|  |  |
| --- | --- |
| Is a quantum computing future actually possible?  Quantum computing  Report | Patrick Barsoum (19240058), Richard Alexander (19270151), Eoin Chedzey (18223796), Elton Babela (18196497)  CS4182 Foundations of Computer Science 2 |

Table of Contents

[Abstract 2](#_Toc39674754)

[Introduction 3](#_Toc39674755)

[Applications of Quantum Computing 4](#_Toc39674756)

[Cryptography 4](#_Toc39674757)

[Introduction 4](#_Toc39674758)

[Quantum Key Distribution 4](#_Toc39674759)

[Medicine 5](#_Toc39674760)

[Economy and Finance 5](#_Toc39674761)

[Information Technology 5](#_Toc39674762)

[Natural Sciences 5](#_Toc39674763)

[Bibliography 6](#_Toc39674764)

# Abstract

# Introduction

# Applications of Quantum Computing

One of the biggest applications for Quantum Computing is cryptography.

## Cryptography

### Introduction

One of the important areas in modern society is communicating securely. Quantum information transmission and processing contributes significantly to this. Quantum cryptography is a great example that may be the main protection against quantum codebreaking for the future. One of the new features of quantum cryptography is that the security of quantum key generation and quantum cryptographic protocols is based more on the laws of nature than classical cryptography. The security of classical cryptography is based on “unproven assumptions concerning the computational hardness of some algorithmic problems.” (Gruska 2002)

### Quantum Key Distribution

Quantum key distribution is a method in which quantum states are used to make a random secret key for cryptography.

Basically, Sarah tries to send qubits to Patrick and an eavesdropper Leah, tries to learn and change as much as it can without being detected. This is a difficult task for the eavesdropper as quantum states cannot be measured and copied without causing some sort of disturbance which are immediately detected. (Gruska 2002)

This is the idea of it: There are two people who are separated and want to communicate with each other. In this case, we will be using Sarah and Patrick. Sarah sends to Patrick 2n qubits which are randomly chosen from one of the states |0) , |1) , |+) , |−). Patrick measures the bits he received. He does this by using the measurement basis randomly between {|0), |1)} and {|+), |−)}. Sarah and Patrick tell each other publicly where anyone can listen to how they prepared and measured each qubit. They find out by chance that they may have used the same method which on average, happens half the time and keep those results. If there are no errors, they now “share the same random string of n classical bits.” An example of this is to associate |0) and |+) with 0 and |1) and|-) with 1. This is known as *raw quantum transmission*, RQT. (Steane 1997)

So far, it is impossible to learn Patrick’s measurement results by just looking at the qubits journey. Some evidence of their presence is left behind. One way for an eavesdropper of whom we will call Leah, to try and find out the key, is to catch the qubits and measure them before passing them to Patrick. On average, Leah guesses Sarah’s qubits correctly not disturbing her cycle. Leah’s correct guesses doesn’t cause conflict with Patrick’s. This causes Leah to learn the state of half of the n qubits which Sarah and Patrick trust, and interrupts the other half. Leah basically corrupts n/4 bits of the RQT. By randomly choosing n/2 bits of the RQT, Sarah and Patrick can detect the presence of Leah and so decide to publicly announce the values they have. They can be sure that no eavesdropper was present if they agree on these bits. This can be done since the probability that Leah was present and they happened to choose n/2 uncorrupted bits is (3/4)^n/2 ≃ 10^−125 for n = 1000. The secret key is the n/2 unrevealed bits. This method is used to detect eavesdropping. (Steane 1997)

Quantum computing can provide helpful advancements to human life thanks to the enormous abilities of quantum technology. Not only does it aid in security (cryptography) but also everyday jobs.

## Medicine

* The research and development of medical sciences. An example is analysing a sequence of DNA which are usually large in size.
* Diseases like cancer can be diagnosed faster and more accurate.
* Producing and discovering drugs at a scale.
* Analysing and processing heavy images which bioengineering, and telemedicine rely on. (Al-maghraby 2017)

## Economy and Finance

* Investment decisions can be done through the analysis and simulation of stock portfolios.
* The detection of fraud is more effective and can be viewed in real time.
* Applications for planting and agriculture. (Al-maghraby 2017)

## Information Technology

* Analysing and searching data from big data warehouses.
* Testing and simulating software that is time consuming and complex for current computers.
* The fast response and analysis of massive data such as traffic management is enhanced using quantum processes. (Al-maghraby 2017)

## Natural Sciences

* Use quantum computing power to study and simulate experiments that are too costly and time consuming.
* Analysing time series and forecasting. (Al-maghraby 2017)

# Bibliography

Al-maghraby, R. (2017) ‘Promising Real-Life Applications of Quantum Computing’, 1–5, available: http://www.onewayforward.info/Papers/Promising Real-Life Applications of Quantum Computing.pdf.

Gruska, J. (2002) ‘Quantum computing’, *Technology Review*, 70(7), 632–636, available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.397.2253&rep=rep1&type=pdf.

Steane, A. (1997) ‘Quantum computing’, *Reports on Progress in Physics*, 61(2), 117–173, available: https://arxiv.org/pdf/quant-ph/9708022.pdf.