Noise Model Simulation of QKD Protocols using QSim

Proposal Submitted:

The advancement of smart technology makes data hacking or robbery currency a major threat to necessary online communications. Smart computation, i.e., online communication and transaction are solely depending on internet technology. So, most of every important data of any human being is traversing through internet on daily basis. It is not surprising if some data through internet can be hacked or utilized for some mischievous purpose. Although cyber cryptography is taking care of the security of data which communicating through various networks or paths between the receivers and senders through classical computation. However, it lacks providing the security for huge data available in internet before reaching to its proper destination. Although classical cryptography-based security is provided but, the hackers become knowledgeable with all these cryptography algorithms. Hence the role of quantum cryptography becomes essential for providing the secret key through quantum channel. Classical computational security or authentication need to utilize quantum computation techniques to provide robust cyber security in business.

Many large companies, such as, Microsoft, IBM, Google, CDAC, etc. are investing lot of money in development of quantum computer. Learning of quantum computing blends quantum physics, quantum mechanics with information theory and computer science. Quantum computation is based on mathematics, super basic linear algebra, such as, matrix, vector, and tensor product. Polarization can be cited as a simple quantum phenomenon. Execution of the same complicated problem in quantum computer will enhance the speedup exponentially rather than in classical computer. Point to be noted that we should not misuse the power of quantum computer with simple problems, which can be easily solved in classical computers. Evidently, quantum computers mostly solve the hard problems in polynomial time. Unlike, classical computer, each operation performed by quantum computer is reversible. Reversible operations require million times more energy, hence exponential speedup is achieved in quantum computer.

In quantum computer, the operations or information are processed using qubits, $|0\rangle$ or $|1\rangle$, and sometimes between $|0\rangle$ or $|1\rangle$ using superposition of these qubits. In quantum secure communication the information is carried on any of the degree of freedom of these photons. They are generated, encoded, and transmitted from one location to another over a fiber optic cable or in free space. Since the information is encoded in quantum entity hence by the rules of quantum mechanics any disturbance or tampering of information on these qubits will be detectable. This is the role of quantum cryptography, and it plays an essential part in security of communication. Generally, quantum cryptography is based on the polarization property of photon and quantum key distribution (QKD) in free space communication.

Simulation is applicable while it is hard to get the opportunity to execute in real system. Thus, simulation actually mimics the execution environment to get the essence of real-life scenarios. Sometimes it is not feasible to get the practical environment to test the algorithm. In case of, quantum

computing, quantum computers are expensive and not easily procured. Moreover, QKD link requires strong internet connection, optical fibers. Then QKD network needs to have the quantum computers or nodes to complete the testbed for real execution of the algorithm or protocol. To overcome this situation various simulators are available to verify the QKD protocols. Thus, the simulators are used to do comparative study of QKD protocols with respect to a few performance parameters, such as, key generation rate, bit error rate, transmission distance and resulted noise due to transmission. In order to apply these QKD protocols in business solutions, such as, healthcare or finance, simulation results guided improvement of the quantum circuits or quantum cryptography algorithm can be proposed.

Due to the fragile tendency of qubits, it is very easy to be affected by noise. Quantum noise can be observed on top of these general or common noises. In order to measure quantum noises the conventional sources of noise need to be restricted. Noise in quantum communication can be categorized into *circuit noise* and *channel noise*. Noise occurs in circuit or logic gates are identified as *circuit noise* while during message communication, noise may occur in channel, hence named as *channel noise*.

Necessary detection of any disturbance or tampering of information on these qubits is possible. Thus, this Project also studies various noises in quantum circuit and channel both. Therefore, it is absolute necessary to evaluate the QKD protocol in real platform of quantum computer.

In India, simulation-based research on quantum computing moves one step further with the first initiative of Government of India to propose QSim, a graphical user interface-based simulator, in 2020-2021. QSim is an indigenous simulation platform proficient by C-DAC, IISc Bangalore and IIT Roorkee, multidisciplinary group of researchers from industry and academics. The researchers from academics and industry can easily explore quantum computing through this platform, QSim. This project also deals the common challenges faced by the simulator. It provides a robust platform, as playground for students and teachers or researchers to customize the simulation with quantum circuits and observe the effects of quantum noises.

Therefore, this proposal will explore QSim to study the performance parameters of QKD protocols. The results achieved from simulator will help in filling the gap between abstract simulations of QKD and the actual experimental performance. With a more accurate prediction of experimental performance, resources may be more confidently allocated towards real-world QKD implementations.

This proposal presented simulation results of these various QKD protocols in the presence of circuit noise, bit flip, and channel noise, depolarization, executed in QSim.

To conclude, the major motivation of this proposal is to study the security impact using the graphical representation from implementation of two different QKD protocols in a QSim and introduce different noise and analyze the results in both the protocols in QSim.

Quantum Computing Hackathon July 2023

on

Noise Model Simulation of QKD Protocols using QSim

Implemented and submitted by:

Dr. Ajanta Das, ajanta.desarkar@gmail.com

and

Varsha Chakraborty, chakrabortyvarsha1@gmail.com

The major objective of this proposal is to carry out comparative evaluation of quantum key distribution protocols in noisy environment of quantum computing. In order to do this, this research presents the simulation of two QKD protocols, such as, BB84 and Differential Phase Shift (DPS), in two different simulators, QASM [IBM Quantum Lab] and QSim [IISC Bangalore and IIT Roorkee] varying qubits.

1. This Project work implemented and presented simulation results of two QKD protocols, such as, BB84 and DPS in ideal case.
2. This Project work implemented bit flip and depolarization in qiskit followed by simulation in QASM, using qiskit runtime on IBM cloud.
3. Next, this Project work also implemented bit flip and depolarization and executed the simulation in CPU based simulator QSim through proper job submission in quantum computing workbench [IISC Bangalore and IIT Roorkee].
4. This Project implemented following cases in QASM and QSim for BB84 and DPS respectively:
   A. **Case Study -I:** Simulation of Ideal QKD Protocols
   B. **Case Study -II:** Simulation of QKD Protocols with *10% Bit Flip noise*
   C. **Case Study -III:** Simulation of QKD Protocols with *70% Depolarization noise*

File Names for Proposed Implemented Case Studies:

A. **Case Study -I:** Simulation of Ideal QKD Protocols

Coding for Ideal case and specific Noise case is done together.

B. **Case Study -II:** Simulation of QKD Protocols with *10% Bit Flip noise*

Sl. No.	Sub Case Titles	Program Name	JobID
1.	Coding for BB84 with 3 Qubits and 10% Bit Flip Noise in QASM	QASM-3 Qubit-Bit Flip-DM.ipynb	Not Applicable
2.	Coding for BB84 with 3 Qubits and 10% Bit Flip Noise in QSim	QSim-3 Qubit-Bit Flip.ipynb	86232 – Param Utkarsh
3.	Coding for BB84 with 5 Qubits and 10% Bit Flip Noise in QASM	QASM-5 Qubit-Bit Flip-DM.ipynb	Not Applicable
4.	Coding for BB84 with 5 Qubits and 10% Bit Flip Noise in QSim	QSim-5 Qubit-Bit Flip.ipynb	86298– Param Utkarsh
5.	Coding for DPS with 5 Qubits (3 + 2 ancilla qubits) and 10% Bit Flip Noise in QASM	QASM-DPS-Bit Flip.ipynb	Not Applicable
6.	Coding for DPS with 5 Qubits (3 + 2 ancilla qubits) and 10% Bit Flip Noise in QSim	QSim-DPS-Bit Flip.ipynb	1202079, 1202143 – Param Shakti

C. **Case Study -III:** Simulation of QKD Protocols with *70% Depolarization noise*

Sl. No.	Sub Case Titles	Program Name	JobID
1.	Coding for BB84 with 3 Qubits and 70% Depolarization Noise in QASM	QASM-3 Qubit-Depolarization-DM.ipynb	Not Applicable
2.	Coding for BB84 with 3 Qubits and 70% Depolarization Noise in QSim	QSim-3 Qubit- Depolarization.ipynb	86122 – Param Utkarsh
3.	Coding for BB84 with 5 Qubits and 70% Depolarization Noise in QASM	QASM-5 Qubit-Depolarization -DM.ipynb	Not Applicable
4.	Coding for BB84 with 5 Qubits and 70% Depolarization Noise in QSim	QSim-5 Qubit- Depolarization.ipynb	86169 – Param Utkarsh
5.	Coding for DPS with 5 Qubits (3 + 2 ancilla qubits) and 70% Depolarization Noise in QASM	QASM-DPS-Depolarization.ipynb	Not Applicable
6.	Coding for DPS with 5 Qubits (3 + 2 ancilla qubits) and 70% Depolarization Noise in QSim	QSim-DPS- Depolarization.ipynb	1202193 – Param Shakti

This project presents BB84 and DPS QKD protocols in the following:

BB84 Protocol

In 1984, Charles Bennett and Gilles Brassard invented the first quantum cryptography protocol, BB84 [**Error! Reference source not found.**, **Error! Reference source not found.**]. In this protocol, Alice can send a random secret key to Bob where the secret key is encoded in their polarization. Alice encodes the classical bits in qubit states by randomly choosing between two bases, for example, the perpendicular (z) and diagonal (x) bases, as represented in Figure 3.1. The no-cloning theorem ensures that Eve, eavesdropper, cannot measure these photons and send them to Bob without changing the photon's state in a detectable way. The proposed fact is true, considering that there is no error on the quantum channel. If the quantum channel is prone to error, Alice and Bob will never be able to detect Eve's presence all the time.

Algorithm

BB84 protocol is explained in two different phases. Phase 1, *Transmission*, elaborates the steps of detailed communication over quantum channel, while detailed communication over classical channel is explained in phase 2, *Negotiation*. Table 3.1 represents exemplary bits and basis during the communication among Alice and Bob.

Phase 1: Steps related to communication over a Quantum channel among Alice and Bob are mentioned in the following:

Step I: Alice selects a string of bits and a string of bases (rectilinear or diagonal) of the same length.

Step II: Alice sends a photon for each bit corresponding to the polarization through an optical fiber.

Step III: For each photon,

Bob randomly chooses a basis to measure its polarization.

For a particular photon,

if Bob selects the same basis as Alice,

then he will find the correct bit sent by Alice.

else, if Bob is unable to guess it correctly,

then he will get a random bit.

Phase 2: Steps related to communication over a Classical channel among Alice and Bob are mentioned in the following:

Step I: Bob tells Alice about the bases he used to measure each photon.

Step II: Alice informs Bob about the bases he guessed correctly.

Step III: Alice and Bob decide to remove the bits that were encoded and measured with different bases.

Step IV: Alice and Bob have an identical bit-string, namely, the *shifted key*.

DPS QKD Protocol

QKD provides security to communicated message using quantum cryptography. It is mandatory to have an encoding key, encoding algorithm and communication channel for message communication distant apart. In 2002, Inoue et al proposed a novel cryptography scheme, Differential phase shift (DPS) QKD protocol [28, 29]. In this scheme, Alice sent three pulses of photon to Bob, while photon is divided using beam splitter. Next, Alice passed these pulses through phase modulator to create different phases for each photon. So, phase modulator assigns either 0 or π phases to the pulses. Hence, the message carries bit information with different phases. Bob measures the information using two different set of detectors: detector 1 detects bit 0 while detector 1 detects bit 1. Application of DPS QKD is mostly for fibre transmission system and compare to BB84, efficiency of secret key is higher in this system.

Algorithm

In differential phase shift quantum key distribution protocol, phases of the photon are considered for encoding the bit values. This protocol uses 3 qubits and secret key is generated using the phase differences between these 3 qubits and timestamp of Bob received by Alice. It is importantly observed that experimental results are not affected with this phase difference.

Assumptions:

i. Communication channel between Alice and Bob is supposed to be lossless, such that no information will not be lost.
ii. Two ancillary qubits are considered measurement at Bob's side using entanglement
iii. Bob uses two detectors to detect different phases. Initially, detector 1 measures bit 0 and detector 2 measures bit 1.
iv. In case of simulation, timestamp of Bob and delay to reach the qubits at Bob are considered for final generation of secret key by Alice.

Steps:

Step I: Alice divides a single photon into three paths and recombines them using beam splitters. Probabilities of photon passing through each path are equal.

Step II: Photon passes through a phase modulator (PM) to create three phases a, b and c as pulse.

Step III: The produced three different phases with time pulse delay T are sent to Bob through lossless channel.

Step IV: Bob measures the differential phases of coming pulses with same time delay T.

Step V: Bob uses two detectors: detector 1 clicks if no phase difference and detector 2 clicks if phase difference is π.

Step VI: Bob notes the time for detector clicks and measures the bit values. Consequently, detector 1 detects bit 0 and detector 1 detects bit 1.

Step VII: Bob shares the timestamp with Alice.

Step VIII: Alice creates the key similar to Bob with his timestamps and her own phase modulation.