شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

بسم الله الرحمن الرحيم

HANAA ALY

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

HANAA ALY

شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

HANAA ALY

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Computer and Systems Engineering Department

Photonic Secure Quantum Communication

A Thesis

Submitted in partial fulfillment of the requirements of the degree of

Doctor of Philosophy in Electrical Engineering

Submitted by

Hossam Mohamed Abdel Rahman AbdEllah

M.Sc of Electrical Engineering

(Electronics and Communications Engineering)

Ain Shams University, 2011

Supervised By

Prof. Ayman Mohamed Bahaa-Eldin

Computer and Systems Engineering Dept., Ain Shams University

Prof. Khaled Abdel Wahab Kirah

Engineering Physics and Mathematics Dept., Ain Shams University

Dr. Mohamed Aly Aly Sobh

Computer and Systems Engineering Dept., Ain Shams University

Cairo, 2021

Examiners' Committee

Name: **Hossam Mohamed Abdel Rahman AbdEllah**

Thesis: Photonic Secure Quantum Communication

Degree: Doctor of Philosophy in Electrical Engineering

Title, Name and Affiliation	**Signature**
Prof. Khaled Hussein Mostafa Misr International University, Faculty of Computer science, Computer Science Dept.	.....
Prof. Hani Mohamed Kamal Mahdi Ain Shams University, Faculty of Engineering, Computer and Systems Engineering Dept.	.....
Prof. Ayman Mohamed Bahaa-Eldin Ain Shams University, Faculty of Engineering, Computer and Systems Engineering Dept.	.....
Prof. Khaled Abdel Wahab Kirah Ain Shams University, Faculty of Engineering, Engineering Physics and Mathematics Dept.	.....

Date:

STATEMENT

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

The work included in this thesis was carried out by the author at the Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt.

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

Name: Hossam Mohamed Abdel Rahman AbdEllah

Signature:

Date:

Curriculum Vitae

Name of Researcher	Hossam Mohamed Abdel Rahman AbdEllah
Date of Birth	29/11/1986
Place of Birth	Egypt
First University Degree	B.Sc. in Electrical Engineering
Name of University	Ain Shams University
Date of Degree	June 2008
Second University Degree	M.Sc. in Electrical Engineering
Name of University	Ain Shams University
Date of Degree	April 2011

ACKNOWLEDGEMENT

I would like first to thank my supervisors Prof. Dr. Ayman Mohamed Bahaa-Eldin, Prof. Dr. Khaled Abdel Wahab Kirah and Dr. Mohamed Sobh for their continuous guidance, encouragement, help and patience. I learned so many valuable things from them, but above all, they taught me how to be devoted to research and how to help others.

Prof. Dr. Khaled Abdel Wahab Kirah was always guiding me step by step through the whole thesis work. He provided me with great help during all phases of this thesis.

Last but not least, I would like to thank my parents. Their patience, care, and love are what guided me through my whole life. I pray to God that I will always be a good faithful son to them.

ABSTRACT

Quantum Cryptography has been playing an important role in communications after the reveal of vulnerabilities of classical channels. The main aim of encryption is to guarantee the security of the messages among communicators, without reducing the efficiency of communication channel. The most popular idea was quantum key distribution which unfortunately leads to the loss of lots of qubits since many of them have to be discarded. In 2002, Quantum secure direct communication QSDC was launched based on transmitting directly the secret messages without first establishing a key to encrypt them. It does not require any additional classical information in communications.

While most of the researches on channel security have focused on point to point communication, little attention was given to multi nodes networks. In this study, the possibilities of loopholes in multi-sites networks using quantum secure direct communication encryption protocols are analyzed. Several solutions are proposed. Depending on the installed topology (linear, ring, star and partially meshed) and on the distance between the nodes, a different solution is proposed.

In this study as well, a complete modeling and simulation has been done for a QSDC communication system using quantum photonic simulator and compared to experimental results. Security enhancements has been done by introducing decoy state function to the system and dispersive compensation techniques to drive the system to match practical fiber lengths which are required in commercial systems.

Key words: Quantum Cryptography; Quantum Secure Direct Communication; QSDC; multisite network; Entangled single photon pair; Two step entanglement based protocol; Frequency coding scheme; Single photon source; Decoy State protocol; Lumerical;

SUMMARY

This dissertation demonstrates the importance of quantum encryption for unconditioned secure communication. The dissertation consists of four chapters organized as follows:

Chapter One: The chapter begins with an introduction on the history of data transfer, data security and the history of cryptography. In addition, the problems of classical encryption have been discussed and the way to defeat them using quantum cryptography.

Chapter Two: In this chapter, physics and concepts behind quantum cryptography and the different protocols that have been proposed to serve this idea. Limitations of the quantum techniques have been showed. the mathematical descriptions of those phenomena and techniques have been studied as well.

Chapter Three: In this chapter, new ideas have been proposed to generalize the quantum encryption techniques, to be able for deployment over practical multi-site networks, rather than working only over point to point case study as in literature.

Chapter Four: complete modeling and simulation for the QSDC system have been done successfully. Proposing decoy state technique as an enhancement to the conventional systems, comparison has been done between the results of the proposed system and the conventional one from security point of view and system performance (information capacity).

Chapter Five: In this chapter Conclusions are drawn and future work based on this work is suggested.

List of CONTENTS

List of Figures

List of Tables