Ain Shams University
Faculty of Engineering
Computers and Systems Department

Quantum Database users and system security privileges

by
Israa Ibrahim Ahmed Hamed Hamouda
Bachelor Degree in Computers and Systems Engineering
Ain Shams University 2011

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF (MASTER OF ELECTRICAL ENGINEERING, COMPUTERS AND SYSTEMS)

DEPARTMENT OF (COMPUTERS AND SYSTEMS)
Supervised By

Prof. Dr. Ayman Bahaa Eldin
Dr. Hazem Said

Cairo, Egypt
FEBRUARY, 2018

Faculty of Engineering
Ain Shams University
Computer and Systems

Examiners Committee

Name : Israa Ibrahim Ahmed Hamed Hamouda

Thesis : Quantum Database users and system security privileges

Degree : Master's of Computer Engineering - Computer and Systems

Name, Title, and Affiliate	Signature
	……

Date: 19 / 02 / 2018

Abstract

Israa Ibrahim Ahmed Hamed Hamouda
Quantum Database users and system security privileges
Master's in Electrical Engineering, Computers and Systems
Ain Shams University, 2017

Now that quantum computing is quickly moving from theory to application, the critical next step is to design and implement the next generation algorithms that will power those quantum systems. In this thesis, a new algorithm that relates to how databases will be accessed and traversed in quantum computers, will be presented along with proposing a system that this algorithm will be analyzed on. All the database operations are going to be introduced based on the proposed system along with examples. The proposed algorithm is based on modifying Grover's algorithm by adding a security bit to the algorithm, this bit is unique for identification of each user. The identification bit is used to maintain the security of traversing the database on the user and the system levels. This bit is added at the table level and is embedded through all the database transactions.

Keywords:

Quantum Computing, Quantum Databases, Grover's Algorithm, Generalized Grover's Algorithm.

Summary

Quantum Database users and system security privileges

Israa Ibrahim Ahmed Hamed Hamouda

Master of Science in Electrical Engineering (Computer and Systems Engineering)

Keywords -- Quantum Computing, Quantum Databases, Grover's Algorithm, Generalized Grover's Algorithm.

The thesis is divided into five chapters including lists of contents, tables, figures and one appendix for explaining Quantum Computing as well as list of references.

Chapter 1

This chapter is divided into four parts. The first part is the problem definition. Second and third parts are the thesis methodology and contribution. Last part gives a brief explanation for each chapter in the thesis.

Chapter 2

This chapter is divided into three main sections, the first one gives introduction on classical databases and their components. It explains the architecture of the databases in general and then gives the same explanation for the quantum databases. The second section explains the main idea behind Grover's iteration algorithm along with in details equations of the algorithm to provide better understanding. At the end of this section, the circuit diagram for Grover's is illustrated and its main components are

explained. The last section in this chapter provides brief explanation of the need to generalize Grover's algorithm. It also explain different approaches used to implement such generalization.

Chapter 3

In this chapter, the proposed database system for the algorithm is going to be discussed in details. An example of one table will be provided, as well as, all the related equations and quantum circuit diagrams. All the methods for traversing the database system will be illustrated by describing common procedures such as SELECT, UPDATE, INSERT and DELETE. At the end of this chapter, the proposed algorithm will be laid out. Detailed quantum circuits, block diagrams and related quantum equations will be provided for each step in the algorithm.

Chapter 4

This chapter is divided into two sections; the first section provides a mathematical analysis for a complete one iteration of the proposed algorithm along with a detailed equations analysis for the different steps in the iteration to better understand the algorithm. At the end of this section, it is shown that the proposed algorithm has the same results as the main Grover's algorithm. The second section shows a security analysis explaining some of the different security threats on the database nowadays, and shows if the algorithm can mitigate such threats or not, based on the target of each attack.

Chapter 5

This chapter is divided into two main parts. The first part gives a brief conclusion about the mathematical and security analysis that was conducted in the previous chapter. The second part is the future work, giving different ideas that could be used to extend the proposed algorithm to enhance it by maintaining the security levels provided by the algorithm.

Thesis supervisors:

Prof. Dr. Ayman Bahaa El-Din

Dr. Hazem Said

Preface

The topic of this thesis was stemmed from my passion and interest in the Quantum Computing field. As we all know, the world is moving forward and the classical world is limiting lots of our implementations and breakthroughs. With the new Quantum world, what we thought impossible is becoming possible. From that and based on my work in the IT field and knowing how important databases are and how securing them is so crucial. My interest was shifted to the Quantum Database and how they differ from the classical ones and the different ways to secure them. That is why in this thesis a new algorithm for securing the Quantum Databases is proposed.

Acknowledgements

First, I would like to thank God for all the blessings that I have and one of them is the ability to finish my thesis.

I would like to thank my supervisor, Prof. Dr. Ayman Bahaa, for all his guidance, encouragement and patience through all the phases of my thesis along with dedicating a lot of his time to help me. I would also like to thank my supervisor, Dr. Hazem Said, for helping me and answering all my questions related to Quantum Systems. I was so lucky to work with them and have the opportunity to gain from their knowledge. I want to express my gratitude for all the employees in Computers and Systems department for helping me and guiding me through my master's journey.

I would like to thank my family, especially mom and dad, and my friends who helped me by their encouragement for me to finish my master's courses and thesis. I would like to express my gratitude to Brandon who assisted me through my pre-masters courses and then again through writing the thesis itself. I would also like to thank my best friends Aalaa and Noha, who helped me a lot through all times. Finally yet importantly, I want to express my appreciation for my cousins Sondos, Sarah and Sama, for providing a great encouragement system to me.

I am very gracious for all of them for their help.

Statement

This dissertation is submitted to Ain Shams University for the degree of Master's in Electrical Engineering in Computers and Systems department

The work included in this thesis was out by the author at Computers and Systems Department, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : 21/10/2017

Signature :

Name : Israa Ibrahim Ahmed Hamed Hamouda

Table of Contents

Table of Figures

Table of Tables

1: Introduction

1.1 Problem definition

Quantum computers far surpass that of their classical predecessors in many different ways. Power requirements and efficiency, to the sheer performance of billions of calculations per second. One of the most striking differences, however, is that quantum computers take advantage of attributes that exist only at sub-atomic levels. It is the ability of sub-atomic particles to exist in more than one state and any time that quantum computing draws its power. In a classical computer, the most basic unit is called the bit, which at any given time exists either as a 0 or as a 1 (+/- 5v). While in quantum computing, this unit is called the q-bit. The q-bit is capable of existing in both the 0 and the 1 state at the same time, this ability is known as superposition. Quantum computers use the superposition property to compute the needed data at a bit level, while in classical computers such computations are done on CPU level. If the quantum computer is in a superposition, it will be broken randomly to one of the superposed values. If there is no superposition, it will act normally as a classical computer.

A database is used to organize data in a computer system, so it would be easy to retrieve, manage, access and modify. It is one of the cornerstones of how data is stored on private and public networks, the web and in the cloud. As we move forward into the digital age, when security threats and cyber-attacks are constantly on the rise, the world is continually faced with the limits of existing technologies when it comes to securing the most critical information. The quantum database, conceptually thanks to the superposition property, will allow the delay of making choices using transactions that are held in a superimposed state until an application or user forces the choice by observation. With the aid of quantum cryptology,

data and transactions will be proven secured on both the system and the user level.

Quantum cryptography with the aid of quantum mechanics theories maintain that the distribution of private information is secured against any attack, even when faced with any adversaries who are more technologically advanced, who in some cases could potentially have more computing power and resources. There are different quantum security algorithms that are used to secure the quantum world. The most popular algorithms are the quantum key distribution algorithms, which are used to produce and exchange the shared key between the communicating parties.

The aim of this thesis is to propose a new method by modifying Grover's algorithm to access the quantum databases securely. The proposed algorithm searches the database and retrieves the data based on the user's' privilege. Every user in a database is unique; the proposed algorithm depends on the users' uniqueness to decide if the user should be able to view the data or if he is not authorized to do so. The proposed algorithm depends on securing the quantum database at the table level by having each table in the database contain the information of the eligible users to access that table. The algorithm also depends on embedding the vector of users who are eligible to access the table in all the queries that would be performed on that table in order to make sure that the authorized users are the only ones who are retrieving, inserting, modifying or deleting the data from the table.

1.2 Thesis Methodology

In this thesis, the methodology used was to first identify the problem. The problem here is there is that a quantum database that stores all the sensitive data for an organization. This database needs to be secured on the system