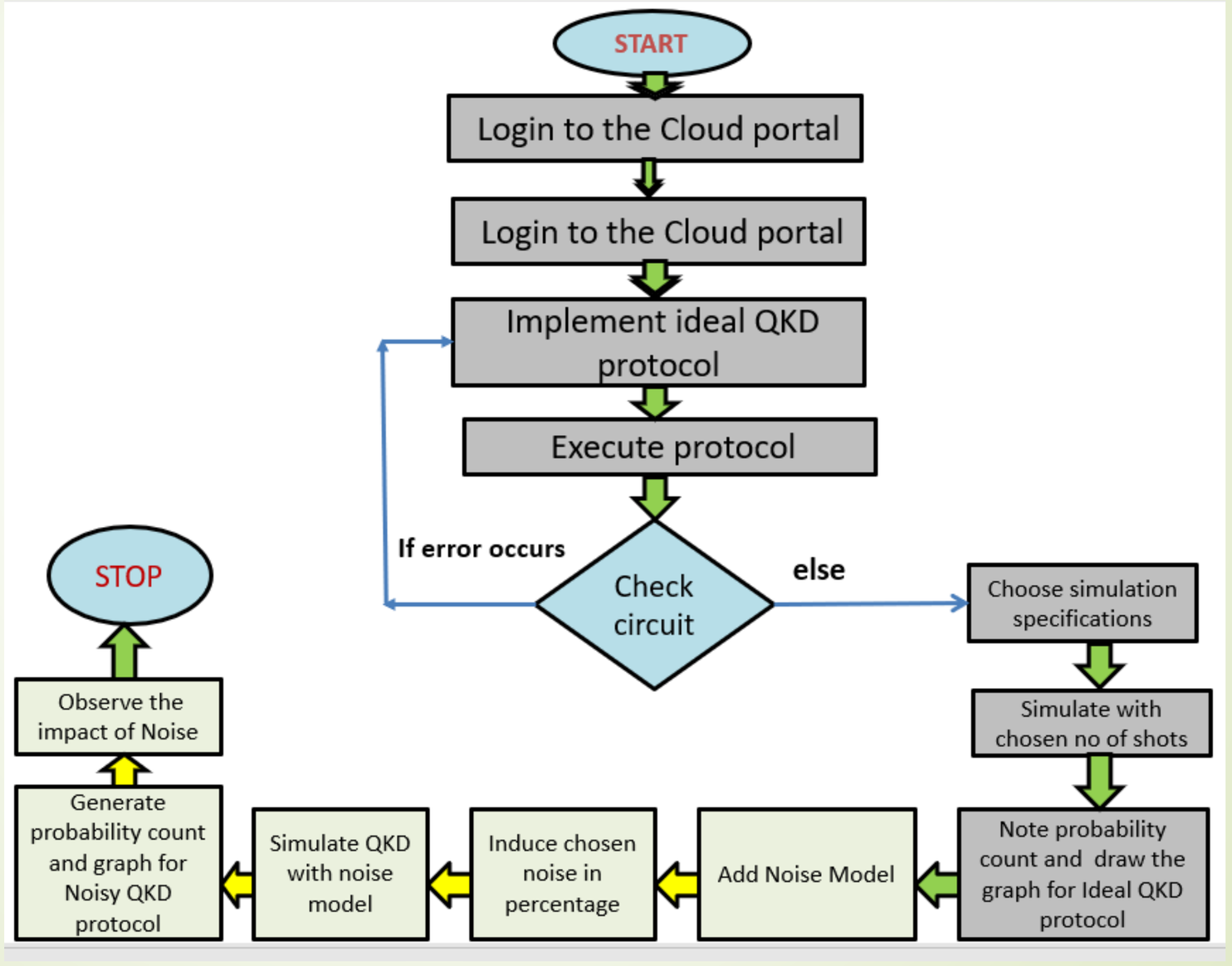
- Selected Backend PARAM UTKARSH
- Snapshot of execution of one Job



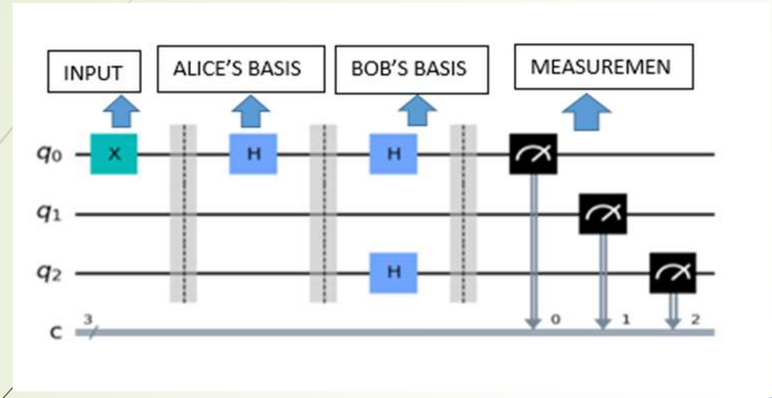
- Selected Backend PARAM SHAKTI
- Snapshot of execution of one Job

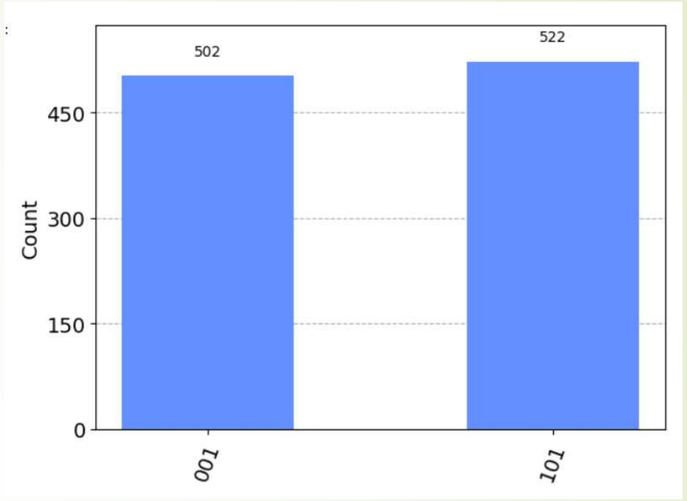


Flowchart of Methodology

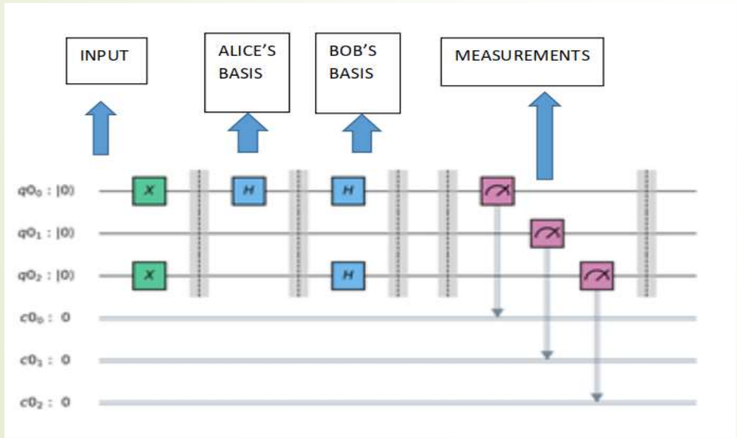


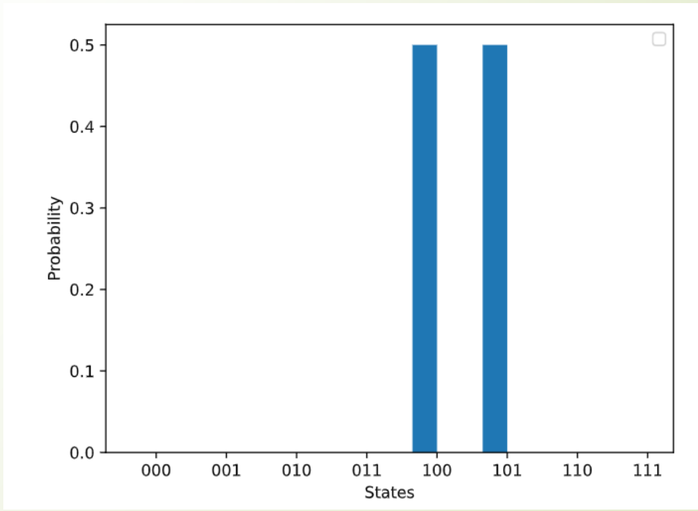
Ideal BB84 - QASM Vs QSIM using 3 Qubits





QASM



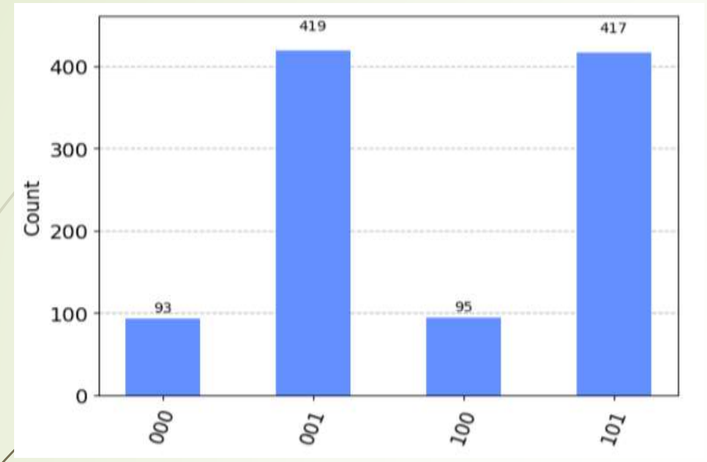


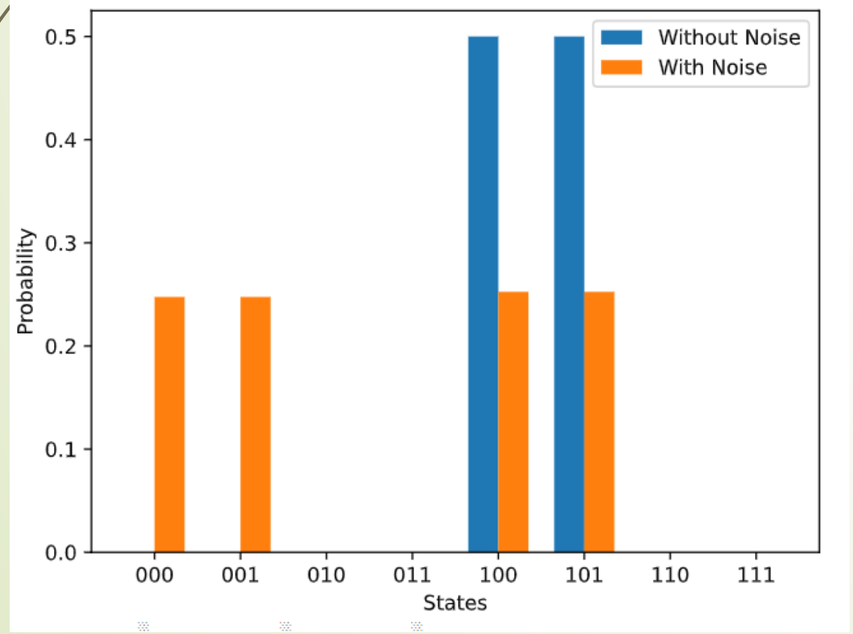
QSIM

Noise Models - QASM Vs QSIM
BB84 - using 3 Qubits

BIT FLIP

10%=0.1



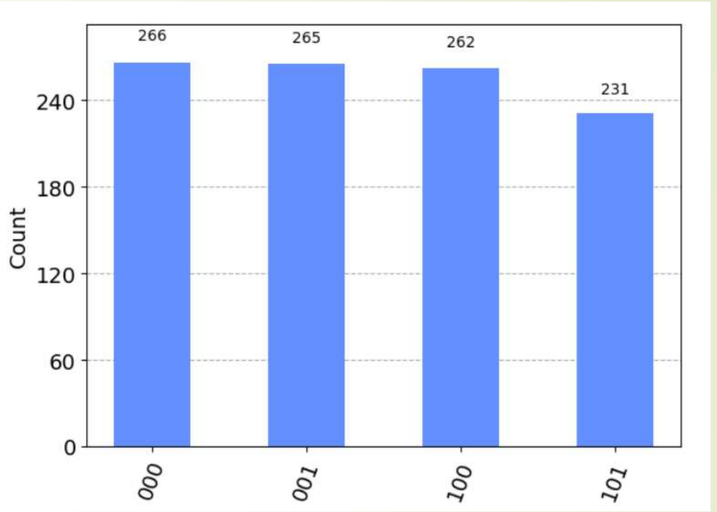


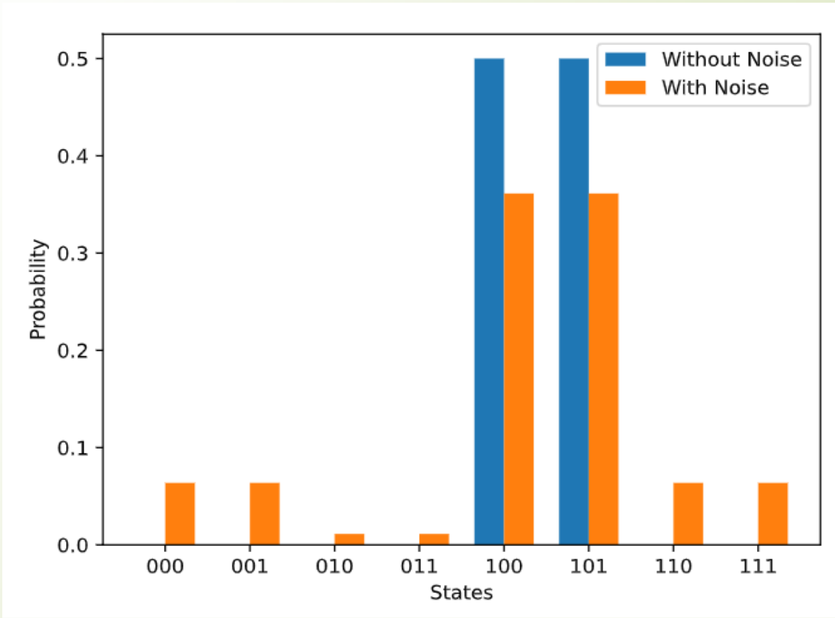
QASM

QSIM

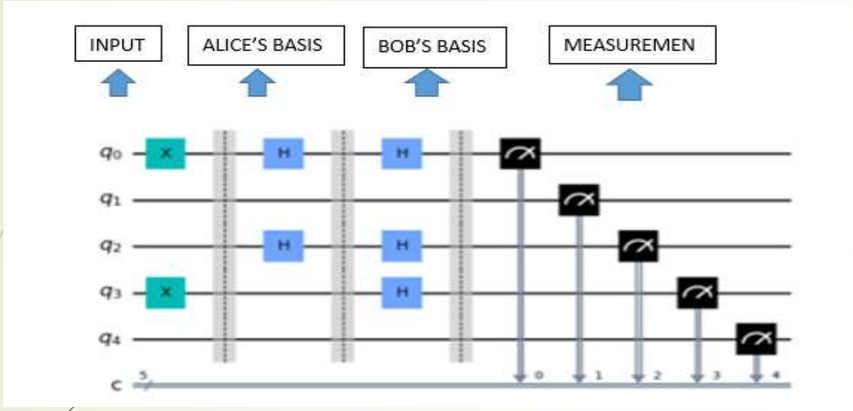
DEPOLARIZATION

70%=0.7

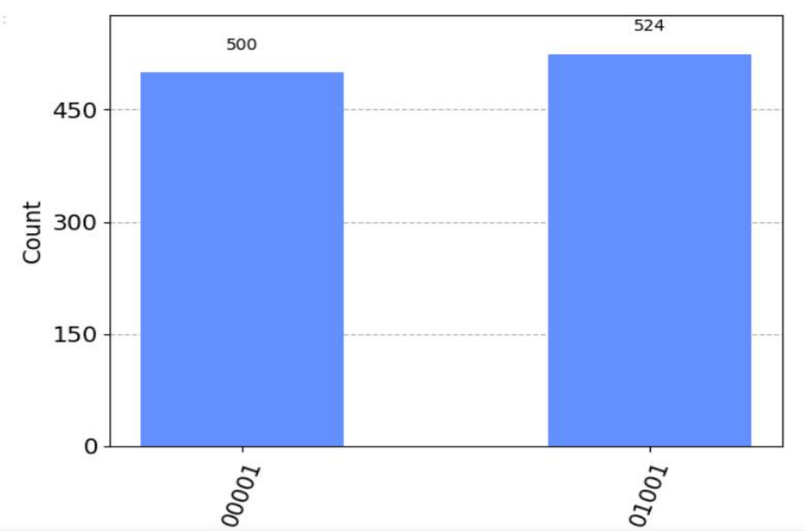


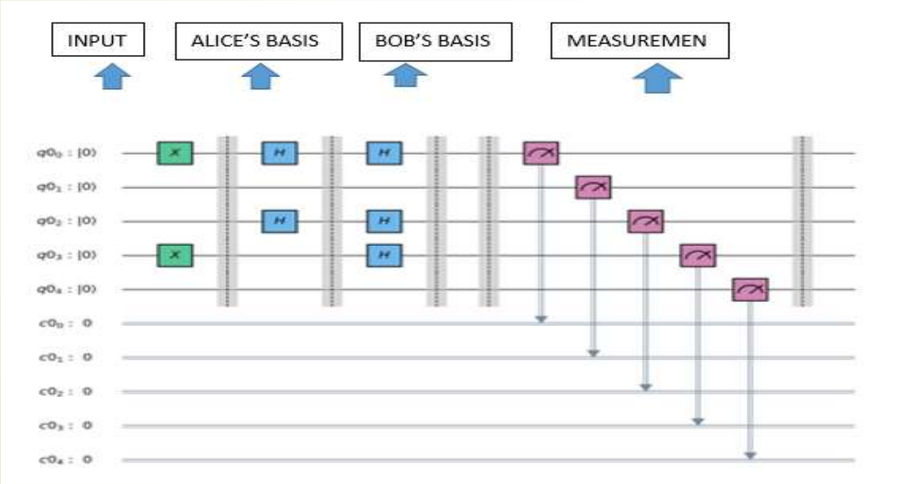


Ideal BB84 - QASM Vs QSIM using 5 Qubits

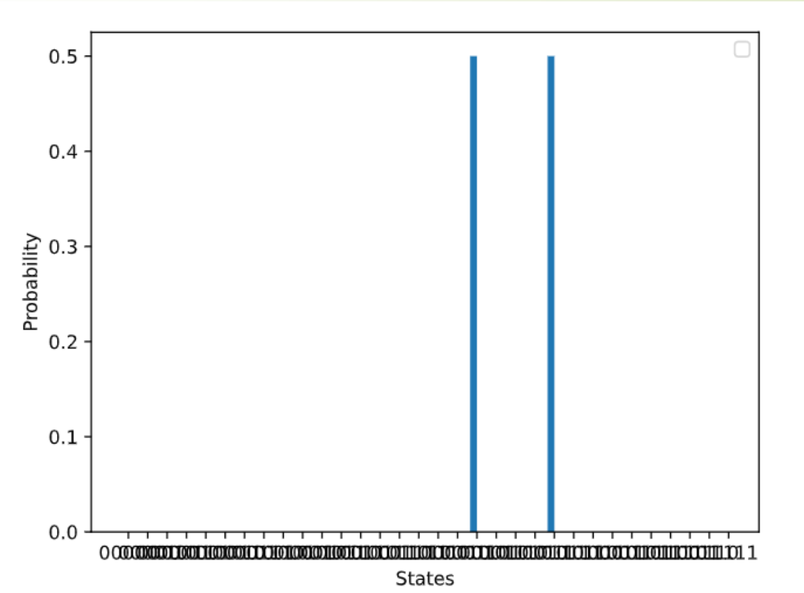


QASM





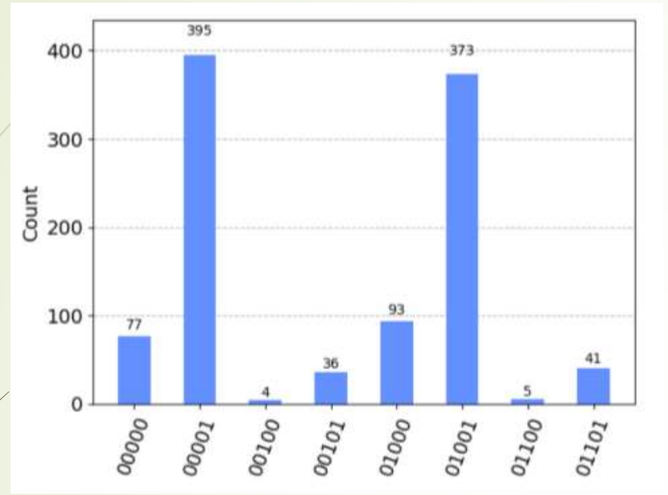
QSIM

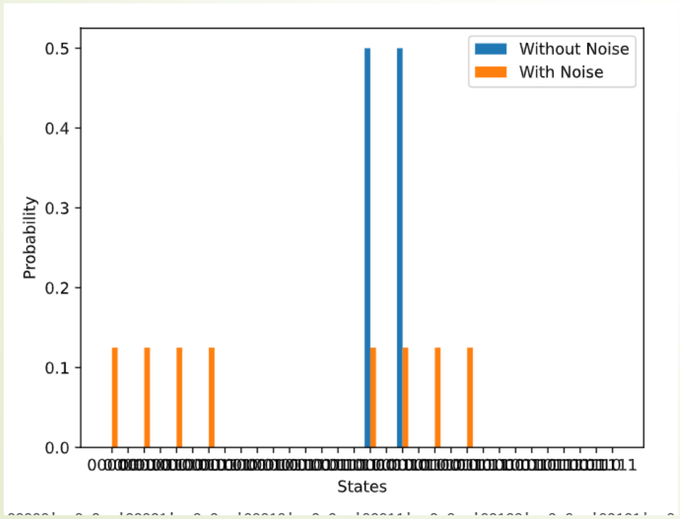


Noise Models - QASM Vs QSIM
BB84 - using 5 Qubits

BIT FLIP

10%=0.1



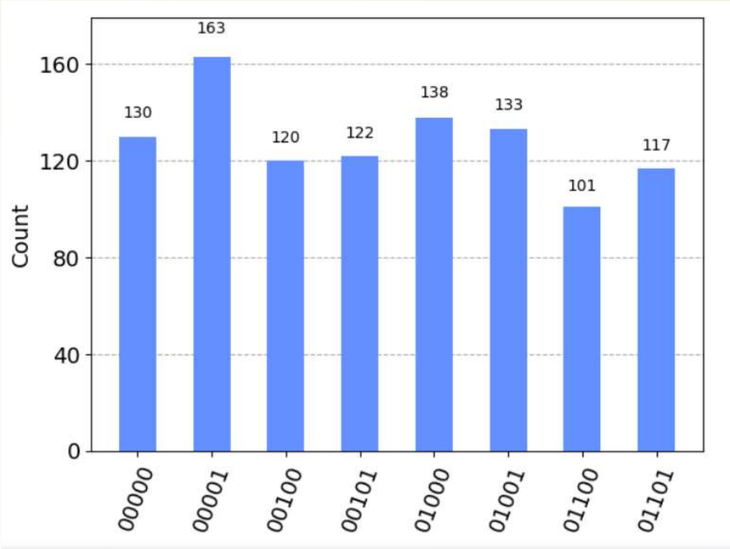


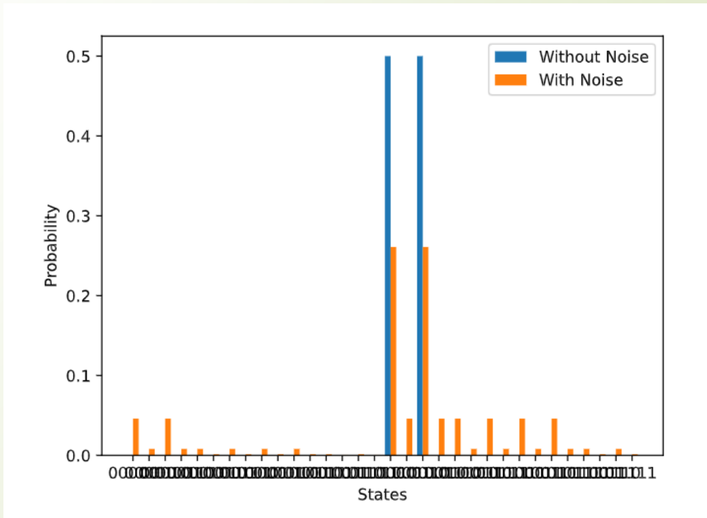
QASM

QSIM

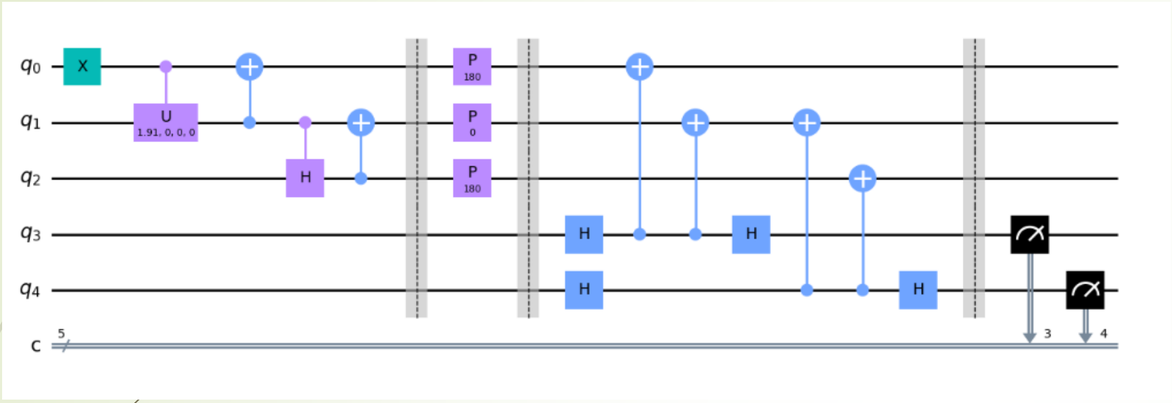
DEPOLARIZATION

70%=0.7

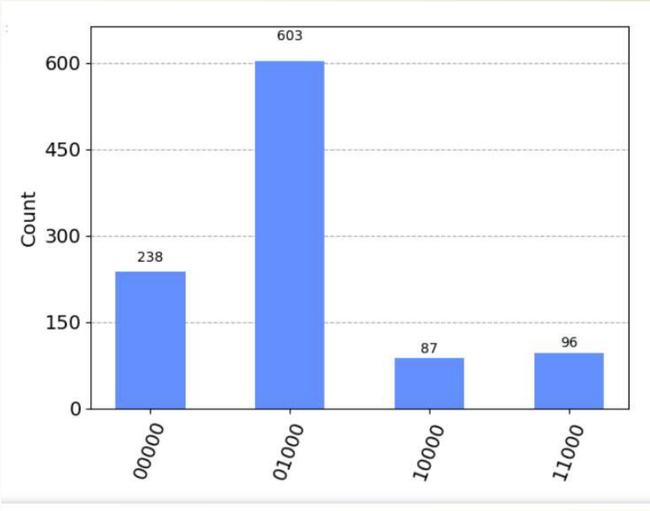


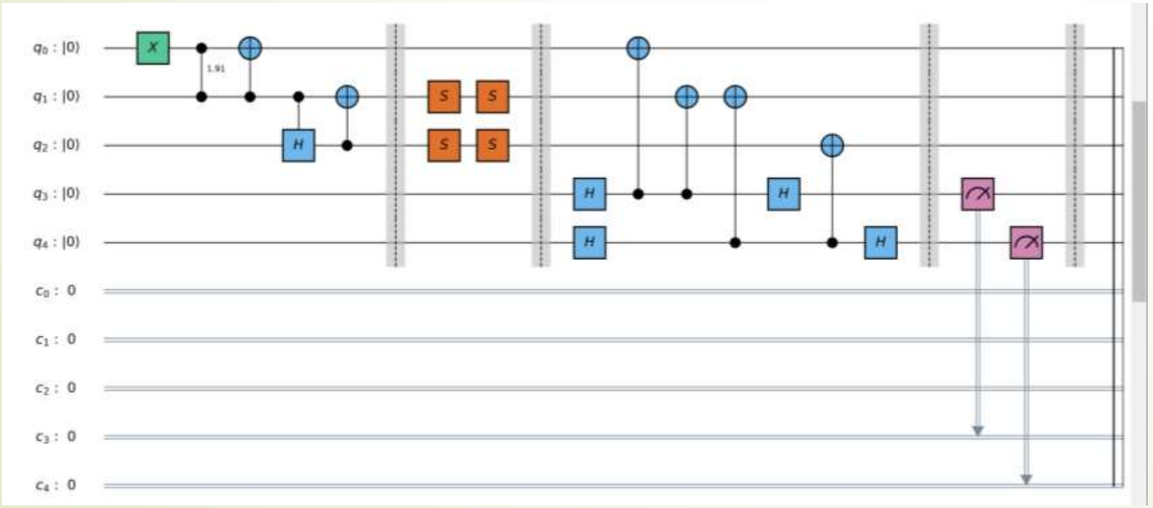


Ideal DPS - QASM Vs QSIM

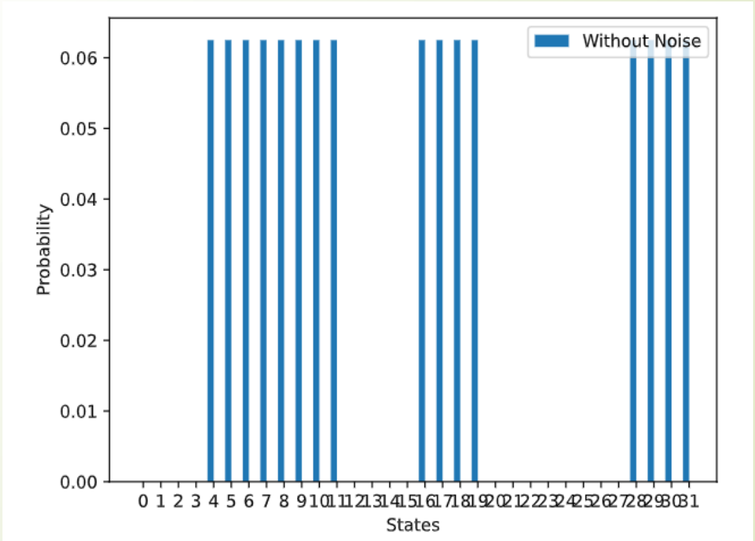


QASM





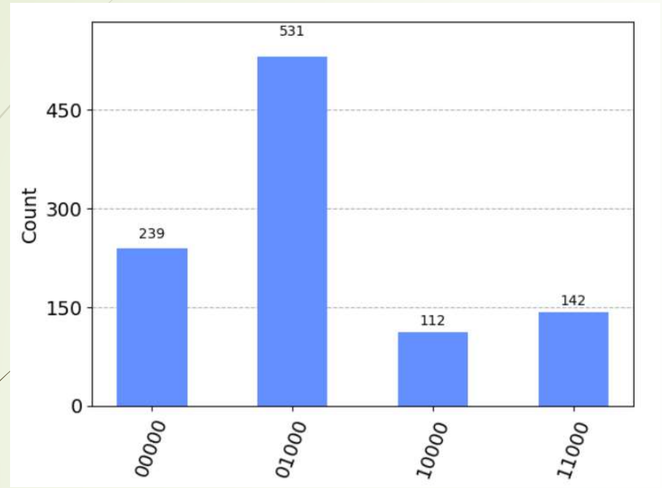
QSIM

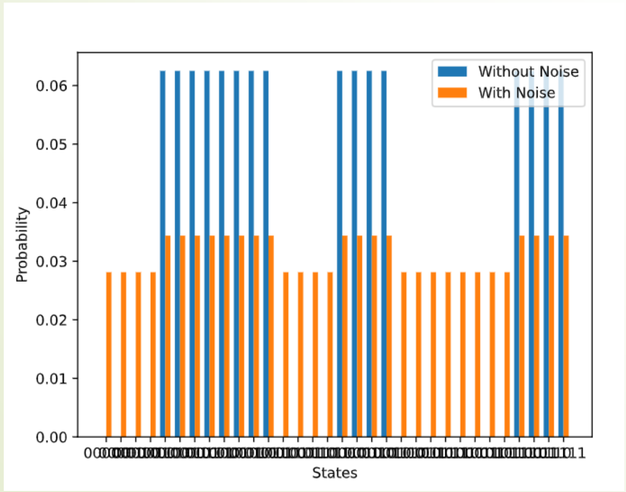


Noise Models - QASM Vs QSIM DPS

BIT FLIP

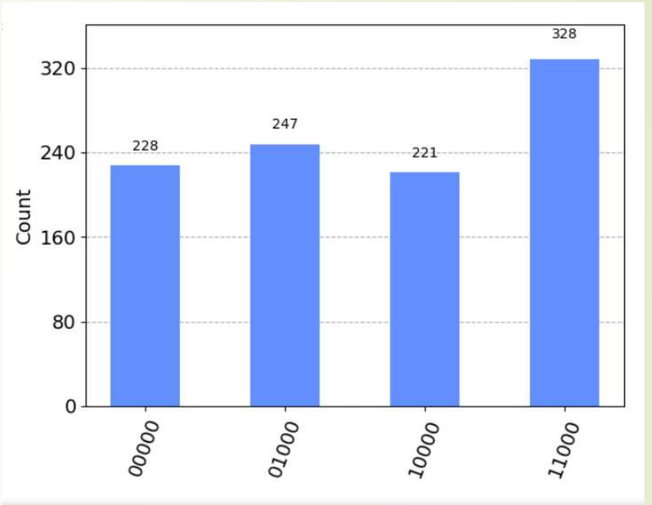
10%=0.1



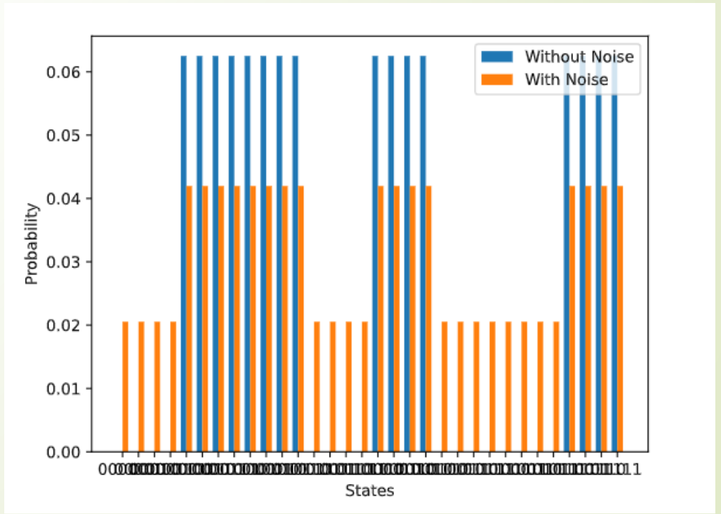


QASM

DEPOLARIZATION



70%=0.7



QSIM

Observations and Analysis

- In case of Ideal models, both simulators QASM and QSim produce identical results
- In case of Noise models, results for QASM and QSim vary:
  - Complexity increases with increase of Qubits, hence noise propagates or spreads more
  - Logic operations are different – mathematical formulations are different
  - QASM uses Least Significant Bit first and Most Significant Bit last; QSim uses conventional: Most Significant Bit first and Least Significant Bit last
  - QSim is slower that QASM, as it produces the complete output probability distribution in one run. However, QASM requires multiple runs of the same program to verify the purpose

Conclusion

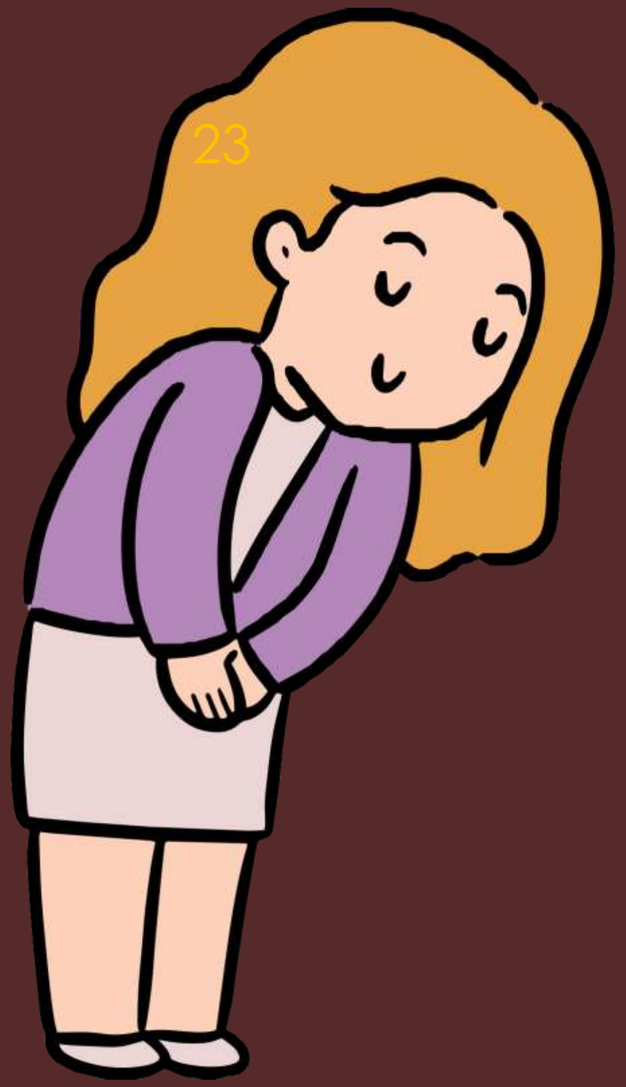
- Quantum Key Distribution Protocols – BB84 and Differential Phase Shift (DPS)
- Simulations of BB84 in QASM and QSim
- Simulation of Circuit and Channel Noise models of BB84
- Simulations of DPS in QASM and QSim
- Simulation of Circuit and Channel Noise models of DPS
- Comparison between results achieved in QASM and QSim simulators
- **Future Scope:**
  - ✓ Essential to understand gap between real environment and simulators
  - ✓ Study of security impact using Noise models

References

1. N. Alshaer, A. Moawad and T. Ismail, "Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System," in IEEE Access, vol. 9, pp. 168052-168067, 2021, doi: 10.1109/ACCESS.2021.3137357.
2. Peng-Liang Guo, Chen Dong, Yi He, Feng Jing, Wan-Ting He, Bao-Cang Ren, Chun-Yan Li, and Fu-Guo Deng, "Efficient quantum key distribution against collective noise using polarization and transverse spatial mode of photons," Opt. Express 28, 4611-4624 (2020).
3. K. Lim, H. Ko, K. Kim, C. Suh and J. -K. K. Rhee, "The Error Tolerance Bound for Secure Multi-Qubit QKD Against Incoherent Attack," in IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 178-186, May-June 2015, Art no. 6600809, doi: 10.1109/JSTQE.2014.2369498.
4. Konstantinos Georgopoulos, Clive Emary, Paolo Zuliani, “Modelling and Simulating the Noisy Behaviour of Near-term Quantum Computers”, Phys. Rev. A 104, 062432 (2021), DOI: https://doi.org/10.1103/PhysRevA.104.062432.
5. Himanshu Chaudhary, Biplab Mahato, Lakshya Priyadarshi, Naman Roshan, Utkarsh, Apoorva D. Patel, “A Software Simulator for Noisy Quantum Circuits”, https://arxiv.org/abs/1908.05154, 2019, DOI: 10.48550/ARXIV.1908.05154.
6. IBM Quantum Simulators, https://quantum-computing.ibm.com/lab/docs/iql/manage/simulator/
7. Jupyter Notebook: https://jupyter.org/
8. Learn Quantum Computation using Qiskit: https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html

References

9. Michael A. Nielson and Isaac L. Chuang, “Quantum Computation and Quantum Information”, 2010, Cambridge University Press, 978-1-107-00217-3.
10. Noson S. Yanofsky and Micro A. Mannucci, *Quantum Computing for Computer Scientists*. Cambridge: Cambridge University Press, 2008, doi:10.1017/CBO9780511813887.
11. Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem, “Quantum Key Distribution: Simulation and Characterizations”, Procedia Computer Science, Volume 65, 2015, Pages 701-710, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.09.014.
12. Philip Kaye, Raymond Laflamme and Michele Mosca, “An Introduction to Quantum Computing”, Oxford University Press, 2007, 978-0-19-857000-4.
13. Qsim – Quantum Computer Simulation Toolkit, https://qctoolkit.in/.
14.. Rakesh Saini, Ankit Papneja, Bikash K. Behera and Prasanta K. Panigrahi, “Experimental Realization of Differential Phase Shift Quantum Key Distribution on IBM QX”, Preprint Dec 2019, DOI: 10.13140/RG.2.2.10904.14089.
15. Inoue, Kyo and Waks, Edo and Yamamoto, Yoshihisa, “Differential Phase Shift Quantum Key Distribution”, PhysRevLett.89.037902, Vol 89, Issue 3, pages 037902 – 037904, 2002, American Physical Society, DOI: 10.1103/PhysRevLett.89.037902
16 Riley T. Perry, “The Temple of Quantum Computing”, December 2004.



THANK YOU