الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يونيرسيتي إسلام انتارابغسا ملسيا

VULERNABILITY EVALUATION OF OPTICAL FIBER BASED QUANTUM KEY DISTRIBUTION SYSTEM UTILIZING VISIBILITY INTERFERENCE

BY

ABDULLA ABDULQADER AL-ATTAS

A dissertation submitted in partial fulfilment of the requirement for the degree of Masters of Science in (Computer and Information Engineering)

Kulliyyah of Engineering

International Islamic University

Malaysia

APRIL 2010

ABSTRACT

In Trojan-horse attack, settings of phase modulators inside Quantum Key Distribution (QKD) system are read by external interrogating light pulses, without interacting with quantum states and without raising security alarms. This thesis experimentally demonstrate two methods of eavesdropping onto a QKD system using Trojan horse attack, which eliminate the need of immediate interaction with transmitted quantum states. First, a strategy is proposed to gain the different four phase states of Alice's or Bob's phase modulator, depending on parameters of the interrogating pulse and apparatus. Second, an experimental setup is proposed to achieve the visibility interference for the eavesdropper and whether it matches with the QKD system visibility interference. Furthermore, the visibility interference will alert the eavesdropper whether it exceeded the QBER threshold of the QKD system to alert its presence. If it didn't exceed the threshold, the QKD system will use the transmitted qubit to generate the key for encrypting the data, while unknowingly it been obtained by the eavesdropper to decrypt the data. The Trojan horse attack proved to be a terrifying eavesdropping strategy that will gain information about the key without the exceeding the QBER threshold. It is also observed such attack could be implemented with the current level of technology and overcome the security proof, however it can be stopped with technical counter measures.

ملخص البحث

هجوم حصان طروادة، يقرأ مغير الطور داخل نظام تبادل المفتاح الكمى (الكيو كي دي) بواسطة نبضات ضوئيه خفيفة، دون التفاعل مع وحده الكم الضوئي ودون إثارة إنذارات أمنية. هذه الأطروحة سوف تقوم بتجريبتين عملياً لتوصف أستخدام المتنصت هجوم حصان طروادة ضد نظام تبادل المفتاح الكمى، حيث أنها سوف تلغي الحاجة للتفاعل الفوري مع وحده الكم الضوئي المرسلة. أولا ، تم اقتراح استراتيجية للحصول على الأطوار الأربعة المختلفة الصادره من أليس أو بوب مغير الطور، اعتمادا على معايير النبض واستجواب اجهزتها. الثاني ، وهو إعداد التجريبة المقترحة لتحقيق متوسط الرؤية البصرية للمتنصت وعما إذا كان يتماشى مع متوسط الرؤية البصرية لنظام تبادل المفتاح الكمى. وعلاوة على ذلك ، نتيجة متوسط الرؤية البصرية سوف تنبه المتنصت بوضوح إذا تجاوزت قياس وحده الكم الضوئي التابعه لنظام تبادل المفتاح الكمى وأخطرته بوجودها. إذا لم تتجاوز الحد الأدنى ، فإن نظام تبادل المفتاح الكمى سوف يستخدم الكم المتنقل لتوليد مفتاح تشفير البيانات ، في حين أنه لا يدري بأن المتنصت حصل عليها أيضاً لفك تشفير البيانات. أثبتت استراتيجية حصان طروادة للتنصت بأنها فعالة وبإستطاعتها الحصول على معلومات حول مفتاح التشفير دون أن تتجاوزالحد الأدنى لقياس وحده الكم الضوئي. وأن مثل هذا الهجوم يمكن تنفيذها بإستخدام التكنولوجيا الموجودة حالياً، ولكن يمكن مكافحتها بتدابير تقنية على نظام تبادل المفتاح الكمى.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science (Computer and Information Engineering)

……
Wajdi Al-Khateeb
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science (Computer and Information Engineering)

……
Khalid Al-Khateeb
Examiner

This dissertation was submitted to the Department of Electrical and Computer Engineering and is accepted as a partial fulfilment of the requirements for the degree of Master of Science (Computer and Information Engineering)

……
Othman O. Khalifa
Head, Department of Electrical
and Computer Engineering

This dissertation was submitted to the Kulliyyah of Engineering and is accepted as partial fulfillment of the requirements for the degree of Master of Science (Computer and Information Engineering)

……
Amir Akramin Shafie
Dean, Kulliyyah of Engineering

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Abdulla Al-Attas

Signature:…… Date:……

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

VULERNABILITY EVALUATION OF OPTICAL FIBER BASED QUANTUM KEY DISTRIBUTION SYSTEM UTILIZING VISIBILITY INTERFERENCE

Affirmed by Abdulla Al-Attas

…… …….

Signature Date

ACKNOWLEDGEMENTS

This research work was done under MIMOS-IIUM research collaboration. Within the collaboration period, some names have to be acknowledged for the successful completion of this thesis. Without their help, the long path that I covered would have been a rough one:

My Family: Who always been there for me, and helped morally and encouraged me throughout the thesis. Thanks for their numerous help and love.
Atiyah, Shariq, Salim and Sofia: My dear friends who always helped me technically, morally and encouraged me throughout the thesis. Thanks for their numerous help.
Dr. Wajdi Al-Khateeb: Supervisor of the thesis. Without his guidance and suggestion the thesis would not be in its entirety.
Dr. Suhairi Saharudin: Co supervisor of the thesis. He thought me a lot on optics and fundamentals of experimental work. He also provided us with essential equipments and experts support.
Prof. Dr. M. Ridza Wahiddin: A professor in IIUM and the Director of the Information Security Laboratories (ISL) at MIMOS Limited. He thought us a lot about quantum cryptography and conducted various lectures and courses on fundamentals to quantum mechanical theories.
Prof. Dr. Hugo Zbinden and Dr. Grégoire Ribordy: Expert opticians from University Of Geneva. Their training and experience was a great help in constructing, analyzing and understanding the basic optical setup of the Plug and Play QKD system.
Prof. Dr. Sergei Kulik: A professor in M.V.Lomonosov Moscow State University. His continuous support providing solutions to problems regarding SPD and lectures for advance topics on quantum cryptography was a great help for us.
Dr. Jesni, Ressa and Sellami: Lecturer and two postgraduate students at IIUM, They helped a lot on many aspects of fundamentals to quantum mechanical theories and quantum cryptography.

May Almighty accept all of us.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AES	Advance Encryption Standards
APD	Avalanche Photo Diode
BB84	Bennett, Brassard Protocol 84
BS	Beam Splitter
CIR	Optical Circulator
DES	Data Encryption Standard
DET	Detector
DPSK	Differential Phase Shift Keying
FM	Faraday Mirror
HWP	Half Wave Plate
InGaAs	Indium-Gallium-Arsenide
LiNbO3	Lithium Neonate
OFDR	Optical Frequency Domain Reflectometer
OTDR	Optical Time Domain Reflectometer
P&P	Plug & Play
PBS	Polarization Beam Splitter
PC	Polarization Controller
PM	Phase Modulator
PMF	Polarization Maintenance Fiber
POVM	Positive Operator Value Measure
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QWP	Quarter Wave Plate
RSA	Rivets-Shamir-Adelman
SMF	Single Mode Fiber
RSA	Rivets-Shamir-Adelman
SOP	State Of Polarization
SPD	Single Photon Detector
SPDC	Spontaneous Parametric Down Conversion
SPS	Single Photon Source
VOA	Variable Optical Attenuator

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Secure classical cryptosystems have been tested over the past few decades and sufficient work has been done to implement them for secure communication. Although RSA, DES, and ECC cryptosystems are in use, some groups claim that it has been proven theoretically that each of these systems can be hacked. Some of these algorithms are secure in terms of computational power, which is restricted by the capabilities of present hardware. However, if the message is tapped and stored, maybe with the rise of new technologies those messages will be decrypted with sufficient computational power. Nevertheless, with quantum cryptography, decryption of the quantum key is not possible so far. Because quantum cryptography utilizes the principles of quantum mechanics to devise a cryptosystem to generate random strings of qubits that can be used as key to encrypt and decrypt messages transmitted between two parties.

The most important feature of quantum cryptography is the ability to detect whether a third party is trying to intercept the key. As quantum bits cannot be copied, if the sender sends qubits to the receiver and an eavesdropper tries to gain knowledge of the key, then the eavesdropper has to corrupt the qubits during measurement, according to quantum mechanics.

Another difference between classical and quantum cryptography is that in quantum cryptography the transmission of the qubits is continuous because qubits cannot be copied and stored. In contrast, in classical cryptography the encrypted

message does not need to be continuous. It can be stored and transmitted in parts or in any desired way, which may not be true for quantum cryptography.

In principle, the security of QKD has been proven against many eavesdropping strategies provided that the eavesdropper's capabilities are not limited by the current level of technology (Biham, Boyer, Oscar Boykin, Mor, & Roychowdhury, 2000; Huttner & Ekert, 1994; Mayers & Yao, 1998). Furthermore, the QKD system has been proven against eavesdroppers attack that interact with quantum states transmitted in the communication line for an idealized model of equipment with certain non-idealities of components (laser source because it produce multiphotons instead of single photon & detectors because of its low efficiency) (Lütkenhaus, 1999; Inamori, Lütkenhaus, & Mayers, 2001; Gottesman, Lo, Lütkenhaus, & Preskill, 2004). However, security against eavesdropping attacks that use non-idealities of optical and electro-optical components in real setups has not been included into the security proof.

Nevertheless, every assumption in a security proof should be explicitly written down and examined. In fact, a number of theoretical eavesdropping attacks have recently been proposed. This thesis will demonstrate experimentally one of those proposed attacks based on the exploitation of the loss of the reflective optical components. This type of attack is not restricted to one particular QKD protocol or scheme since it can allow the eavesdropper to access to the system from outside, through a common optical channel connecting to the sender and the receiver, resulting in gaining the information key without disturbing the system. Hence, this thesis is devoted to how much information the eavesdropper will gain using this type of attack.

1.2 BACKGROUND

Since ancient times, people have sought ways of communicating information relevant to the needs of diplomacy, trade, and military affairs that would ensure the preservation of secret information from third parties.To achieve this, various kinds of coding information need to be applied. These methods provided secrecy of information to some extent, but none of them gave absolute protection. In 1918, Gilbert Vernam proposed a simple “one-time pad” cipher where each symbol of the message was added modulo alphabet size with a symbol of a random secret key to form a ciphertext; on the receiving end, the same operation was used to extract the message (Vernam, 1926). In 1949, Claude Shannon mathematically proved that the security of this cipher was perfect provided the key material was never reused (Shannon, 1949). The perfect security of this cryptosystem exists only on condition that:

1. The key is completely random
2. It is as long as the message itself
3. It is used only once for one single message.

Therefore, before conveying any secret message, it is necessary first to transmit it on a channel which is very well protected from unauthorized access, and it must be of the same length as the message containing the key. Such a system is inconvenient to use, and expensive.

In 1976, Whitfield Diffie and Martin Hellman, proposed the principle of public key cryptography. The idea was to use two different keys – one key for encryption and the other one for decryption. The encryption key is supposed to be spread as widely as possible and does not have to be hidden from any eavesdropper. That is why this key is called “public”. In contrast, the decryption key, called the “private” key, has to be

held by the receiving party in secret and must not be spread, otherwise an eavesdropper will be able to decipher the messages. These two keys must be connected by the means of a one-way function, which will make it easy to compute the public key from the private one, but which will make it extremely hard to do the reverse calculation. Although this principle was invented in 1976, no one at this time knew the one-way function to fulfill these requirements. However, in 1978 Ronald Rivest, Adi Shamir and Leonard Adleman succeeded in finding such a function, which was then implemented in an algorithm known as RSA (Sing, 1999). The security of RSA is actually based on the factorization of large integers to achieve the one-way function. However, it is easy to do the calculation in the difficult direction provided that you have some additional information of the factored integer. Moreover, systems with the public key can lose their effectiveness with the advent of light quantum computers, which have already been developed for rapid factorization algorithms. Therefore, there is a need for cryptographic systems based on other principles.

The work "Conjugate coding" (Wiesne, 1983), which was first noticed by only a few and was not even published, was the beginning of a new direction in cryptographic science - quantum cryptography. By using the laws of quantum mechanics, it has become possible to communicate between two or more parties using a secret key that satisfies all the requirements for the cipher pad, which provide secrecy of the information. In 1984, Bennett and Brassard patented the first protocol for the exchange of quantum cryptographic systems, known as BB84 (Bennett & Brassard, 1984). Since then, interest in quantum cryptography has started to grow very rapidly in the world, and to date a great number of studies have been conducted involving a variety of aspects (example: Quantum memory, Quantum repeaters, Teleportation)

According to the wording of the authors of BB84, quantum cryptography is a system by which two users, who share no secret information. Initially: 1) exchange a random quantum transmission, consisting of very faint flashes of polarized light. 2) by subsequent public discussion of the sent and received versions of this transmission estimate the extent of eavesdropping that might have taken place on it, and finally 3) if this estimate is small enough, distill from the sent and received versions a smaller body of shared random information, which is certifiably secret in the sense that any third party's expected information on it is an exponentially small fraction of one bit (Bennett C. , Bessette, Brassard, Salvail, & Smolin, 1992).

In quantum cryptography, the sender, commonly called Alice, transmits a sequence of photons to the receiver, commonly called Bob, while the person conducting unauthorized access (eavesdropping) is known as "Eve". The Thesis will not deviate from these norms and preserve this terminology in the present work.

1.3 PROBLEM STATEMENT

The principles of quantum mechanics are applied by the quantum cryptosystem to establish a secure key rate. However, relying on the law of quantum physics does not give the QKD system absolute security even with non-ideal components. Moreover, attacking those non-ideal components (i.e.: Phase Modulator) can give the eavesdropper information about the secret key. Since the key rate uses the phase modulator to generate quantum states to represent the bit values 0 & 1, which is called the qubit, the eavesdropper can focus her attack on that particular component to gain information about the key without interacting with the transmitted quantum state to disclose her presence.

1.4 SCOPE OF RESEARCH

The scope of this thesis is to show the full potential of attacking non-ideal components (i.e.: Phase Modulator) and its end result other than intercepting the transmitted quantum states, since most of the work conducted on this type of attack has been theoretical in nature (Chapter 2 will review most of the those works). The proposed experimental setup is going to increase the eavesdropper's information gain about the secret key by up to 90% and the QBER inflected by the attack will not exceed the threshold to disclose her presence. Furthermore, modifications to the proposed experimental set-up will gain the eavesdropper the different four phase shifts, since most QKD systems depend on the phase modulator to generate the BB84 protocol states.

1.5 RESEARCH OBJECTIVES

The objectives of this research can be achieved by acting as an eavesdropper to find a way to gain information about the secret key and then suggest an appropriate solution to counter the eavesdropping strategy. This can be achieved by the following:

1. To design an eavesdropper optical setup to gain information about the two-quantum bit of the QKD system through visibility interference this will also detect the phase drift in the system if it occurs. This will be one of the main contributions of this thesis as the new modification is expected to perform much more efficiently than its predecessors.
2. To develop a strategy to gain the four different phase states as a result of eavesdropping since the phase modulator is applied in the BB84 protocol. This will be the other main contribution of this thesis as the new

modification is expected to perform much more efficiently than its predecessors.

3. To study the effect of the Trojan horse attack on the Quantum Bit Error (QBER) and to ascertain whether the information gained about the key is reliable or not (Fidelity).

1.6 Research Methodology

This research is conducted by looking at the QKD system from eavesdropper prospective to help the security analyst to counter such attack. An experimental optical set-up has been constructed for the transmission and receiver of the quantum key distribution (QKD) system and an experimental setup for eavesdropping onto the QKD system. Quantum cryptography is reliable for detecting an eavesdropper if the attack is focused on the quantum states but has few drawbacks in its optical set-up. The optical set-up for the transmission and the receiver was constructed using optical fiber, a phase modulator, laser source, Faraday mirror, beam splitter, coupler, polarizer and two photon counting detectors and an unbalanced Mach-Zehnder interferometer. Meanwhile, the eavesdropper optical set-up used a coupler, OTDR, laser source, two Photon Counting Detectors, a delay line and a Michelson interferometer to eavesdrop on the QKD system.

Most of the work concentrated on the eavesdropping onto the QKD system. However, some time had to be spend in constructing a QKD optical set-up to achieve eavesdropping onto a practical system. To compare the visibility interference of the QKD system with the eavesdropper and to compute its Quantum Bit Error to establish whether it had reached the threshold because of the attack or disclosed the

eavesdropper's presence. Certain problems were anticipated either from the optical setup or electric-optical components but were handled accordingly.

1.6.1 Procedure

In order to prove the hypothesis of this study, the following procedures are taken:

1. Develop a clear understanding of Quantum Communication to show how it can be used in an effective way to meet the objectives.
2. Investigate the previous work applied to the development of the QKD system and eavesdropping strategies.
3. Implement a QKD optical setup that uses the BB84 protocol.
4. Design an efficient and effective Trojan horse eavesdropping optical set-up that will measure the characteristics of the reflected pulses and determine the different states of the QKD system.

1.6.2 Data Collection and Treatment

At the end of each experiment, the data that has been registered earlier from the attack will be processed to compute its validity. Since there are two processes for this attack, they will be evaluated separately:

1. The First process is to evaluate the different four phase states as a result of eavesdropping into the QKD system to achieve the four states in the BB84 protocol and compare it with the obtained phase shift in the literature review
2. The Second process is to evaluate the eavesdropping by comparing the visibility interference of the QKD optical set-up with the eavesdropper and

whether the QBER of the QKD system exceeded the threshold because of the attack.

These steps will aid in proving the hypothesis, and then those values can be plotted using Origin Pro for further interpretation.

1.7 THESIS ORGANIZATION

This thesis is divided into six chapters. The first chapter, which is the introductory chapter, includes a history and some of the principles of quantum cryptography, the problem statement, objectives, and the research methodology. This chapter provides an in-depth review required to comprehend the concept of quantum cryptography. The literature review is presented in the second chapter in which previous work in the area and its successes will be highlighted. This leads to the third chapter, where we present the security of the best-known protocol, and we compare the performance of quantum cryptography systems implementing these protocols with practical components. The concepts and analysis presented in this chapter and the previous one will be useful for the rest of the thesis. Chapter four caters for the parameters of the Trojan horse attack and proposes the experimental setup and its strategies, whether it will have some effect on the photonic qubit and how the eavesdropper will gain information. In the next chapter, chapter five, we present the obtained results and present their critical analysis. The final chapter includes the conclusion and recommendations for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter will highlight the works related to non-quantum interaction attacks and Trojan horse attack, which is the focus of this thesis. However, only two groups have indicated the significance of the Trojan horse attack and its potential but it had some limitations which will also be highlighted. This chapter will go through the current technology has reached in QKD system. This chapter will introduce the concept of BB84 protocol used in QKD systems, which the attack will focus on. Then it describes the concept of QKD over optical fiber and the difference between the one-way and the two-way system.

2.2 QUANTUM KEY DISTRIBUTION SYSTEM

Quantum cryptography uses quantum states, such as polarizations of single photons, to transmit bits of information. It is impossible to make a perfect copy of an unknown quantum state (Wootters & Zurek, 1982) which prevents an eavesdropper from measuring it accurately. There are many photon pairs polarization with the characteristic, which cannot be precisely measured at the same time, for instance, horizontal and vertical states, diagonal and angular states and left and right circular. The unique characteristics of quantum states inspired Wiesner, in 1983, who proposed using quantum states as a protection mechanism against counterfeit money. He gave the idea that it will be impossible to forge money physically using conventional way