Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

A Model of Security Protocols for Distributed Quantum Systems

by

Ola Mohamed Hegazy

Master of Electrical Communication

(Electrical Communication Engineering)

Cairo University, 1993

A THESIS

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

(Electrical Engineering)

DEPARTMENT OF COMPUTERS AND SYSTEMS ENGINEERING

Supervised By

Prof. DR. Yasser Hisham Dakroury

DR. Ayman Mohamed Bahaa El-Din Sadek

Cairo, Egypt

January, 2009

П

بسم الله الرحمن الرحيم

"قالوا سبحانك لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم"

صدق الله العظيم البقرة 32

بسم الله الرحمن الرحيم

"وقالوا الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله"

صدق الله العظيم الأعراف 43

Faculty of Engineering
Computer and Systems
Eng. Dept.

Examiners Committee

Name	**:**	**Ola Mohamed Abo El-Regal Hegazy**
Thesis	**:**	**A Model of Security Protocols for Distributed Quantum Systems**
Degree	**:**	**Doctor of Philosophy**

Name, Title, and Affiliate	Signature
	....

Date: / /

Abstract

Ola Mohamed Hegazy

A Model of Security Protocols for Distributed Quantum Systems

Doctor of Philosophy dissertation

Ain Shams University, 2009

In this thesis we propose a new protocol in information transmission security using a new technology based on the quantum theory that uses the quantum mechanics phenomena and characteristics, which give a higher level of security for any cryptography scheme.
We present a new scheme here for direct secure and confidential communication between two parties, where there is no need for exchanging a shared key first, but alternatively, we construct an algorithm to send the message bits at the same time of sending the quantum bits that are used in the encoding process simultaneously on two different channels.
Also, in our proposed algorithm, we apply an important application of the quantum systems that is superdense coding. This application procedure gives, not only a higher level of security, but also a higher efficiency for the transmission process, as in this procedure we encode two classical bits per one quantum bit.

After demonstrating the main idea of the protocol, we introduce different kinds of errors that the quantum channel could be exposed to due to the noise effect, and with that we also introduce some error correcting schemes for some of them.
As the effects of the eavesdropping on the quantum channel is very similar to the effect of the noise, we show in the security analysis some of the attacks that our protocol, and other quantum protocols, could be vulnerable to, and advice the way of treatment that we apply comparing with the other work in that issue of security.

Finally, we introduce some other modifications that could be used as a future work in this direction.

Keywords:
Quantum cryptography, quantum secure direct communication, quantum key distribution, quantum entanglement, super-dense coding theorem.

Acknowledgements

First of all I thank Allah for all his generosity and help.

Second I would like to express my deep gratitude to Prof. Dr. Mohammad Adeeb El-Ghonaimy for his great help in choosing the point of research, and his big efforts along the thesis development since it was just thoughts in mind. I would like to thank him also for his great support and all the materials and references he gave to me. Also I would like to dedicate my thanks to Prof. Dr. Yaser Hisham Dkroury, and Dr. Ayman Mohamed Bahaa El-Din, for their valuable advises, and their enormous efforts in directing me in my work and revising the thesis. I can not express my thanks to them for his care and interest since I was just joining the department for study for the degree. Throughout the years I have worked in the department of computer and systems engineering, I can not forget continuous effort for directing me before and during the preparation my thesis.

I would like also to thank all my professors, and my teachers, Staff of Computer and Systems Engineering Department for all what they taught me, the way they treated me, and for their care and support that they give to me all the time of study and research.

I would like also to thank my mother, and all my family, specially, my uncle Prof. Dr. Mahmoud Hanafi Ahmed, in laser department in the college, Prof. Dr. Sana'a El-Ola Hanafi Ahmed, the Vice Dean of faculty of Computers, Cairo University, and Prof. Dr. Mohamed Gamal Darwish, the Dean of faculty of Engineering, El-Ahram Canadian University, for

their deep support and encouragement they give to me during the thesis development.

Finally I would like to thank my small family, my husband and children for her patience and great support and encouragement during the years of research and development of the thesis.

Statement

This dissertation is submitted to Ain Shams University for the degree of Doctor of Philosophy in Electrical Engineering, Computer and Systems

The work included in this thesis was out by the author at Computer and systems Engineering Department, Ain Shams University.

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

Date : 31/1 /2009

Signature :

Name **:** Ola Mohammad Abo El-Rgal Hegazy

Table of Contents

List of Tables

List of Figures

1: Introduction

Classical cryptography can be divided into two major branches; secret or symmetric key cryptography and public key cryptography, which is known as asymmetric cryptography. Secret key cryptography represents the most traditional form of cryptography in which two parties both encrypt and decrypt their messages using the same shared secret key. While some secret key schemes, such as one-time pads, are perfectly secure against an attacker with arbitrary computational power, they have major practical disadvantage that before two parties can communicate securely they must somehow establish a secret key. In order to establish a secret key over an insecure channel, key distribution schemes based on public key cryptography, such as Diffie-Hellman, are typically employed.

In contrast to the secret key cryptography, a shared secret key is not needed prior to communication in public key cryptography. Instead, each has a private key, which remains secret, and a public key that they may distribute freely. If one party, say; Alice, wants to send a message to another party, Bob, she would encrypt her message with Bob's public key then send it to him who is the only one who can decrypt it with his own private key. While there is no need to exchange a key, the security of public key cryptography algorithms are currently all based on the unproven assumption of the difficulty of certain problems, such as integer factorization or the discrete logarithm problem [Schneir, 1996] [Haitjema, 2007].

Conventional cryptosystems such as DES or even RSA are based on a mixture of guess-work and mathematics. Information theory shows that traditional secret-key cryptosystems cannot be totally secured unless the key is at least as long as the plaintext, and it is used only once [Shannon, 1949]. On the other hand, the theory of computational complexity now is not well enough to prove the computational security of public-key