RV Educational Institutions ®
RV College of Engineering ®

Autonomous Institution Affiliated to Visvesvaraya Technological University, Belagavi

Approved by AICTE, New Delhi, Accredited By NAAC, Bengaluru And NBA, New Delhi

Go, change the world

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Comparison Of Quantum Computing Algorithm Using Qiskit

MINOR PROJECT REPORT

Submitted by,

Aarush Gupta	**1RV18CS002**
Ansh Singal	**1RV18CS026**
Ayush Daga	**1RV18CS034**

Under the guidance of

Dr. Sharvani G.S

Associate Professor

Dept of CSE

RV College of Engineering

In partial fulfilment for the award of degree of

Bachelor of Engineering

in

Computer Science and Engineering

2020-2021

RV COLLEGE OF ENGINEERING®, BENGALURU-59

(Autonomous Institution Affiliated to VTU, Belagavi)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

Certified that the minor project work titled '***Comparison Of Quantum Computing Algorithm Using Qiskit'*** is carried out by **Aarush Gupta (1RV18CS002), Ansh Singal (1RV18CS026), and Ayush Daga (1RV18CS034)** who are bonafide students of RV College of Engineering, Bengaluru, in partial fulfilment for the award of degree of **Bachelor of Engineering in Computer Science and Engineering** of the Visvesvaraya Technological University, Belagavi during the year 2020-2021. It is certified that all corrections/suggestions indicated for the Internal Assessment have been incorporated in the minor project report deposited in the departmental library. The Minor Project report has been approved as it satisfies the academic requirements in respect of minor project work prescribed by the institution for the said degree.

Signature of Guide	Signature of Head of the Department	Signature of Principal
Dr. Sharvani G.S	**Dr. Ramakanth Kumar P**	**Dr.K.N.Subramanya**

External Viva

Name of Examiners	**Signature with Date**
1	
2	

RV COLLEGE OF ENGINEERING®, BENGALURU-59

(Autonomous Institution Affiliated to VTU, Belagavi)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We, Aarush Gupta, Ansh Singal, Ayush Daga students of sixth semester B.E., department of CSE, RV College of Engineering®, Bengaluru, hereby declare that the minor project titled ***'Comparison Of Quantum Computing Algorithm Using Qiskit'*** has been carried out by us and submitted in partial fulfilment for the award of degree of **Bachelor of Engineering** in **Computer Science and Engineering** during the year 2020-21.

Further we declare that the content of the report has not been submitted previously by anybody for the award of any degree or diploma to any other university. We also declare that any Intellectual Property Rights generated out of this project carried out at RVCE will be the property of RV College of Engineering, Bengaluru and we will be one of the authors of the same.

Place: Bengaluru

Date:

Name **Signature**

1. Aarush Gupta (1RV18CS002)

2. Ansh Singal (1RV18CS026)

3. Ayush Daga (1RV18CS034)

ACKNOWLEDGEMENT

We are indebted to our guide**, Dr. Sharvani G.S,** Associate Professor**, Dept of CSE** for her wholehearted support, suggestions and invaluable advice throughout our project work and also helped in the preparation of this thesis.

We also express gratitude to our Minor Project lab faculty **Dr.Azra Nasreen, Assistant Professor** and **Dr. Sandhya.S, Assistant Professor,** Department of Computer Science and Engineering for their valuable comments and suggestions.

Our sincere thanks to **Dr. Ramakanth Kumar P.**, Professor and Head, Department of Computer Science and Engineering, RVCE for his support and encouragement.

We express sincere gratitude to our beloved Principal, **Dr. K. N. Subramanya** for his appreciation towards this project work.

We thank all the **teaching staff and technical staff** of Computer Science and Engineering department, RVCE for their help.

Lastly, we take this opportunity to thank our **family** members and **friends** who provided all the backup support throughout the project work

List of figures

List of Tables

Abstract

Quantum computing is one of the most modern fields of Computer Science Research and has gained amazing traction recently due to recent development by technology Giants such as Google, Microsoft and IBM. Quantum computing uses the principles of quantum mechanics including principles such as entanglement and interference for achieving faster computation than classical methods which depend on classical bits. Quantum computing is not a new concept. The Origins of quantum computing can be traced back to 1981 at the Physics and computational conference at MIT held by MIT and IBM. since then great feats has been achieved in the field of quantum computing including quantum communications, Quantum hardware, Quantum algorithms and more recently quantum machine learning. Owing to its very short history a lot of people have not yet adopted Quantum computing fully. Therefore the main idea of this study is to demonstrate the theoretical superiority of quantum computing over classical methods.

To achieve the objective stated above a four-step approach to compare Quantum algorithms with their classical counterparts. First Quantum algorithms are found, understand their functioning and mathematics behind their operation. Next the algorithms are implemented in IBM's open source Quantum computing Framework for Python known as Qiskit. After the implementation of the algorithms analogous algorithms in the classical domain which perform similar functions are the quantum algorithm are found. The algorithms are implemented and understand their function is similar to the quantum case. Finally a few metrics determined to compare the quantum and classical algorithms and conduct a thorough comparison between the two Algorithms.

Using the approach stated above the authors could successfully compare four Major algorithms used very often in Quantum computing- Quantum support vector machine, variational Quantum eigensolver, BB84 protocol and the quantum Fourier transform. For the classical counterparts we use the support vector machine, the QR algorithm, the RSA algorithm and the fast Fourier transform. Although all of these algorithms exist in literature, there has been no such large-scale study which directly compares Quantum algorithms with their classical counterparts. The study compared the algorithms both analytically and quantitatively. The results provide adequate evidence to prove the superiority of quantum computing.

TABLE OF CONTENTS

Chapter 1 Introduction

Quantum Computing is a new and exciting field at the intersection of mathematics, computer science and physics. It concerns a utilization of quantum mechanics to improve the efficiency of computation. Here a gentle introduction to some of the algorithms in the field of quantum computing is presented. The exploration begins by motivating the central ideas , application and motivation to in these algorithms. From there the report moves on to an actual simulation of the quantum algorithm and compare them to their classical analogue Central notions of quantum algorithm along with circuit and outputs (qubits and quantum gates) are described. The project ends with a proper comparison of the quantum algorithms with their classical counterparts.

1.1 State of the art

Recently, Google reported a demonstration of quantum supremacy with its 53-qubit digital quantum computer [1][2][3], in that it beat classical machines for a specific task. But quantum computers have yet to show a clear advantage in tackling practical problems, such as simulating quantum systems. Are current commercial quantum computers with tens of qubits ready to run useful quantum simulations? Not yet. Writing in npj Quantum Information Adam Smith and colleagues report on a textbook example of a condensed matter system simulated on the IBM 20-qubit quantum computer. Smith et al. investigated the far-from- equilibrium dynamics of 1D spin-1/2 chains that underlie interesting physics from quantum magnetism to many-body localization. The unitary time evolution of the system is broken down into elementary operations that are the building blocks (one- and two-qubit gates) of quantum computation. An initial state is prepared, then evolved to the final state through the series of operations. From the final state quantities such as the magnetization are extracted and compared with numerical results obtained with a classical computer. The results of this digital quantum simulation show low quantitative accuracy, because the error rates quantum computers are still large. On the bright side, they do qualitatively reproduce the physics. Smith and co-workers conclude that, for this type of problem, quantum simulation still “requires an order of magnitude improvement in fidelity and coherence until it will realistically outperform classical computers”. Thus, dealing with errors is at the top of the agenda.

1.2 Motivation

Quantum mechanics is one of the leading scientific theories describing the rules that

govern the universe. It's discovery and formulation was one of the most important revolutions in the history of mankind. The really interesting motivation is how the quantum computing model compares to classical computing. Most people believe it is strictly stronger in terms of efficiency. And so the murky depths of the quantum swamp must be hiding some fascinating algorithmic ideas. One want to understand those ideas, and explain them up to our own standards of mathematical rigor and lucidity. To draw a difference between the storage and time complexity between the algorithm and its analogue. One more reason the authors want to do is to explore and show the applications of these algorithms in the real world and to learn the mathematical models and logics behind each algorithm.

1.3 Problem Statement

To implement quantum algorithms using QISKIT and establishing a comparative study between the Quantum algorithms and their classical counterparts

1.4 Objectives

- Implementation of quantum algorithms using Qiskit.
- Comparison of quantum algorithms with their classical counterparts.
- Defining metrics for accurate comparison between classical and quantum algorithms.
- Demonstrating theoretical quantum advantage.

1.5 Methodology

- Studying the quantum algorithms theoretically and design a circuit using quantum gates on paper.
- Build the circuit using QISKIT library
- Check the output of the algorithm using QASM simulator with 1024 shots
- Run algorithms on IBMQ's Quantum Systems by queuing the job and getting relevant outputs.
- Compare the outputs of QASM simulator and actual quantum computer
- Using the above procedure as an umbrella methodology for all quantum algorithms, study and execute the quantum algorithms.
- Find appropriate input data for comparing the classical and quantum algorithms to do a comparative study.
- Establish theoretical quantum advantage of the quantum algorithm

1.6 Summary

To summarize, there have been significant and interesting developments in the Quantum Computing technology that have made the researchers in several fields including mathematics, computer science and physics turn their heads. Everyone is looking at Quantum computing to solve the problems that have remained unsolved. The limitations of Classical Computing technology have now been known for long. This gives rise to the comparisons between the two and how efficient and practical can Quantum computing be and what are the aspects where Classical Computing still has the upper hand overall.

This leads to the problem statement where the authors intend to do a comparative study between the two types of computing by implementing the quantum algorithms on QISKIT. The primary objective here is to identify the quantum advantage and define corresponding metrics to identify the accurate comparisons between the quantum and classical algorithms.

Chapter 2 Literature Survey

2.1 Introduction

A literature survey is the synthesis of the available literature regarding the research topic. This synthesis merges the conclusions of many different sources to explain the overall understanding of the topic, thus laying a foundation for both the research question and primary research. Although a literature survey will cite sources and should discuss the credibility of the sources included, it is more than an annotated bibliography. The literature survey needs to review all the significant sources on a topic, regardless of whether or not they support the claims the study will eventually be working toward. A literature survey is a comprehensive summary of previous research on a topic. The literature review surveys scholarly articles, books, and other sources relevant to a particular area of research. The review should enumerate, describe, summarize, objectively evaluate and clarify this previous research.

2.2 Related Work

The authors explored several papers pertaining to our topic. From those papers the authors concluded the following points.

From paper 1 titled "A variational eigenvalue solver on a quantum processor" [4] by author Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, X Q Zhou, P J. Love, A Aspuru-Guzik, Jeremy L. The objectives of this paper was to demonstrate an alternative approach that greatly reduces the requirements for coherent evolution and combine this method with a new approach to state preparation based on ansatze and classical optimization. The results which were obtained from this paper was that the paper was a seminal paper and one of the cornerstones on which all of Quantum Chemistry is based. This method does away with the requirement of having a fully coherent evolution of using QPE for finding eigenvalues of given eigenvectors. The limitations of this paper was that VQE requires a lot of n-qubit controlled operations which is very costly in terms of gate fidelity while implementing the algorithm on actual hardware. Also, no comparison with classical methods has been offered in the paper, only its own analytical proof.

From paper 2 titled "Quantum Computation and Quantum Information- The quantum Fourier transform" [5] by author M. Nielsen and I. Chuang. The objective of this paper was that this chapter is a pedagogical description of the Quantum Fourier transform covering the math and physics of the subject matter. The results which were obtained was that the chapter starts with QFT and later moves on to describe QPE based on QFT. It provides a mathematical

description of both algorithms and ends with their applications. The limitation was that the chapter does not dive into the classical counterparts of all the algorithms discussed in the chapter. This leaves the subject matter unfulfilled of comparing quantum and classical algorithms.

From paper 3 titled "QKD Algorithm BB84 Protocol in Qiskit" [6] by author M Ramachandra Kashyap. The objective of the paper is to implement the BB84 protocol on a quantum simulator and demonstrate the working of the secret key generation protocol on quantum simulators. The results obtained were that the paper theoretically demonstrates the capability of the algorithm to detect eavesdropping attacks using the Qubit error rate parameter. The author also infers from his findings that longer the key being shared, higher the probability that the eavesdropper can be detected. The limitation was that the paper does not talk about practical implementations or classical analogues of the algorithm. This makes it difficult to understand the quantum advantage that it brings to the table.

From paper 4 titled "The Applications and Challenges of Quantum Teleportation" [7] by author Tao Liu. The objective of this paper was that the first part of the paper talks about the theory of quantum teleportation and the applications that have been achieved in recent years. Next, the results of current experiments and the challenges that should be overcome in the future are presented. The final section discusses the development of quantum teleportation and its future implementations. The results obtained was that the paper discusses the past and present of quantum teleportation. The biggest hurdle for any quantum communication protocol is the loss in quantum information stored in the qubits (mostly photons with information stored in polarization or phase of the photons) which has traditionally been a major issue. Modern advancements such as creation of states with higher fidelity and stronger entanglement. The limitations was that its challenges in longer range teleportation have not been highlighted although it has been considered an important application of the protocol.

From paper 5 titled "Quantum Computing and Shor's algorithm" [8] by author Tristan Moore. The objective was that the The paper covers the basic aspects of the mathematical formalism of quantum mechanics in general and quantum computing in particular, underscoring the differences between quantum computing and classical computing. It culminates in a discussion of Shor's algorithm. The results obtained was that the paper theoretically and mathematically reviews quantum computing in general and shor's algorithm in particular. The author first describes basic definitions often used in quantum computing, followed by a description of Quantum Fourier transform and then moved on to describe Shor's algorithm. The limitation was Although the algorithm does touch up on classical analogues of Shor's algorithm, they are compared directly on the basis of their quantum vs classical time complexities. Such a

comparison may be vague and not accurate.

From paper 6 titled “Quantum Driven Machine Learning” [9] by author Shivani Saini, PK Khosla, Manjit Kaur & Gurmohan Singh. The objective was that the paper presents a quantum machine learning model based on the quantum support vector machine (QSVM) algorithm to solve a classification problem. The breast cancer dataset is used for the classification problem. The results obtained was that the paper presents a quantum machine learning model based on quantum support vector machine (QSVM) algorithm to solve a classification problem. The breast cancer dataset is used for the classification problem. The limitation was that the paper compares classical and quantum SVMs using classification results from running both the algorithms on the same dataset. The paper does not provide implementation details of both the algorithms used. This leads to ambiguity in how the algorithms were compared with each other

2.3 Summary

From all such informational researches, a clear understanding on the workflow of what is to be done while implementation was achieved, as the papers not only mentioned what the authors had achieved, but also specified the various techniques they had used to achieve it, the constraints they had to face while implementation and also the future developments were mentioned.

Chapter 3 Software Requirement Specifications of the Algorithms

3.1 Quantum Support Vector Machine

Quantum Support Vector Machines (QSVMs) [10][11][12], or more accurately, Quantum-enhanced SVMs can improve the training performance of support vector machines by making the process of applying the kernel filter to all the data points more efficient. Quantum computing does this using special feature maps for data encoding and to find the best configuration and dimension in which the data can be separated. SVMs typically apply the feature maps to find a higher dimension in which the data is separable. Quantum enhanced support vector machines are useful when calculating the kernel of a dataset directly is inefficient classically. The feature maps can encode large amounts of data simultaneously and thus compute the kernel function parallelly on all the data points. This speeds up the process of training by several fold, even exponentially in some cases.

3.2 Variational Quantum Eigensolver

As the name suggests, the variational quantum eigensolver [13] is used to find the eigenvalues of Hamiltonians (Hermitian matrices) for which finding the eigenvalue classically is very computationally expensive. Eigenvalue estimation is a very common problem in several applications be it computer graphics or structural design. However, the VQE cannot estimate all the eigenvalues of the Hamiltonian. It can give an upper limit of the smallest eigenvalue of the Hamiltonian. Though comparatively limited in scope, it is still a problem of great importance to estimate the smallest eigenvalue of a given Hermitian matrix, for example in finding the configuration of a protein molecule with the minimum energy. Therefore, the VQE finds great applications in quantum chemistry and occasionally in quantum machine learning.

3.3 BB84

As stated earlier, Shor's algorithm threatens the security of contemporary cryptographic methods whose security is based on the incapability of classical machines in factoring large numbers. Quantum computing provides a viable alternative to the network security problem by providing unconditional security based on quantum mechanical principles including the no cloning theorem and the Heisenberg's uncertainty principle. The umbrella technique for such quantum cryptography is called Quantum Key Distribution (QKD) [14][15]. The very first protocol to be introduced under QKD was the BB84 algorithm. Introduced by Gilles Brassard

and CharlesBennett in 1984 (hence the name BB84), it is regarded as the birth of Quantum Key Distribution and ultimately inspired several major developments in the field of quantum cryptography and communications including practical implementations of the protocols (in lab and large scale) and the formulation of several other protocols under QKD (including B92, E91, SPD, decoy, etc.)

3.4 Quantum Fourier Transform

Quantum Fourier Transform (QFT) [16][17] are quantum computing's analogue to the Fast Fourier Transform (FFT). The Fourier transform is most commonly used for energy routing problems by converting problems from the time domain into the frequency domain and vice versa where solving the problem may be easier. It also finds a lot of use in Quantum and Non-linear optics for solving complex wave equations. In the quantum case, Fourier transforms are most commonly used for the implementation of the Shor's algorithm. QFT exploits quantum interference to find the most appropriate solution to the problems and destructively filters out solutions which are not applicable to the problem.

3.5 Hardware Requirements

- CPU Requirements
  - x86 processor @ 1.6 GHz or faster
  - 4 GB ram or more
- Good Internet Connection (to access Quantum computers on the cloud, by IBM)

3.6 Software Requirements

- Ubuntu 16.04 or later / macOS 10.12.6 or later / Windows 7 or later
- Anaconda Development environment
- Python 3.6 or above
- Jupyter Notebook
- Python libraries required
  - IBM Qiskit software- Terra, Aer, Ignis, Aqua
  - Numpy
  - Matplotlib

Chapter 4 Design of the Algorithms

4.1 Algorithms

4.1.1 Quantum Support Vector Machines

Quantum Support Vector Machines or Quantum Enhanced Support vector machines aid classical machine learning by easily calculating the kernel functions which are inefficient to calculate classically. The process starts with encoding classical information to quantum information by using feature maps. There are multiple types of feature maps using different types of encodings:

1. Amplitude Encoding: the data is encoded in the amplitude if the superposition of quantum states.
2. Phase encoding: the data is encoded in the phase of qubits.

Amplitude encoding is the most commonly used encoding scheme due to the ease of manipulating amplitudes of quantum states and putting multiple states in superpositions simply by applying the Hadamard gates. That is what the study would explore next.

Data encoding is done using feature maps which take as input classical information (which has usually undergone some form of transformation to fir the parameter of the qubits modified by the data). Feature maps are often expressed using two properties:

Expressibility and entangling capability [18] of the circuits. Expressibility is the range of the Bloch sphere covered by the quantum circuit whereas entangling capability is the extent of entanglement between multiple qubits in the circuit. Both of these properties are complementary to each other, that is, a high expressibility would mean that the circuit can explore a large portion of the state space but would hurt the entangling capability, which would render the system no more powerful than a classical system. On the other hand, a highly capable circuit in terms of entanglement may not be able to explore a very large part of its state space, thereby limiting the power of the data encoding. Thus, it is essential to find the right feature map (represented as $\varphi(x)$) for the problem at hand.

Coming back to QSVMs, quantum support vector machines would be superior to the classical counterparts only when calculating the kernel function (which can be calculated using quantum circuits) is classically infeasible for the entire dataset and thus requires quantum techniques. Quantum processors can calculate kernel functions using a two-step process: data encoding and variational circuit. We have already discussed the data encoding step above. The variational circuit is the step that is optimized by the classical optimizer to find a higher dimension in which the 2 (or more) classes can be separated. A high-level diagram of the

variational architecture of QSVMs is shown in fig. 4.1.

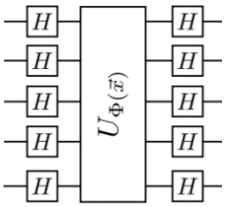


Figure 4.1 General structure of QSVMs

The Hadamard gates are used to increase the expressibility of the quantum circuit and the multi- qubit operation $U_{\varphi}(x)$ comprises of several single and multi-qubit gates to increase both the expressability and entanglement capability of the circuit. Several iterations of such a variational structure are followed by measurements which give outputs for the classical optimizer to use in optimizing the parameters. Several shots of the circuit are performed to get a good estimate of the probability distributions of the resulting quantum state and finally calculate the kernel function. Thus, the QSVM technique can be used if the kernel has a function similar to:

$$\langle \varphi(\boldsymbol{x}) | W^{\dagger}(\boldsymbol{\theta}) M_y W(\boldsymbol{\theta}) | \varphi^{\dagger}(\boldsymbol{x}) \rangle$$

where, $\varphi()$ is the feature map

W is the variational circuit

M_y is the binary measurement in the z basis

and is difficult to calculate on a classical machine.

4.1.2 Variational Quantum Eigensolver

As the name suggest, the VQE algorithm is a variational quantum algorithm which is used to find the eigenvalues of a given Hamiltonian (Square Matrix). The Hamiltonian used in VQE is limited to those which can be formed as a linear combination of multiple Pauli gates. Therefore, this limits the matrices (Hermitian) whose eigenvalues this algorithm can find. However, the VQE gives a major advantage when compared to other methods of estimating eigenvalues that VQE gives us on estimate of the smallest eigenvalues of the matrix. This has several use cases such as finding the minimum energy state configuration of quantum system such as protein molecules which are essential for drug design.

The VQE algorithm is based on the variational method of Quantum mechanics. For a given Hermitian matrix spectral decomposition state that its eigenvalues would be real where a Hermitian matrix H satisfies the following property:

$$H = H^{\dagger}$$

∴ Spectral decomposing a Hermitian matrix:

$$H = \sum_{i=1}^{N} \lambda_i \ |\varphi_i \ \times \varphi_i| \ ❶$$

Also, the expectation value of an observable H is:

$$\langle H \rangle_\psi = < \psi \ | H | \varphi > \quad ❷$$

Where $\langle H \rangle_\psi$ is the expectation value of H for the state $|\psi$

Substitute ❶ in ❷

$$\langle H \rangle_\psi = < \psi \ | (\sum_{i=1}^{N} \lambda_i \ (\varphi_i \ \times \ \varphi_i)) | \psi >$$

$$= \sum_{i=1}^{N} \lambda_i < \varphi | \varphi_i >< \varphi_i | \varphi >$$

$$\langle H \rangle_\psi = \sum_{i=1}^{N} \lambda_i \ | \ < \varphi | \varphi_i \ > |^2 \qquad ❸$$

❸ is known as the variational method in quantum mechanics. This is helpful to us because one can now query the Hamiltonian operator H with several eigenstates which would converge at

$$\lambda_{min} \text{ when } | \ \varphi \ > = | \varphi_{min} >$$

Therefore,

$$\lambda_{min} \leq \ < H >_\varphi \quad \& \quad \lambda_{min} = < H >_{\varphi_{min}}$$

Now φ is optimized to bind λ_{min} to the minimum value one can find.

So, as one can see, the VQE algorithm only gives an upper bound of the minimum eigenvalue of a given Hermitian matrix. However,

the variational nature of the algorithm suggests that the minimum eigenvalue can be estimated to an arbitrary level of accuracy using optimization techniques.

Another major point to consider is that the algorithm should be able to explore a wide range of input states to get the best chance of finding the minimum eigenvalue. However, a finite set of gates can only cover a polynomial order of input states in on exponential Hilbert space. Thus, on appropriate variational form must be used to find the minimum eigenvalue.

4.1.3 BB84

First introduced as conjugate coding where a qubit can be used to encode information and use it for cryptographic purposes. Although the original idea was for implementing quantum money, Charles Bennett and Gilles Brassard in 1984 introduced the idea of quantum cryptography where similar conjugate coding on polarization of photons was used to communicate cryptographically secure keys between 2 parties. One must note that the 1st quantum cryptographic protocol, the BB84 protocol (which is explored in this chapter) is a key growing protocol rather than a key exchange protocol since the 2 parties must already have some shared secret between them.

As stated by Bennett and Brassard in their original work on quantum cryptography, titled 'Quantum Cryptography: Public key distribution and coin tossing', the author presented an application of the conjugate coding scheme for communicating secret keys between 2 remote parties. The protocol goes as follows:

1. Alice chooses a string of random bits, subset of which would ultimately serve as the key. Also, Alice chooses a set of random bases for encoding the bits she first chose.
2. The 2 bases she chooses from are: Rectilinear (↑,→) and diagonal (↖,↗).These act as the bases of encoding of quantum information at Alice's side to send to bob. Therefore, Alice's encoding scheme is represented in table 4.1.

Table 4.1 Encodings in BB84 protocol

Bit	Base	Quantum State
0	0	|0>
0	1	|+>
1	0	|1>
1	1	|->

NOTE: In the original paper, Bennett and Brassard suggested using polarization of single photons for creating these States. Other means of encoding quantum information for communication have been explored in other works such as the phase encoding. One of the most a prominent phase encoded protocol, the B92 protocol, uses interferometers at 2 ends to enable shifting and measurements. Phase encoded quantum states are more appropriate for use in commercial optical fibres since in optical fibres is tough to maintain polarization of photons, while maintaining phase is much easier.

3. Alice encodes these states in the polarization of photons and transmit the photons to bob through a quantum channel.
4. Bob receives the photons, however, is still unaware of true basis in which photon was encoded. So, Bob simply chooses a random basis (for measurement) from the rectilinear or diagonal bases. This gives Bob a measurement result.
5. Now, Alice has a set of bits which she transmitted, and Bob has a set of bits which he measured; however, the bits would be the same at both ends only when both Alice &bob choose the same basis of encoding and measurement.
6. Sifting: Alice & Bob both communicate the bases of encoding and measurement respectively over an insecure classical channel. (This is the part where Alice &Bob must have a shared secret

between them, since they need to authenticate the classical messages from either side).The bits for which the bases match are used as the key bits and all the other bits are discarded.

The algorithm at a glance is shown in table 4.2.

Table 4.2 BB84 Algorithm

Alice Bits	1	0	1	0	0	0	1	0
Alice Bases	1	1	0	0	0	1	1	0
Alice Photons	1->	1+>	1I>	10>	10>	1+>	1->	10>
QUANTUM CHANNEL								
Bob Bases	0	1	1	0	1	1	1	1
Bob Bits	0	0	1	0	1	0	1	0
Shifted Bits[Key]	X	0	X	0	X	0	1	X

4.1.4 Quantum Fourier Transform

The Fourier Transform, as expressed in the classical sense is shown using the equation below.

$$y_k \equiv \sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} x_j \mathrm{e}^{2\pi \mathrm{i} jk/N}$$

The Quantum Fourier Transform also has a very similar form:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} jk/N} |k\rangle$$

Therefore, the algorithm (in essence) perfrorms the follwoing transormation:

$$\sum_{k=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

which, implies that the transformation had an effect of changing the basis of the quantum state. Basic Linear algebra can be used to prove that the above equation is equivalent to:

$$|j_1, \cdots j_n\rangle \rightarrow \frac{\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0 \cdot j_n}|1\rangle\right)\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0 \cdot j_{n-1} j_n}|1\rangle\right) \ldots \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0 \cdot j_1 \ldots j_{n-1} j_n}|1\rangle\right)}{2^{n/2}}$$

which can very easily be represented as a quantum circuit (discussed in chapter 5)

Chapter 5 Implementation of the Quantum Algorithms

5.1 Programming Language Selection

The programming language selected for the project is Python with IBM's Qiskit library. The motivation behind choosing Qiskit for implementing the algorithms are:

- Qiskit is based on the Gate model paradigm of quantum computing which is presently the most commonly used paradigm and eases the implementation of the algorithms.
- Qiskit is seamlessly connected to the IBMQ systems which allow us to execute our algorithms on actual quantum computers provided by IBM over the cloud.
- Qiskit is open-sourced which makes getting support much easier through online forums and discussions.

5.2 Platform Selection

The algorithms are implemented in Qiskit on the Jupyter notebook platform since IBM recommends Jupyter for working with Qiskit with its inline graphs and plots. Other alternatives to Jupyter notebooks and the reason for not choosing them are:

- IBM Quantum composer: The IBM Quantum Composer is a great GUI based drag and drop quantum circuit composer to implement quantum circuits. However, it does not provide the amount of functionality and freedom as Python based circuit creation can provide (using loops and if statements, etc.)

- IBM Quantum Lab: The IBM quantum lab is a cloud-based platform based on the jupyter notebook environment. Though very similar to the local installation of Jupyter lab, python and Qiskit, it needs an active internet connection to work, even for simulator executions, unlike the local version.

5.3 Implementation Details

5.3.1 Quantum Support Vector Machines

Quantum Support vector Machines, as discussed above, assist in calculating the kernel function of some functions where it is classically inefficient to do the same classically. The first step in the process is the data encoding step. The data can be encoded using feature maps [19]. A few commonly used feature maps are shown in figs. 5.1-5.3.

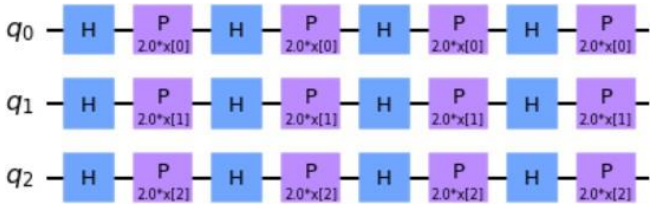


Figure 5.1 Z Feature Map in 3 qubits and 4 repetitions

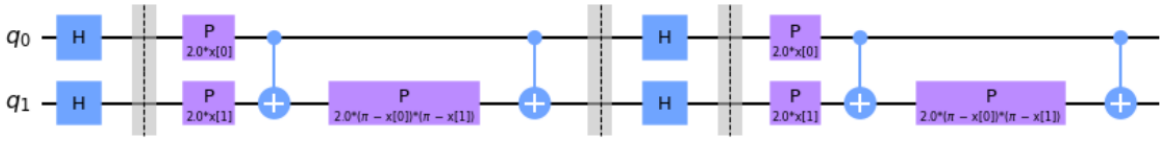


Figure 5.2 ZZ Feature map in 2 dimensions and 2 repetitions

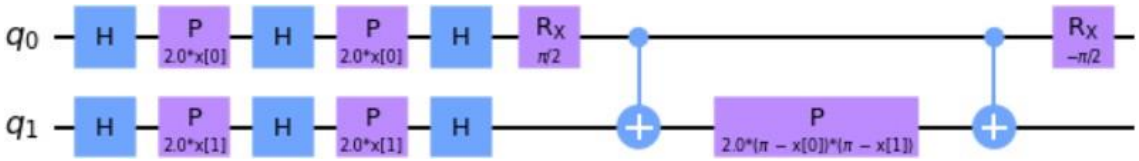


Figure 5.3 Pauli Feature map with 2 qubits and single repetition

Next, one needs the variational circuit of the algorithm which is followed by the feature map. Some of the common variational circuits are shown in figs 5.4 and 5.5.

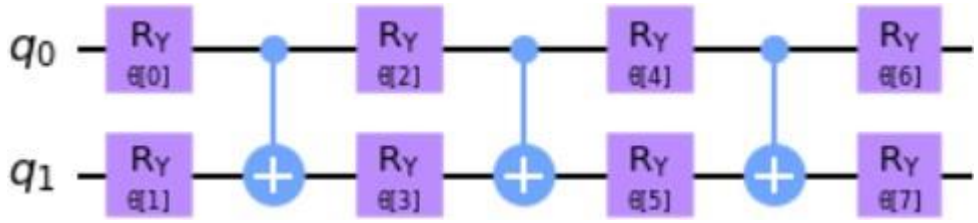


Figure 5.4 Real Amplitudes variational circuit with 2 qubits and 3 reps

Figure 5.2 EfficientSU2 variational circuit with 2 qubits and 2 repetitions

5.3.2 Variational Quantum Eigensolver

The variational quantum eigensolver also works on the variational principle of quantum mechanics, and thus its implementation also includes variational gates which can be optimized to find the configuration the minimum eigenvalue. The circuits required for finding the upper bound of the minimum eigenvalue of the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Are shown in figures 5.6.

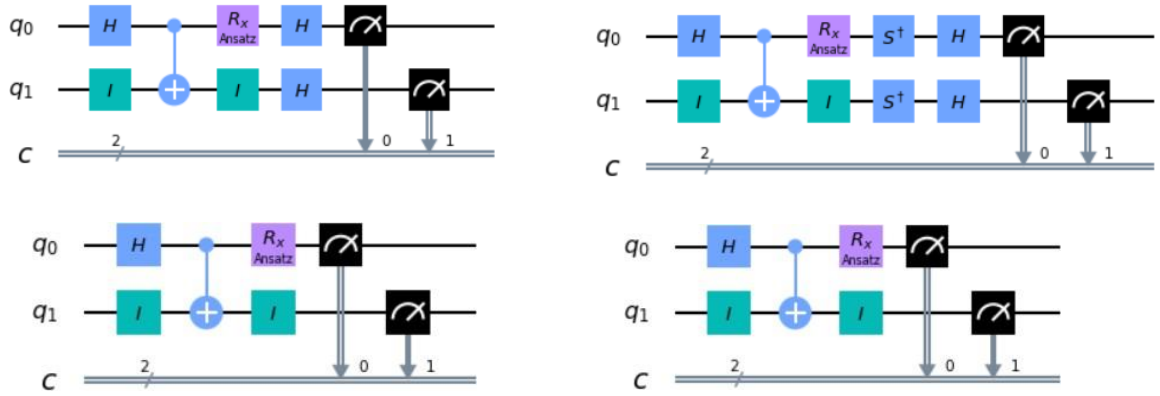
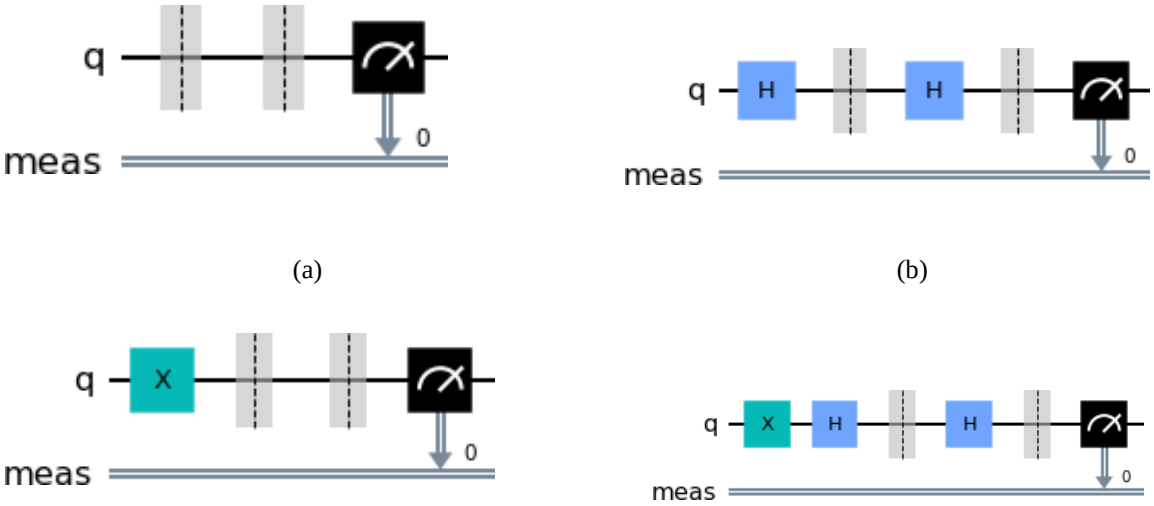


Figure 5.6 Circuits for VQE

All of these circuits represent different elements in the Puli decomposition of the Hamiltonian (given matrix).

5.3.3 BB84

The BB84 protocol is based on a stream of single qubit quantum systems communicated between 2 parties. Each of the quantum system (photon) would have the following quantum circuit representation as shown in fig. 5.7.



(a) (b)

(c) (d)

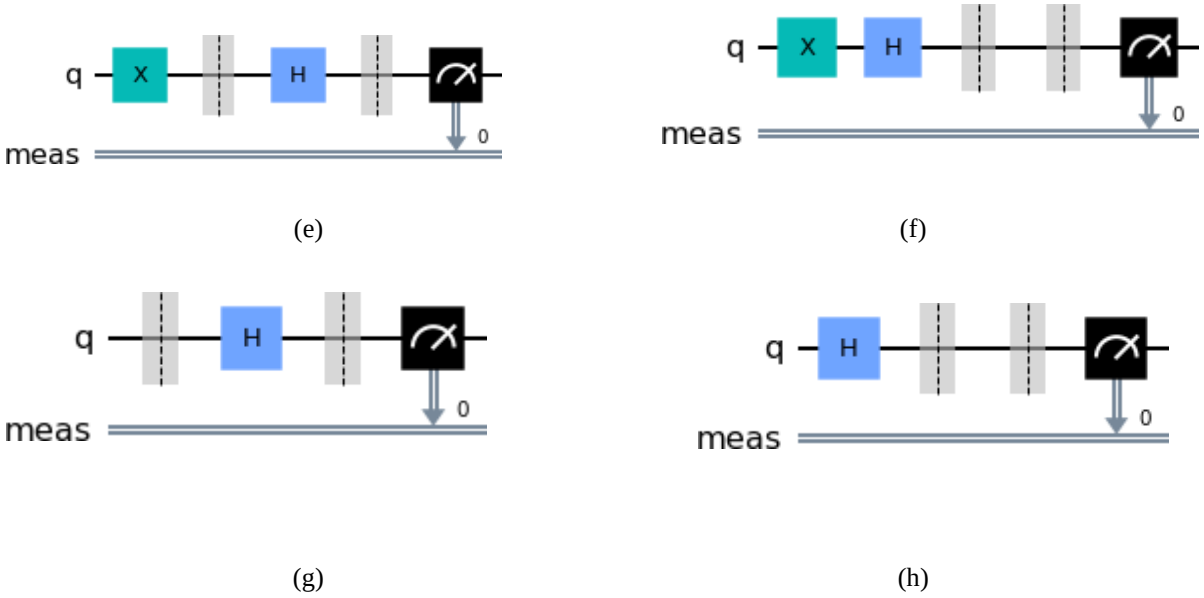


Figure 5.7 All possible quantum circuits in BB84 protocol

Circuits (a)-(d) represent outcomes where the basis of measurement and encoding chosen by Bob and Alice respectively are the same. Circuits (e)-(h) represent the circuits in which Bob and Alice chose different bases, and thus that bit would be removed during sifting.

5.3.4 Quantum Fourier Transform

The Quantum Fourier Transform is used to change bases of a given quantum state from some basis set |h> to some basis set |k>. This can be done using the following quantum circuit, implemented in Qiskit as shown in fig. 5.8.

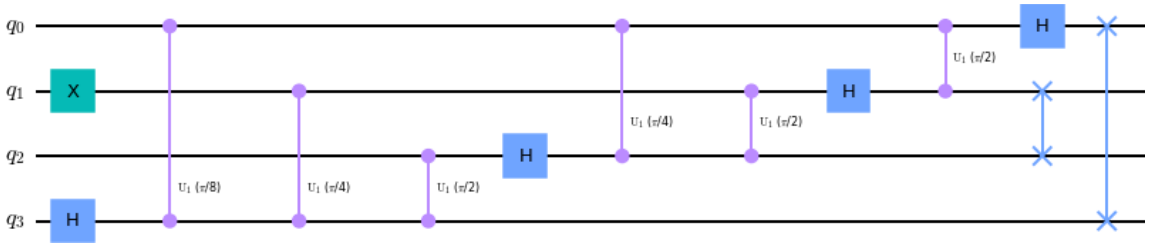


Figure 5.8 QFT Circuit

The math and logic behind the circuit has been discussed in chapter 4.

Chapter 6 Experimental Results

6.1 Results and Analysis

6.1.1 Quantum Support Vector Machines

Dataset Details

The PCA reduced Breast cancer dataset was used for the sake of this study to get a real world yet, simple dataset. The dataset is available through Qiskit as a sample dataset. A subset of the dataset is shown in fig. 6.1.

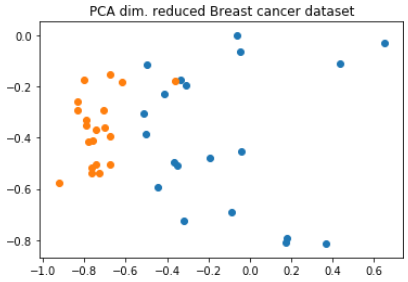


Figure 6.1 PCA reduced Breast cancer dataset

The ZZFeature map with 2 qubits and 2 reps was used to run the entire training process. After running the training process, the following Kernel matrix as shown in fig. 6.2 which represents the proximity (inner product in greater dimension) between every pair of data points.

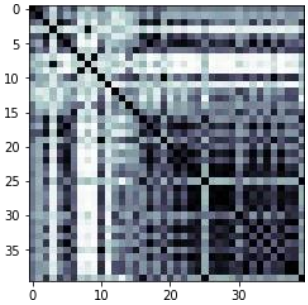


Figure 6.22 Kernel Matrix from QSVM

It can be observed from the kernel matrix above that the diagonal element are all black, which means that the distance of them with themselves is zero. The elements with white or grey entries correspond to greater distances. Also, a testing accuracy of ~0.9 on the same dataset was achieved.

6.1.2 Variational Quantum Eigensolver

VQE was run to find the minimum eigenvalue of the following Hamiltonian:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The Pauli decomposition of this Hamiltonian is:

$$\frac{1}{2}(I \otimes I + Z \otimes Z) - \frac{1}{2}(X \otimes X + Y \otimes Y)$$

where I, X, Y and Z are the Pauli matrices and $\otimes$ is the Tensor product operator. Instead of using an optimizer to scan through possible parametric angles for the circuits discussed in chapter 5, 800 angles were checked from -4π to 4π. For every angle that is sampled, the expectation value of the above decomposition is estimated by performing 100 shots of the quantum circuits as discussed in chapter 5. The final state space and final solution is represented in figure 6.3.

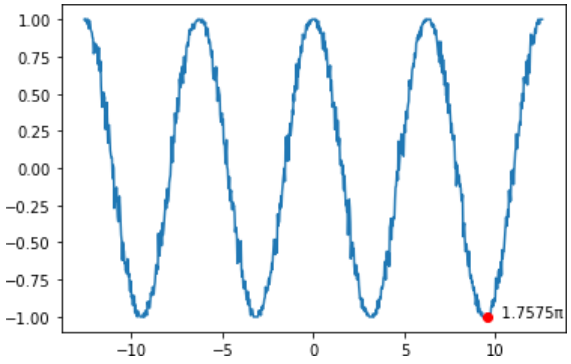


Figure 6.3 Result from VQE

Due to the cyclic nature of the bloch vector, it is observed that there are multiple solutions to the problem. Applying the solution in the equation of the expectation value of the eigenvalue of the Hamiltonian gives us a minimum eigenvalue of -1.

6.1.3 BB84

BB84 protocol was simulated in Qiskit by suing random functions in the NumPy library to generate lists of random bits and bases. Using these random bits, the quantum circuits were generated and the protocol was followed. The protocol was performed with 100 bits of key being shared between the parties, which ultimately produced 48 key bits, which is statistically accurate with theoretical considerations as shown in figure 6.4.

```
  bob_sample = [0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0]
alice_sample = [0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0]

  bob_key =  [0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0]
alice_key =  [0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0]
```

Figure 6.4 Keys generated using BB84 protocol

In the case where an eavesdropper had attacked the QKD link, the eavesdropper could be detected with a probability of 0.89 as shown in fig. 6.5.

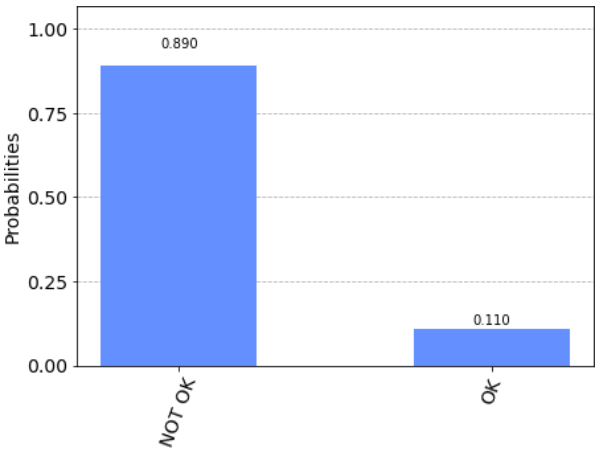
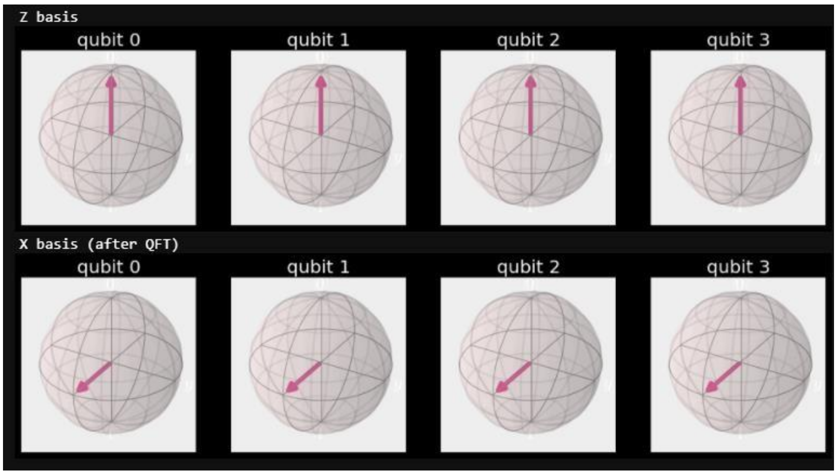


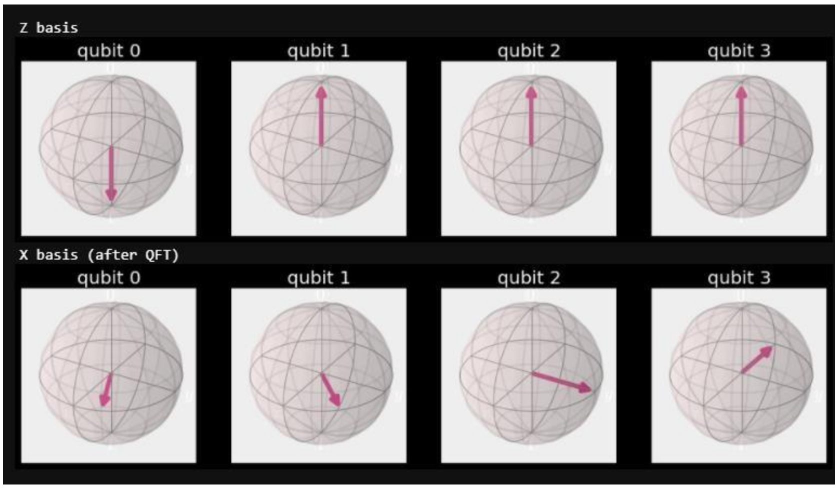
Figure 6.5 Probability of successfully detecting Eve using BB84 protocol

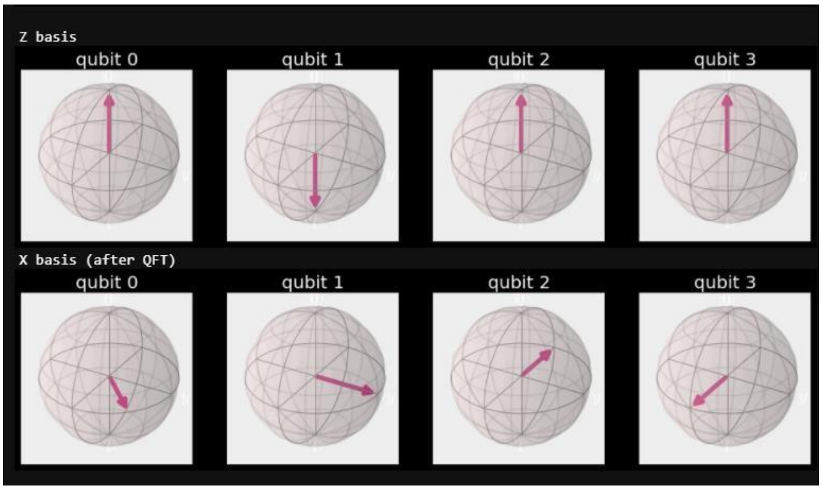
Where the NOT OK describes the case where the eavesdropping was detected.

6.1.4 Quantum Fourier Transform

QFT circuit for 4 qubits with the inputs 0000, 0001, 0010 and 0011 were run. As is visible from the image shown below, QFT changes the basis of the encoding of the quantum state from the Z to the X basis. Also, the X encoded states are encoded in their frequencies around the XY plane. So, the qubits have different frequencies of rotation (1st being the slowest and last being the fastest), as shown in fig. 6.6. This is analogous to the discrete Fourier transform as seen in the classical case where time domain functions are converted to frequency domain and vice versa. However, although this is very efficient it does not produce the same results as classical Fourier transforms, since the data cannot be readily extracted out of the circuit although the data is present in the state functions of the quantum states. QFT instead finds applications in different quantum algorithms, most prominent of which is the Shor's algorithm.


Z basis
qubit 0
qubit 1
qubit 2
qubit 3
X basis (after QFT)
qubit 0
qubit 1
qubit 2
qubit 3


Z basis
qubit 0
qubit 1
qubit 2
qubit 3
X basis (after QFT)
qubit 0
qubit 1
qubit 2
qubit 3


Z basis
qubit 0
qubit 1
qubit 2
qubit 3
X basis (after QFT)
qubit 0
qubit 1
qubit 2
qubit 3

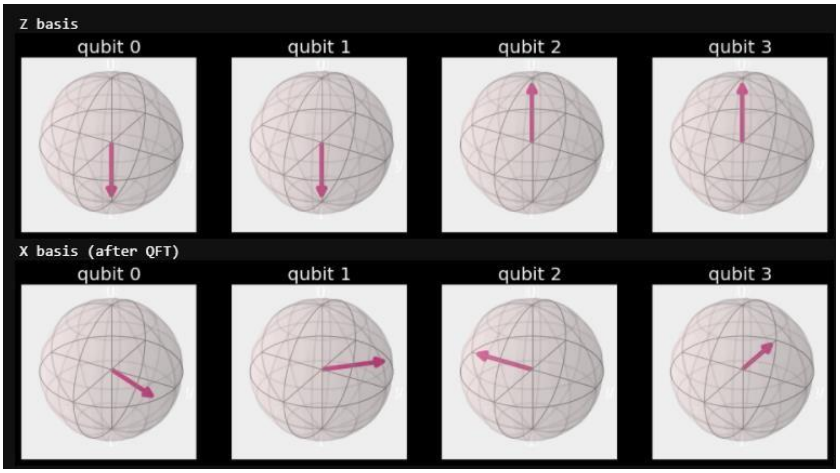


Figure 6.6 4 examples of encoding states from Z basis to X basis using QFT

6.2 Evaluation and Comparison with Classical Algorithms

6.2.1 Quantum Support Vector Machine

The main motivation behind QSVMs over classical SVMs is that QSVMs can be used in cases where the feature map is tougher to calculate classically. QSVMs can calculate certain types of feature maps much more efficiently as compared to classical methods. For example, running the same example that was run on the QSVM on a classical SVM (using the Scikit Learn SVM module), the following feature matrix as shown in fig. 6.7 was observed.

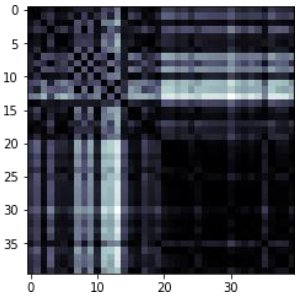


Figure 6.7 Kernel matrix obtained from classical SVM

and a testing classification accuracy of just 0.85. Therefore, the QSVM performed better in this case. It is therefore essential to understand the problem and choose a feature map accordingly to get the best performance and then make a decision between the classical and quantum counterparts.

6.2.2 Variational Quantum Eigensolver

One of the major classical alternatives to finding eigenvalues of matrices is the QR [20] or the Francis algorithm. The QR algorithm uses repeated application of the QR factorization to convert an input matrix to an upper triangular matrix with the diagonal elements being

approximately the eigenvalues of the matrix. However, the algorithm may fail if the eigenvalues are too close together. This happens due to cancellation of non-orthogonal vectors. The QR algorithm works as follows:

For the given matrix the QR factorization of the matrix is found such that

(MATLAB code)

$$[Q,R] = qr(A) \qquad ❶$$

Where A is original matrix and qr(M) is the function for finding the QR factors for the matrix M.

Now, A is reinitialized as follows:

$$A = RQ \qquad ❷$$

This can be compared with the Schur Decomposition with the following form:

$$U^{+}AU = T \rightarrow \text{Triangular Matrix}$$

Now, since A=Q.R

$$Q^{+}A = R \qquad ❸$$

Where Q is unitary.

However, R is not upper triangular, since unlike the Schur decomposition, it does not have the extra unitary multiplied after it

So, to create an upper triangular matrix, simply multiply on both sides on the right of ❸.

Therefore:

$$Q^{+}AQ = RQ$$

Thus, simply reinitializing A=RQ

where A tends towards a triangular matrix. Thus, the QR algorithm is an iterative algorithm in which 2 steps ❶ & ❷ are repeated until A is almost triangular. The final matrix would ultimately contain the eigenvalues on the diagonal.

The first and foremost point of difference between the 2 algorithm is that while QR algorithm finds all the eigen values of a given matrix, the VQE can only find on upper bound to the smallest eigen values. Although this may seem to limit the scope of usability of the VQE algorithm, (eigenvalue analysis is often used in several fields of science math and engineering where all the eigenvalues of the matrix are very useful, for example, in structural engineering) it is still very useful for very important applications such as drug design where one wants to find the protein configuration of minimum energy which would give us the most stable form of the drug. Another major difference is that although the QR algorithm is an iterative algorithm, it cannot be optimized using statistical analyses that can be used in the case of VQE which would converge faster. Theoretically, the VQE algorithm could converge to the minimum eigenvalues of the Hamiltonian matrix which the variational form could explore. However, as seen before,

there is a limitation in the space that can be explore, it is very tough to actually find the eigenvector corresponding to the minimum eigenvalue and one can only settle for an upper bound estimate of the eigenvalue. Similarly, the QR algorithm does not converge to a specific answer. However, one may stop the algorithm after it converges to some desired level of precision.

Table 6.1 lists the difference between the VQE and QR algorithm:

Table 6.1 QR vs VQE algorithms

QR	VQE
1. Finds all eigenvalues of the matrix.	1.Finds an upper bound of min eigenvalue of the matrix
2. Applicable to any matrix.	2.Applicable only on Hermitian matrices
Iterative algorithm but cannot be accelerated using statistical methods.	3.Iterative algorithms depend on optimization algorithms which find the $\|\varphi_{min} >$ of the Hamiltonian.
The QR algorithm fails in situations when eigenvalues are very close.	4.Since VQE only gives an upper-bound of the smallest eigenvalue it is invariant to other eigenvalues.
The QR algorithm has an exponential time complexity of $\theta(n.\ e^n)$ where n is the dimension of the matrix.	5.The VQE algorithm depends on optimization techniques such as gradient descent to find the minimum eigenvalue of the matrix.
Since QR algorithm is classical algorithm, it poses no such problem.	6.Due to the nature of quantum measurements, one need to perform multiple state measurements of the quantum circuit for every iteration.

6.2.3 BB84

The BB84 will be compared with its classical counterpart- the RSA algorithm. The most striking difference between the 2 algorithms is the security they provide. Although RSA is considered secure based on today's computing capabilities, it is not impossible to crack RSA. Often while carrying out security analysis of a cryptographic protocol or algorithm, one tests the protocol against a practical adversary and also against an adversary with infinite resources. Although the RSA algorithm holds up against a practical adversary (testimony to which is the wide usage of the RSA algorithm in industrial and defence purposes). the RSA algorithm quickly

falls apart against an all-powerful adversary since the adversary can simply factor the large numbers used by the communicating parties. The BB84 protocol on the other hand is impervious to such attacks since the security of the BB84 protocol is guaranteed by laws of physics and not unbased computational assumptions. Another major difference between the 2 protocols is that the while the RSA algorithm is a public key cryptographic algorithm, the BB84 protocol is a key growing protocol since they must already have a shared secret key before starting key exchange. So, one does not create a key, but grows one out of a pre-existing key.

The differences between RSA & BB84 protocols have been listed in table 6.2.

Table 6.2 RSA vs BB84 algorithms

RSA	BB84
1. Key exchange protocol	1. Key growing protocol.
Can be used to send discrete messages from A to B. Therefore, RSA cannot be used directly for stream-oriented communication	2. Produces a continuous stream of secure key bits which can be used in one time pad to enable stream-oriented protocols such as TCP
3. Security unproven	3.Provably secure(theoretically)
Does not require any additional hardware	4.Requires considerable amount of extra hardware [Alice substation, Bob substation, etc.]
Faster key exchange since all communications happen through classical channels which have much higher transmission rates.	5.Slower key exchange rates due to the noise induced in quantum channels and hardware limitations.

6.2.4 Quantum Fourier Transform

The best-known classical alternative to the quantum Fourier transform is the Fast Fourier Transform (FFT). The fast fourier transform has a time complexity of $O(n2^n)$ for 2^n elements. The Quantum Fourier transform is a much faster alternative to the FFT in that respect. However, extracting information out of a quantum circuit is not that simple. For example, consider the example considered in the implementation details of QFT with an input ‘0101’. The input and output bloch vectors are shown in fig. 6.8.

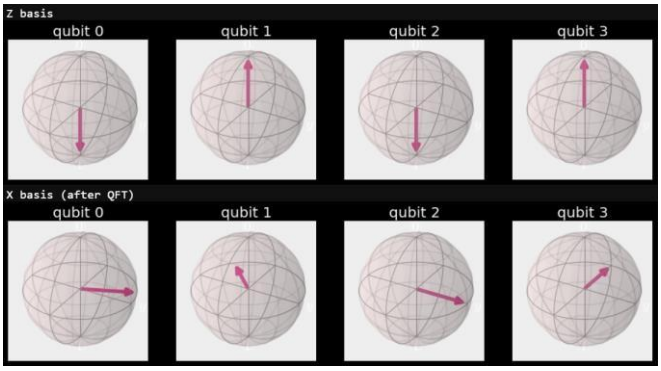


Figure 6.8 Output of QFT form 0101

The statevector for the 2nd set of qubits is shown in fig. 6.9.

```
(0.25-0j)|0000> +
(-0.1+0.23j)|0001> +
(-0.18-0.18j)|0010> +
(0.23-0.1j)|0011> +
0.25j|0100> +
(-0.23-0.1j)|0101> +
(0.18-0.18j)|0110> +
(0.1+0.23j)|0111> +
(-0.25+0j)|1000> +
(0.1-0.23j)|1001> +
(0.18+0.18j)|1010> +
(-0.23+0.1j)|1011> +
(-0-0.25j)|1100> +
(0.23+0.1j)|1101> +
(-0.18+0.18j)|1110> +
(-0.1-0.23j)|1111>
```

Figure 6.9 Statevector of output of QFT from 0101

However, running nearly 10,000 shots of quantum measurements on the circuit produces the following histogram as shown in 6.10.

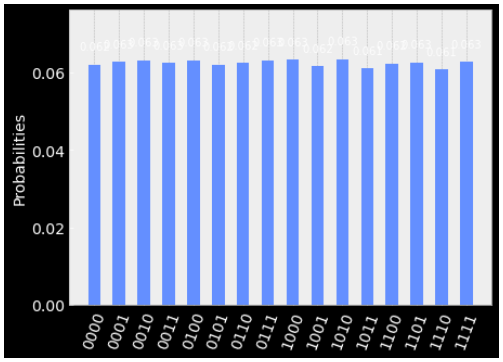


Figure 6.10 Measurement outcome statistics in Z basis

As you can see from the plot above, all the states are equally probable which is obvious from the bloch vectors since all the qubits lie in the xy-plane and a projective measurement on the z axis would ultimately produce all possible states equally probably, irrespective of the phase angle.

Measuring in the X basis gives the following result as shown in fig. 6.11.

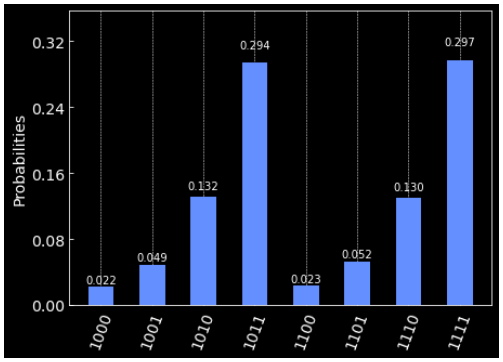


Figure 6.11 Measurement in the X basis

Although this gives comparatively more information about the statevector, the phases can still not be estimated using just this information. For example, consider the states '1011' and '1111' from the above plot. It may seem that qubit 2 is a superposition of the |+> and |-> states. However, there are 2 such possible superposition states:

$$\frac{1}{\sqrt{2}}|+\rangle + |-\rangle$$

and,

$$\frac{1}{\sqrt{2}}|+\rangle - |-\rangle$$

In the present case of 4 qubits and an input of 0101, it is in the prior case (looking at the Bloch sphere), but it would not be possible to get that information using the measurement statistics alone. Therefore, the QFT alone cannot be used to find the discrete Fourier transform directly using the quantum circuit alone, despite its near exponential speedup.

Chapter 7 Conclusion and Future Work

Quantum computers are machines that use the properties of quantum physics to store data and perform computations. This can be extremely advantageous for certain tasks where they could vastly outperform even our best supercomputers.

7.1 Concluding points

- In this work, the authors conducted a thorough comparison of quantum algorithms and protocols with classical techniques to theoretically prove the supremacy of quantum computing.
- A lot of work still remains, however. Although all the algorithms are theoretically more efficient than their classical counterparts, the practical implementation is not as
- straightforward. Quantum hardware still lacks behind in comparison to the development of quantum software.
- Therefore, although the authors could prove theoretical quantum supremacy, achieving similar practical advantage is tough and still requires major research.

7.2 Future Developments

- The most important part would be to research and explore hardware advancement properties
- Research and implement advance error correction techniques
- Research on Quantum Fault Tolerance
- Explore other IDE's and libraries supporting quantum computing
- Explore Quantum Optimization algorithms using D-waves system. Dabble into quantum annealing.

References

[1] Arute, Frank, et al. "Quantum supremacy using a programmable superconducting processor." Nature 574.7779 (2019): 505-510.

[2] Pednault, Edwin, et al. "Leveraging secondary storage to simulate deep 54-qubit sycamore circuits." arXiv preprint arXiv:1910.09534 (2019).

[3] Babadi, Mehrtash, Eugene Demler, and Michael Knap. "Far-from-equilibrium field theory of many-body quantum spin systems: Prethermalization and relaxation of spin spiral states in three dimensions." Physical Review X 5.4 (2015): 041005.

[4] Peruzzo, A. "A variational eigenvalue solver on a quantum processor. eprint." arXiv preprint arXiv:1304.3061 (2013).

[5] Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002): 558-559.

[6] Kashyap, M. Ramachandra. "QKD Algorithm BB84 Protocol in Qiskit." (2020).

[7] Liu, Tao. "The Applications and Challenges of Quantum Teleportation." Journal of Physics: Conference Series. Vol. 1634. No. 1. IOP Publishing, 2020.

[8] Yimsiriwattana, Anocha, and Samuel J. Lomonaco Jr. "Distributed quantum computing: A distributed Shor algorithm." Quantum Information and Computation II. Vol. 5436. International Society for Optics and Photonics, 2004.

[9] Han, Yu, et al. "Machine-learning-driven synthesis of carbon dots with enhanced quantum yields." ACS nano 14.11 (2020): 14761-14768.

[10] Bologna, Guido, and Yoichi Hayashi. "QSVM: A support vector machine for rule extraction." International Work-Conference on Artificial Neural Networks. Springer, Cham, 2015.

[11] Ahmed, Sajjad. Pattern recognition with Quantum Support Vector Machine (QSVM) on near term quantum processors. Diss. Brac University, 2019.

[12] Bologna, Guido, and Yoichi Hayashi. "QSVM." Lecture Notes in Computer Science; Proceedings of International Work-Conference on Artificial Neural Networks 2015 (IWANN), 10-12 June 2015, Palama de Mallorca, Spain. No. CONFERENCE. 10-12 June 2019, 2015.

[13] Grimsley, Harper R., et al. "Adapt-vqe: An exact variational algorithm for fermionic simulations on a quantum computer." arXiv preprint arXiv:1812.11173 (2018).

[14] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters 85.2 (2000): 441.

[15] Chong, Song-Kong, and Tzonelih Hwang. "Quantum key agreement protocol based on BB84." Optics Communications 283.6 (2010): 1192-1195.

[16] Weinstein, Yaakov S., et al. "Implementation of the quantum Fourier transform." Physical review letters 86.9 (2001): 1889.
[17] Hales, Lisa, and Sean Hallgren. "An improved quantum Fourier transform algorithm and applications." Proceedings 41st Annual Symposium on Foundations of Computer Science. IEEE, 2000.
[18] Sim, Sukin, Peter D. Johnson, and Alán Aspuru-Guzik. "Expressibility and entangling capability of parameterized quantum circuits for hybrid quantum-classical algorithms." Advanced Quantum Technologies 2.12 (2019): 1900070.
[19] Schuld, Maria, and Nathan Killoran. "Quantum machine learning in feature Hilbert spaces." Physical review letters 122.4 (2019): 040504.
[20] Watkins, David S. "Understanding the QR algorithm." SIAM review 24.4 (1982): 427-440.