iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50574

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Implementation of Quantum Key Distribution Algorithm in Real Time IBM Quantum Computers

Arvind Balakumar[1], Harish Nandakumar[2], Asst Prof.Mrs.V.Bhuvaneswari[3]
[1, 2, 3]*B.Tech-Electronics and Communication Engineering, Specialization in Bio Medical Engineering SRM Institute of Science and Technology Vadapalani, Chennai, India*

Abstract: ***We are Currently in the NISQ(noisy intermediate scale quantum) era. Current Quantum computers have a high noise error rate. With the increasing number of qubits every year we can develop fault tolerant quantum systems which have immense power to change our current computing power. Current quantum systems have shown to have the potential to break the classical RSA algorithm using shors algorithm. With more development and increase in number of qubits available it could easily break the current security systems of our computing. In future we could transmit data safely using the same quantum principles in the post quantum cryptography era. Quantum key distribution could be the future protocol used to transfer our secure information without getting hacked even by using quantum computing and break other quantum principles like shors algorithm which can break current encryption techniques like the RSA algorithms. We need to develop Quantum network infrastructure so we can implement the quantum key distribution algorithm in the future to enable secure transmission of data.***
Keywords: Quantum computing, Quantum algorithms, Quantum information, Quantum network, Quantum Cryptography

I. INTRODUCTION

Quantum computing is the inter disciplinary field of computing which combines classical computing and quantum mechanical properties. There are many types of quantum computing which is superconductor type quantum computing, trapped ion quantum computing , quantum computing using optical properties and Topological qubits. In this research project we will be using IBM's superconducting qubits technology to perform quantum key distribution. qubits are the basics element for quantum computing qubit(Quantum Bit) is analogous for a classical bit while a classical bit have a discrete value of 0 or 1 the quantum bit-qubit could take value of 0, 1 or any value of a superposition between 0 and 1. There three main properties for quantum computing which is Superposition, Entanglement and measurement. We would be using all of the quantum computing properties in the project. We will use superposition in the form of hardmard gate which will help to put our qubits into superposition, we will use the measurement property to measure our qubit when in the superposition state and we will use the entanglement property for transmission of out qubits. In the future with the help in the development of superdense coding technique we would be able to transmit many number of qubit which could match the number of bits transmitted using classical computing.

We will be using IBM quantum lab to access their real quantum computer to implement the quantum key distribution algorithm. IBM quantum labs is a cloud based Quantum service delivery system. We can access their quantum simulator like QASM simulator which will help us to run our algorithm and circuit and get immediate results which simulates and matches towards the results which we would get if we are running the software or circuit in real quantum computers. We can also access their real quantum computers like IBMQ Manila and IBMQ_lima. The following quantum computer are 5 qubit quantum computers. We will access IBM quantum computers which uses the superdense conductor technology to build their quantum computers. In this technique the quantum processors' from IBM will be placed under a dilution refrigerator which help to cool down the temperature very low so the superdense property will allow the quantum processor to work. Microwave pulses will be used to send as a signal to the processor to excite the qubits and perform a certain function for example a x gate pulse which will inverts the state of a qubit from 0 state to 1 state . We need good knowledge of microwave engineering and know about the microwave pulses for all our gates which we have used in our circuit to implement our software or circuit in real IBM quantum computers.

In this project we have also used qiskit metal package which is a design tool and an open source software available to develop, design and analyse transmon qubits. Transmon qubit are qubit associated with superconductors and transmon physics property. We designed a 5 qubit quantum chipset to show to size and features of real quantum computer processor.

The primary objective of this project is to implement quantum key distribution a quantum cryptography and quantum network algorithm in real quantum systems like IBM_lima . Quantum cryptography will be one the most import area in our life time after the quantum era.

©IJRASET: All Rights are Reserved

With powerful quantum computers hackers can easily break through any of encrypted data with any technologies build using classical computing technologies. The project also shows import of developing data security systems after the post quantum cryptography era where even quantum computers can hacked using the quantum cryptography principles. The main disadvantage of current quantum cryptography technologies and even quantum key distribution is the lack of infrastructure. We need to create new quantum networks with quantum channels which connect a long distance. Developing quantum channels between cites which have a long distance will be a huge task and also very expensive but after the infrastructure is build the quantum networks will be very secure than current cyber security technologies.

II. PROBLEM STATEMENT

In classical computer networks in the field of security and data transmission we use data encryption techniques. The main idea of an encryption techniques is that to change the text or data into unreadable form or into an encrypted state using a key and transmit the key to the receiver even when someone tries to hacks this encrypted data they cannot extract the information as it is in a encrypted state. This process sounds good but if the hackers hacked even the key they could decrypt the data and extract the information.

For this drawback or problem many algorithm have been developed to distribute the key. In the project we will distribute the key securely over a quantum channel using the quantum key distribution algorithm by implementing the algorithm in real time quantum systems from IBM using IBM quantum labs and also design a 5 qubit quantum chipset using qiskit metal.

III. METHDOLOGY

In this research paper we have implemented the Quantum Key Distribution Algorithm which is also an Quantum Cryptography Algorithm in IBM Quantum labs. We have implemented the algorithm using an simulator from IBM the QASM simulator and also we have implemented the program in real time quantum systems like lima and manila. We use qiskit which is a program language and a package which is available in python which is used to write quantum algorithms design quantum circuits , simulate the quantum algorithms or circuit and also access the real quantum systems by linking the program with IBM quantum labs.

IV. BACKGROUND

A. Need for Quantum Computing

We all use computers and digital systems which require transistor for its functioning. Transistors are used for the computation purpose in our computing. Over the years the size of transistor which we use is constantly being reduced which increase our computing power. By reducing the size of transistor we can have more number of transistor in the area which will directly increase our computing power. But recently the size of our transistors are reducing very small that electron tunnel effect could take place soon.

The tunnel effect which will happen when we the reduce size of our transistor very small that electrons can pass through the transistor walls. Also when we are working with transistors at such small scale quantum effects will also come in place. To handle all the problem and further develop our computation speed and power we need to develop quantum computing which deals with the quantum effect and principles. Quantum computing is developed based on the principles of quantum mechanics so that we will not get the problems like tunnel effect which we may encounter with classical computing.

B. Qubits

Qubits is the analogous of the classical bit. The classical bit can take any discrete value of either 0 or 1 which is similar to on or off similar in transistor. The quantum bit qubit takes the value of 0 ,1 or any value between 0 or 1 which is the superposition of the state of 0 or 1. This property of quantum bit allows it to store more information in one single qubit and transmit more amount of data per bit when compared to a classical bit. Super dense coding is the field of research with in quantum computing which deals with qubits and increasing the number of data which we can transmit. The physical representation of a qubit is usually made by visualization of a bloch sphere which contain all the state 0 and 1 and also the rotation in plus and minus state. We can think about a qubit physically as a photon , which is a example of a real qubit. Ions and superconductors are also an example of physical qubits as we can see the quantum property being experienced by the ion or atoms.

C. Quantum Computer Noise

Currently we are in the noisy intermediate scale quantum system(NISQ) era of quantum computing. In the NISQ era of quantum computing we have fault tolerant quantum systems which have errors and higher run times.

Current quantum systems have high coherence time which means that the time which a qubit or quantum bit is alive and perform computation is very low and performs at a slow time rate in the rate of milliseconds which means quantum systems now take more time than classical computers and quantum supremacy has still now have not been achieved. To solve the quantum error we have developed many quantum noise correction algorithm. The quantum error correction algorithm needs more logical qubits and with increase of number of qubits the computation power will increase and the noise will also decrease drastically. Lets take an example of linear search algorithm in which the complexity of the algorithm is N or the number of elements is the run time. The quantum analogous of the linear search algorithm in quantum which is quantum search algorithm have a complexity of root N which means the quantum algorithm takes very less time to perform drastically when compared to classical algorithm. Currently IBM has osprey quantum system which has the highest number of qubits which is 433. We need at least 1000 qubits system to perform computation which is faster than classical counterpart. Currently with operation which have low number of data which needs to be processed classical computing is best while if the number of data is more quantum computing performs the operation more faster exponentially when compared to quantum computing

D. Superpostion

Superposition is one of the fundamental properties of quantum mechanics and quantum computing. Generally superposition is a combination of many state in the case of quantum computing and our paper quantum superposition takes place between the 0 state and 1 state. We can understand superposition by the example of a thought experiment. Lets take example of a cat in a box with radioactive poison inside the box open. We know that after opening the box if the cat is alive or dead but before opening the box we don't know the state of the cat it can either be dead or alive superposition can be thought as the state which is before we open the box the cat could be dead or alive which is a combination of the state . Superposition is a quantum property by using this property in quantum computing we can induce the qubits state of 0 and 1 in a superposition where it's a combination of both the 0 and 1 state

E. Measurement

Measurement is also an important property for quantum computing. If an object or qubits are in superposition and if we measure the qubits the state will change. Lets take an example of a qubit in superposition of the 0 and 1 state and if we measure the qubit it state will collapse into either the 0 state or the 1 state which is a weird property of measurement. The dual property of light is also an example of this measurement property in real life. If we pass lazer through a hole it will hit the screen at random position but if we don't observe the lazer and the particle hit the screen it will form a pattern which indicates the particle has wave property.

F. Quantum Gates

In the project we have mainly used two different quantum gates. Quantum Gates are similar to classical gates but quantum gates can only be used to build quantum circuits and the quantum gates work on quantum property. In the project we have used the Hardmard gate and the X gate. The Hardmard gate is responsible of the superposition property in our quantum ciruit. With the help of the Hardmard gate only we could implement the superposition property. The main function of the hardmard gate is that it change the state of the qubit from 0 state to the plus state or vise versa and it changes the state of qubit form the 1 state to the minus state or the vise versa. The X gate rotates the qubits 180 degree if the qubit is initially in the 0 state it will change it to the 1 state and if the qubit is initially at the 1 state it will change it to the 0 state. The x gate can be thought as an analogous the classical not gate

G. Quantum Key Distribution Algorithm

The quantum key distribution can thought as a network transmission algorithm. The main target of quantum key distribution algorithm is to securely transmit a key from the sender to receiver through a quantum channel securely.

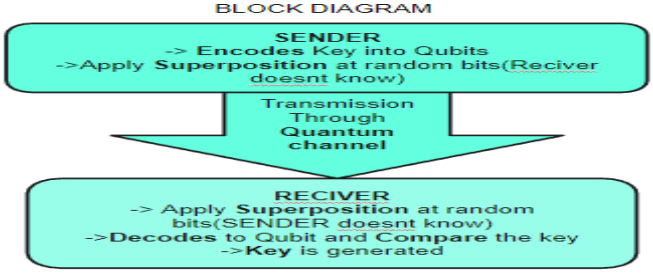


Figure 1

1) Sender

The sender is the first block in the quantum distribution algorithm. In this phase the sender identifies the key which has to transmitted to the sender based on the size of the key the number of qubits required for the transmission is identified . Once the total number of qubits required is identified we encode the classical key in the qubits.

The sender identifies and applies superposition at random at the qubits. The main idea is that the receiver doesn't know which qubits the sender applied superposition. By applying superposition the sender will change the encoded qubits into the plus state or minus state which will change when the receivers' measures the encoded qubits.

2) Transmission Channel

This is the block which contains the transmission channel where the sender send the encoded qubits through the quantum channel. The quantum channel could be any channel which can carry the physical qubits for example optical fibre can also be an quantum channel if the qubits and quantum system is build by optical system. Hackers or eavesdropper usually hack the transmission channel but using this algorithm if the hackers get through the transmission channel they cannot copy the qubits as qubits cannot be cloned and if they measure the qubits it will change the initial state sent by the sender and it will not match with sender and receiver this is the main advantage of the quantum key distribution algorithm.

3) Receiver

In the receiver block the receiver decodes the qubits and the receiver also applies superposition at the random bit and then the receiver and sender compare the bits which have same state that is either superposition or no superposition. If the compared key between sender and receiver is not same it can be said that the qubits have been hacked and if the keys are same the compared bits are used as the new key

V. IMPLEMENTATION

The quantum key distribution algorithm has been implemented in two real time IBM quantum computers which is IBM_Manila and IBM_lima. The real IBM quantum computer can been accessed using IBM quantum labs.

A. IBM Manila

We have implemented the quantum key distribution algorithm in IBM_MANILA and the time taken to process each qubits is noted down which is represented in the table below

Table 1

Quantum Computer	NO OF SHOTS	TIME TAKEN
IBM_MANILA	1	6.21
	1	5.12
	1	5.31
	1	6.53
	1	6.20
	TOTAL TIME TAKEN	29.37

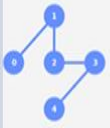
B. IBM Lima

We have implemented the quantum key distribution algorithm in IBM_LIMA and the time taken to process each qubits is noted down which is represented in the table below

Quantum Computer	NO OF SHOTS	TIME TAKEN
IBM_LIMA	1	1.19
	1	1.19
	1	0.59
	1	1.92
	1	1.19
	TOTAL TIME TAKEN	6.08

C. Comparision

We compare The features of the two quantum computer in which we have implemented the quantum key distribution algorithm. We compare various features like the time taken to complete the process, error rate, frequency, and coherence time.

S.NO	QUANTUM COMPUTER	TOPOLOGY	NO: SHOTS	COHERENCE	FREQUENCY	ERROR	TIME TAKEN
1	IBMQ MANILA		1	198.486584 us	4.970698 GHZ	0.02182	29.37
2	IBMQ lima		1	74.777978 us	5.15989 GHZ	0.02824	6.08

It is found that the IBM_lima quantum computer performs better than IBM_Manila and has a lesser timer taken and lower error rate.

VI. LITERATURE REVIEW

In a paper about quantum key distribution by Al-Mubayedh [1] he had done research about quantum cryptography on IBM QX .The paper explained the quantum key distribution algorithm and run it on IBM QX .In another paper on quantum cryptography done by S. Mitra, et al, [2] had done a comparison between the classical computation and the quantum computation. The comparison proved that most of the algorithms that is used by public key encryption and other encryption are not secure and can be broken by quantum computations.

The following research paper were implemented in simulators like matlab or using simulator from IBM. But in this research paper we have implemented the quantum key algorithm using real time quantum systems from IBM labs

VII. CONCLUSION

In the post quantum cryptography era all companies and institution which have not adopted for quantum cryptography and quantum systems can be easily hacked. Quantum computing and quantum cryptography algorithms like quantum key distribution have shown to have the potential to break classical computation easily and have shown to have enormous potential to break and break data which is transmitted using classical computation. Quantum Key Distribution algorithm will be very important in the future which will be used to transfer data securely using quantum channel. The main conclusion is that we need to develop the quantum network and quantum infrastructure in order to build quantum channel across very long distance to secure data and transmit the data across long distance securely in the post quantum cryptography era .

REFERENCES

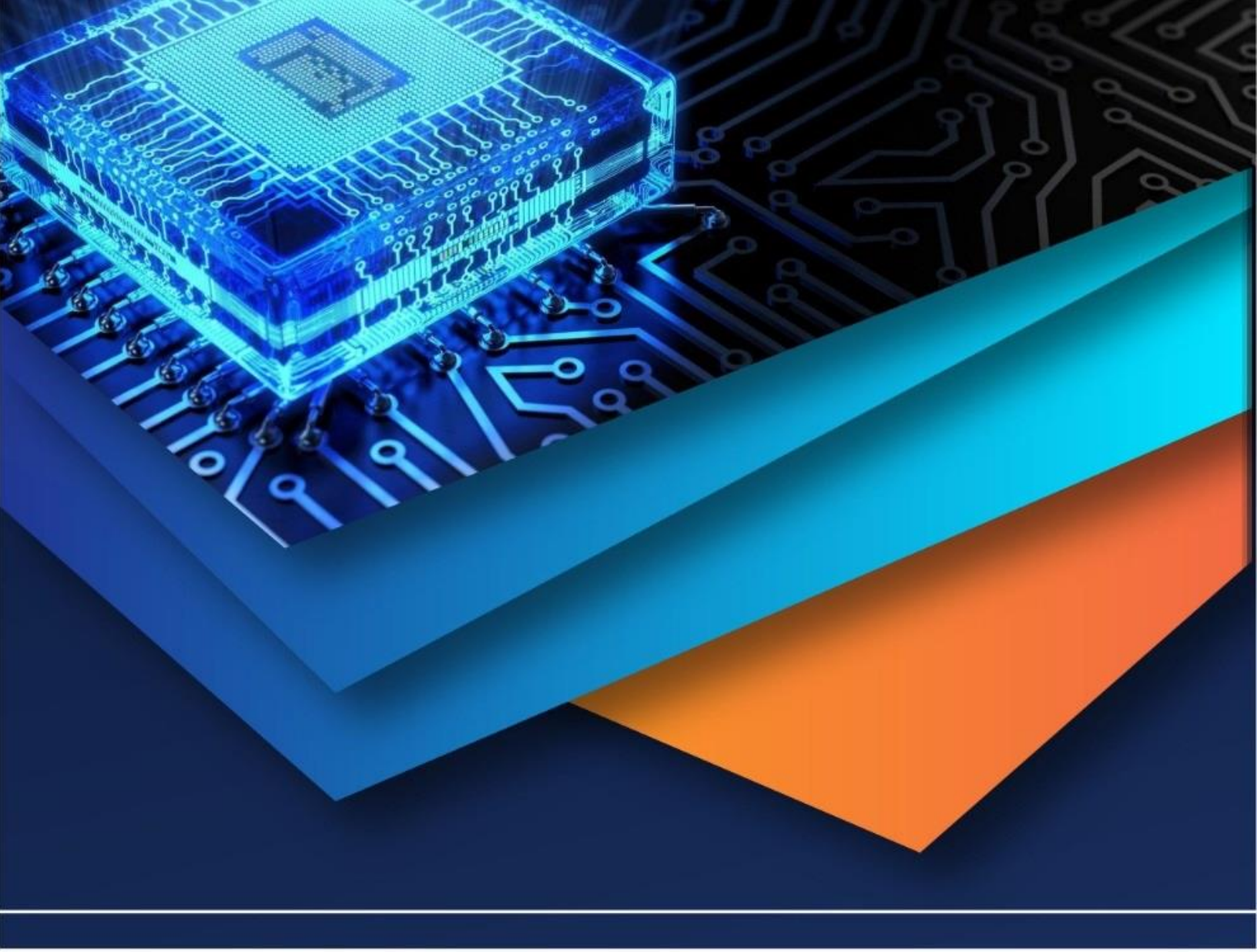
[1] D. AL-Mubayedh, M. AL-Khalis, G. AL-Azman, M. AL-Abdali, M. Al Fosail and N. Nagy, "Quantum Cryptography on IBM QX," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769567.

[2] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, “Quantum cryptography: overview, security issues and future challenges,” 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, 2017, pp. 1-7. Available:https://ieeexplore.ieee.org/document/8350006

[3] P. Kilor, P. Soni, “Quantum cryptography: realizing next generation information security,” International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2014. Available http://ijaiem.org/volume3issue2/IJAIEM-2014-02-28-090.pdf

[4] IBM Research and the IBM QX team, “User guide / frequently asked questions,” 2017. Available:https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user┐ guide/000-FAQ/000-Frequently_Asked_Questions.html

[5] IBM Research and the IBM QX team, "Introducing qubit phase," 2017. Available: https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginner s-guide&page=005-Single-Qubit_Gates~2F005-Introducing_qubit_phase



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)