Title of Independent Study Project

by

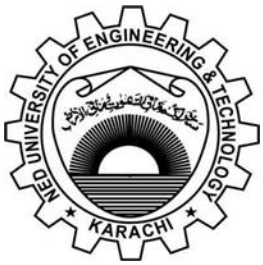
Abdul Qadeer Khan

CT-001/2016-17

Supervised by Dr. Najmi Ghani Haider

MS (Computer Science & Information Technology)

CT-600 Independent Study Project



NED University of Engineering & Technology, Karachi

Department of Computer Science & Information Technology

October 2018

Abstract

All praises to Almighty ALLAH Who enabled me to carry out this research work and gifted me a splendid supervisor, very kind parents and loving family members. My supervisor, Prof. X Y Z, guided and supported me beyond my expectations. I am very much thankful to him for sharing his extensive knowledge and research experience with me.

Acknowledgements

All praises to Almighty ALLAH Who enabled me to carry out this research work and gifted me a splendid supervisor, very kind parents and loving family members. My supervisor, Prof. X Y Z, guided and supported me beyond my expectations. I am very much thankful to him for sharing his extensive knowledge and research experience with me.

Declaration

Some parts of the work presented in this report have been published in the following article:

M. M. Khan, M. Murphy, and A. Beige, "High error-rate quantum key distribution for long distance communication", New Journal of Physics, 11 (2009) 063043.

Some parts of the work presented in this thesis have been submitted for publication in the following:

M. M. Khan, J. Xu, and A. Beige, "High error rate quantum key distribution with two-dimensional photon states", The 41st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2011) (submitted).

Dedication

Dedicated to my beloved parents

Content

1 Introduction

1.1 *Background*

1.2 Objectives

1.3 Report Plan

This section illustrates the composition of thesis in different chapters along with their brief description.

Chapter 1 provides introductory material about the thesis.

Chapter 2 reviews some basic concepts from linear algebra, and describes the standard notations which are used for these concepts in the study of quantum .

Chapter 3 provides the fundamental principles of quantum algorithms.

Chapter 4 presents concept of quantum parallelism which is a fundamental feature of m.

Chapter 5 explains very .

Chapter 6 presents the .

Chapter 7 describes brieflyfunctions.

Chapter 8 presents previous classical this chapter.

Chapter 9 discusses the collision are discussed in this chapter.

Chapter 10 is the conclusion and the recommendations for future research work.

2 Chapter 2 Title

2.1 Introduction

Plank, Einstein and Bohr obtained the early great success in the quantum theory in the period from 1900 to 1925. Nevertheless, up to this time there existed no complete

2.2 Hilbert Space Framework

Every figure must be cross referenced in line with the text under which it is discussed. For instance; Face recognition comprises of four steps as shown in Figure 2.1.

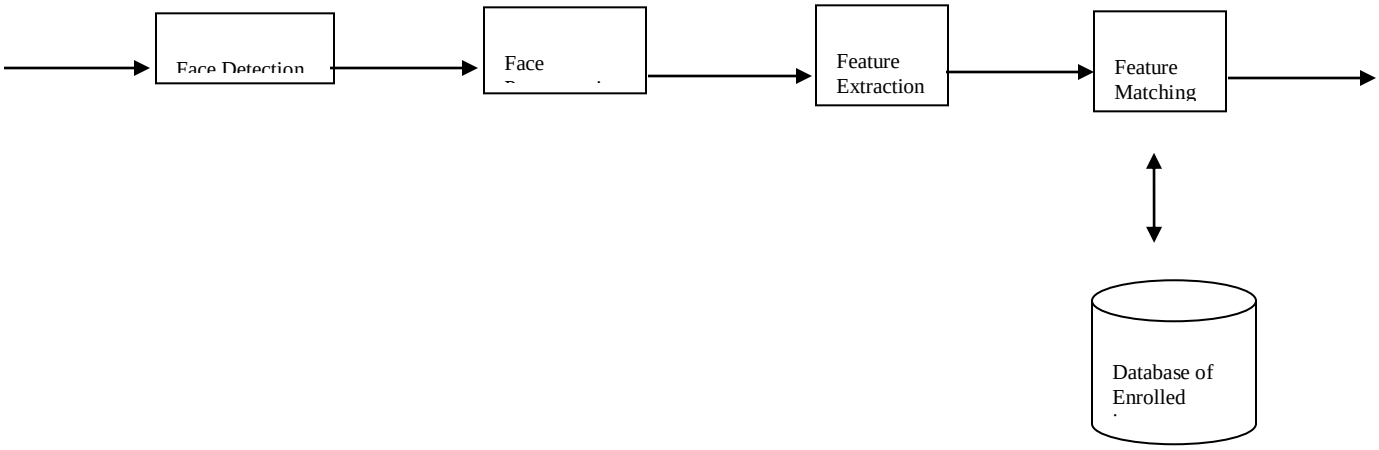


Figure 2.1: The four general steps in face recognition

2.3 Postulates of Quantum Mechanics

2.4 Discussion

3 Title Chap 3

3.1 Introduction

3.2 Quantum Gates:

Description under this section must include cross referencing of Table 1 in line with text.

For instance; Quantum Gates values are shown in Table 1.

TABLE I. **Table Name or title.**

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

3.3 Universal Quantum Gates

the Bloch sphere as well as a circle. So the big question is how do we move an irrational

3.4 Other Important Gates:

3.5 Swap Gate

3.6 Discussion

The development of the quantum computational toolkit begins with operations on the simplest quantum systems of all – a single qubit. Single and multi qubit gates are introduced in this chapter. These gates can be applied to any subset of qubits as desired, and a universal family of gates can be implemented. For example, it can be shown to apply the C-Not gate to any pair of qubits in quantum computer. The Hadamard, CNOT and $\pi/8$ gates form a family of gates from which any unitary operation can be approximated, and thus is a universal set of gates. Other important gates may also be constructed with the help of these gates.

4 Chapter Title

4.1 Introduction

The study of quantum computing is relatively new, most give credit to Richard Feynman for being the first to Parallelism

Most modern quantum

5 The Title Chapter

5.1 Introduction

The study of quantum computing is relatively new, most give credit to Richard Feynman for being the first to Parallelism

Most modern quantum

6 Evaluation Chapter

6.1 Introduction

A deeper understanding of hash function security can be obtained through considerations

7 Conclusion & Future Recommendations

References

(IEEE reference style)

[1] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[2] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings: 35th Annual Symposium on Foundations of Computer Science, November 20–22, 1994, Santa Fe, New Mexico, pages 124–134. IEEE Computer Society Press, 1994.

[3] How significant are the known collision and element distinctness quantum algorithms? Lov Grover and Terry Rudolph† Bell Labs, 600-700 Mountain Ave April 2005

[4] Wang, F. Guo, X. Lai, H. Yu, Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD, eprint archive 2004/199, http://eprint.iacr.org/2004/199, presented at the Crypto 2004 rump session, August 17, 2004.

[4] Wang, X. Lai, F. Guo, H. Chen, X. Yu, Cryptanalysis for Hash Functions MD4 and RIPEMD, Eurocrypt 2005, to appear.

[5] A. Joux, Collisions for SHA0, presented at the Crypto 2004 rump session, August 17,2004.

Plagiarism Report generated from Turnitin must be attached at the end of the report, duly signed by the student.