Quantum Encryption System

Developed by

Muhammad Musharraf Ishtiaq Khan

Supervised by

Dr. Muhammad Sher

Department of Computer Science
International Islamic University, Islamabad
(2003)

بسم الله الرحمن الرحيم

**In the name of ALMIGHTY ALLAH,
The most Beneficent, the most
Merciful.**

Department of Computer Science,
International Islamic University, Islamabad.

24 Jan, 2004

Final Approval

It is certified that we have read the thesis, titled "**Quantum Encryption System**" submitted by **Muhammad Musharraf Ishtiaq Khan** under University Reg. No. **10-CS/MS/01**. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University, Islamabad, for the Degree of **Master of Science**.

Committee

External Examiner
Dr. Abdus Sattar
Consultant Multimedia Center,
Department of Computer Science,
Allam Iqbal Open University, Islamabad

Internal Examiner
Mr. Zaheer Aziz
Assistant Professor,
Department of Computer Science,
International Islamic University, Islamabad.

Supervisor
Dr. Muhammad Sher
Assistant Professor,
Department of Computer Science,
International Islamic University, Islamabad.

24/01/04

Dedication

Dedicated to The Holy Prophet Muhammad (SAW) and to my family.

A dissertation submitted to the
Department of Computer Science,
International Islamic University, Islamabad
as a partial fulfillment of the requirements
for the award of the degree of
Master of Science

Declaration

I hereby declare that this software, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that I have developed this software entirely on the basis of my personal efforts made under the sincere guidance of our teachers. No portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Muhammad Musharraf Ishtiaq Khan
10-CS/MS/01

Acknowledgements

All praise to the Almighty Allah, the most Merciful, the most Gracious, without whose help and blessings, I was unable to complete the project.

Thanks to my Parents who helped me during my most difficult times and it is due to their unexplainable care and love that I am at this position today.

Thanks to my project supervisor Dr. Muhammad Sher, his sincere efforts helped me to complete my project successfully.

I acknowledge teachers and friends for their help in the project.

Muhammad Musharraf Ishtiaq Khan

Project in Brief

Project Title:	Quantum Encryption System
Objective:	To Develop a Key Distribution protocol based on laws of Quantum Mechanics.
Undertaken By:	**Muhammad Musharraf Ishtiaq Khan**
Supervised By:	**Dr. Muhammad Sher** Assistant Professor, Department of Computer Science, International Islamic University, Islamabad.
Technologies Used:	Microsoft® Visual C++ .NET, LaTex
System Used:	Pentium® III
Operating System Used:	Microsoft® Windows® XP Professional
Date Started:	1st December, 2002
Date Completed:	14th August, 2003

Abstract

The contest between code-makers and code-breakers has been going on for thousands of years. Recently, quantum mechanics has made a remarkable entry in the field of data communication. On the one hand, it is generally accepted that quantum cryptography can provide absolute security for communications between two users. On the other hand, code-breakers in possession of a quantum computer can easily break popular encryption schemes such as RSA and Data encryption Standard (DES) which are essentially intractable by any classical computer. This thesis report describes the working and implementation of a Quantum Key Distribution protocol that we have developed to securely share a key between two users. Our scheme uses entangled photon pairs in random polarizations. In this scheme, four local unitary operations and the Bell state measurement are used. The non requirement of classical channel and random selection of polarization basis make this protocol perfectly secure. We also have tested this scheme against known eavesdropping strategies.

TABLE OF CONTENTS

Chapter 1

Introduction

1. Introduction

Secure transmission of information has always been a subject under discussion. Especially in military applications, its importance is well-known. With the proliferation on internet and electronic mail, the importance of achieving secrecy in communications by cryptography–the art of using coded messages–is growing each day. Since an encryption scheme is only as secure as its key, key distribution is a big problem in conventional cryptography. Public-key based key distribution schemes such as the Diffie-Hellman [1] scheme solve the key distribution problem by making computational assumptions such as that the discrete logarithm problem is hard. However, unexpected future advances in algorithms and hardware (e.g., the construction of a quantum computer [2, 3]) may render many public-key based schemes insecure. Worse still, this would lead to a retroactive total security break with disastrous consequences. A big problem in classical public-key cryptography is that there is, in principle, nothing to prevent an eavesdropper with infinite computing power from passively monitoring the key distribution channel and thus successfully decoding any subsequent communication.

Recently, the quantum mechanics has made a remarkable entry in the field of cryptography (The subject of quantum cryptography was started by S. Wiesner [4] in a paper that was written in about 1970 but remained unpublished until 1983). It has been claimed that quantum encryption can solve many issues in data communication that are infeasible from the prospective of conventional cryptography. In quantum mechanics, measurement is not just a passive, external process, but an integral part of the formalism. Indeed, thanks to the quantum no-cloning theorem [5, 6], passive monitoring of unknown transmitted signals is strictly forbidden in quantum mechanics. Moreover, an eavesdropper who is listening to a channel in an attempt to learn information about quantum states will almost always introduce disturbance in the transmitted quantum signals [7]. Such disturbance can be detected with high probability by the legitimate users.

of an encryption/decryption algorithm which is a trapdoor function. As a result, recovering the decryption key from the encryption key is computationally infeasible. The RSA public key cryptographic system is believed to be an example of such a cryptographic system.

One major drawback to public key cryptographic systems is that no one has yet been able to prove that practical trapdoor functions exist. As a result, no one is really sure how secure such public key cryptographic systems are. Moreover, if researchers succeed in building a feasible quantum computer, Shore's quantum factoring algorithm [8] could break RSA easily, i.e., in polynomial time.

Yet another drawback to public key cryptographic systems is that, in terms of some everyday implementations, such systems frequently do not circumvent the catch 22 of conventional cryptography after all. The keys for many practical public key cryptographic systems are frequently managed by a key bank that is independent of Ali and Bina. Thus, secret communications over a secure channel from the key bank to Ali and Bina are required before Ali and Bina can secretly communicate.

1.2 Quantum cryptography

Quantum cryptography is a means of transmitting an encryption key in a way that guarantees no eavesdropping.

Quantum encryption guarantees no eavesdroppers because it transmits the key as a series of photons (hence the "quantum" part). And photons, as Heisenberg tells us, cannot be observed without altering them. Therefore, any attempt to eavesdrop on the exchange of the key will corrupt it and make it useless.

So if two parties—Ali and Bina—want to exchange a message, then Ali could begin generating randomly polarized photons (each representing a bit) and send them to Bina. Bina then encrypts the message using the value of those photons as the key and sends it to Ali, but first she verifies with Ali that key was uncompromised with a method that cannot be used by Iblees to deduce anything useful (like a checksum or, in practice, a report of the positions in a stream of photons where Bina's randomly polarized receiver was in "agreement" with the polarization of the photon Ali was transmitting). If the key was intercepted on the way by Iblees, then the act of doing so would alter the key and the checksum of Bina's copy wouldn't match Ali's. So if the checksum didn't match, then they could keep trying new keys until Iblees gave up.

The message, once a "safe" key has been confirmed, is uncrackable as long as the photons were sufficiently random.

A variation of quantum cryptography is to use entanglement instead. Entanglement is a phenomena where observing the spin of one particle will set the spin of its entangled cousin—no matter how great the distance they've been separated by (and instantaneously, too, defying the limit of the speed of light). In this case, Iblees has no information to intercept because the value of the entangled particle hasn't been set until it has arrived at its destination and been observed.

1.3 Project scope

As discussed earlier, quantum cryptography provides a unique mechanism for secure data transmission. The first quantum key distribution protocol was proposed by C. H. Bennett and G. Brassard in 1984 (so called BB84 protocol [9]). Since then, several quantum key distribution protocols have been established. Most of the protocols utilize two channels for transmission, a classical unjammable communication channel and a quantum communication channel. However, it is believed that an unjammable classical channel is, in principle, very difficult to achieve

The scope of this project is to develop a quantum key distribution (QKD) scheme based on quantum entanglement. The polarization basis for this entanglement is selected at random. The sender generates pairs of entangled particles and sends one particle from each pair to the receiver. Both sender and receiver randomly and independently execute some unitary transformations on the particle they possess. Finally, a measurement is made on the sender's side to check for possible eavesdropping. This scheme doesn't require any classical public channel. The delicate nature of entanglement along with random selection of basis guarantees that no adversary party can get the key.

Key features include:

- Randomization of polarization bases
- Communication over quantum media (Optical fiber)
- Synchronization between communicating parties
- Variable length data
- Non-requirement of classical channel
- Intrusion detection
- Implementation of several eavesdropping strategies

1.4 Objectives

The objective of this project is to develop a security system based of quantum laws of physics which provides efficient key distribution mechanism. The communicating parties will be able to share a secure key of any length they desire. Intrusion detection is provided which is not found in any other cryptographic system. Some well-known eavesdropping strategies are also taken into consideration.

Chapter 2

Theoretical Background

2. Theoretical Background

Quantum mechanics have provided us with a new approach towards data encryption. In this chapter, we will study the basics of quantum mechanics, its novel properties and some unique features which are missing in its classical counter part.

2.1 Quantum information processing

The foundations of an information processing theory can be constructed by the following procedure:

1. Define the basic unit of information.

2. Give the means for processing one unit.

3. Describe how multiple units can be combined.

4. Give the means for processing multiple units.

5. Show how to convert the content of any of the extant units to classical information.

Note that the last step is not required for classical information processing.

In this section, we follow the general procedure for defining an information processing theory to introduce quantum information processing.

2.1.1 The Quantum Bit

The fundamental resource and basic unit of quantum information is the quantum bit (qubit), which behaves like a classical bit enhanced by the superposition principle. From a physical point of view, a qubit is represented by an ideal two-state quantum system. Examples of such systems include photons (vertical, horizontal and circular polarization), electrons and other spin-½ systems (spin up and down), and systems defined by two energy levels of atoms or ions. From the beginning the two-state system played a central role in studies of quantum mechanics. It is the most simple quantum system, and in principle all other quantum systems can be modeled in the state space of collections of qubits.

From the information processing point of view, a qubit's state space contains the two 'logical', or 'computational', states $|0\rangle$ and $|1\rangle$. The so-called 'ket' notation for these states was introduced by P. Dirac, and its variations are widely used in quantum physics. One can think of the pair of symbols '$|$' and '$\rangle$' as representing the qubit system. Their content specifies a state for the system. In this context 0 and 1 are system-independent state labels. When, say, 0 is placed within the ket, the resulting expression $|0\rangle$ represents the corresponding state of a specific qubit.

The initial state of a qubit is always one of the logical states. Using operations to be introduced later, we can obtain states which are 'superposition' of the logical states. Superposition can be expressed as sum $\alpha|0\rangle+\beta|1\rangle$ over the logical states with complex coefficients. The complex numbers α and β are called the 'amplitudes' of the superposition. The existence of such superposition of distinguishable states of quantum systems is one of the basic tenets of quantum theory called the 'superposition principle'. Another way of writing a general superposition is as a vector

$$\alpha|0\rangle+\beta|1\rangle \leftrightarrow \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{2.1}$$

The qubit states that are superpositions of the logical states are called 'pure' states: A superposition $\alpha|0\rangle+\beta|1\rangle$ is a pure state if the corresponding vector has length 1, that is $|\alpha|^2+|\beta|^2=1$. Such a superposition or vector is said to be 'normalized'. (For a complex number given by $\gamma=x+\iota y$, one can evaluate $|\gamma|^2=x^2+y^2$. Here, x and y are the real and imaginary part of γ, and the symbol ι is a square root of -1, that is, ι^2 = -1. The conjugate of γ is $\bar{\gamma}=x-\iota y$. Thus $|\gamma|^2=\gamma\bar{\gamma}$.) Here are a few examples of states given in both the ket and the vector notation:

$$|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \leftrightarrow \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \tag{2.2}$$

$$|\psi_2\rangle = \frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle \leftrightarrow \begin{pmatrix} 3/5 \\ -4/5 \end{pmatrix} \tag{2.3}$$

$$|\psi_3\rangle = \imath\frac{3}{5}|0\rangle - \imath\frac{4}{5}|1\rangle \leftrightarrow \begin{pmatrix} \imath 3/5 \\ -\imath 4/5 \end{pmatrix} \tag{2.4}$$

The state $|\psi_3\rangle$ is obtained from $|\psi_2\rangle$ by multiplication with $\imath$. It turns out that two states cannot be distinguished if one of them is obtained by multiplying the other by a 'phase' $e^{\imath\theta}$.

2.1.2 The probabilistic bit

The superposition principle for quantum information means that we can have states that are sums of logical states with complex coefficients. There is another, more familiar type of information whose states are combinations of logical states. The basic unit of this type of information is the probabilistic bit (pbit). Intuitively, a pbit can be thought of as representing the as-yet-undetermined outcome of a coin flip. Since we need the idea of probability to understand how quantum information converts to classical information, we briefly introduce pbits.

A pbit's state space is a probability distribution over the states of a bit. One very explicit way to symbolize such a state is by using the expression {p:0; (1-p):1}, which means that the pbit has probability p of being 0 and 1 - p of being 1. Thus a state of a pbit is a 'probabilistic' combination of the two logical states, where the coefficients are nonnegative real numbers summing to 1. A typical example is the unbiased coin in the process of being flipped. If 'tail' and 'head' represent 0 and 1, respectively, the coin's state is $\left\{\frac{1}{2}:0, \frac{1}{2}:1\right\}$. After the outcome of the flip is known, the state 'collapses' to one of the logical states 0 and 1. In this way, a pbit is converted to a classical bit. If the pbit is probabilistically correlated with other pbits, the collapse associated with learning the pbit's logical state changes the overall probability distribution by a process called 'conditioning on the outcome'.

A consequence of the conditioning process is that we never actually 'see' a probability distribution. We only see classical deterministic bit states. According to the frequency interpretation of probabilities, the original probability distribution can only be inferred after one looks at many independent pbits in the same state $\{p:0; (1-p):1\}$: In the limit of infinitely many pbits, p is given by the fraction of pbits seen to be in the state 0. As we will explain, we can never 'see' a general qubit state either. For qubits there is a process analogous to conditioning. This process is called 'measurement' and converts qubit states to classical information.

What is the difference between bits, pbits and qubits? One way to visualize the difference and see the enrichment provided by pbits and qubits is shown in Figure 2.1.

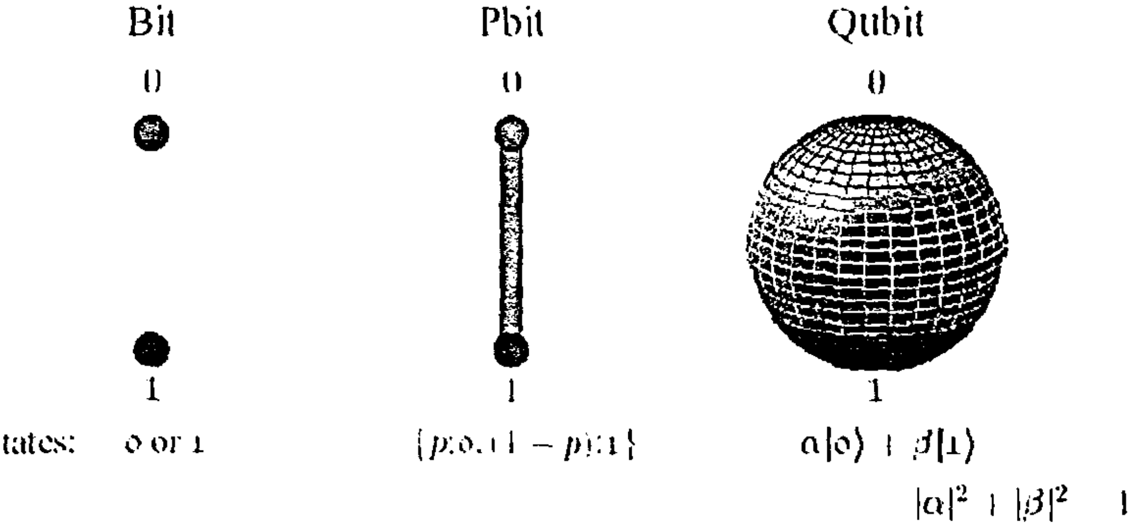

Bit
Pbit
Qubit
0
0
0
1
1
1
States:
0 or 1
$\{p:0, (1-p):1\}$
$\alpha|0\rangle + \beta|1\rangle$
$|\alpha|^2 + |\beta|^2 = 1$

Figure 2.1 Visual comparison of the state spaces of different information units.

2.1.3 Two Quantum Bits

Some states of two quantum bits can be symbolized by the juxtaposition (or multiplication) of states of each quantum bit. In particular, the four logical states $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$ are acceptable pure states for two quantum bits. In these expressions, we have distinguished the qubits by position (first or second). It is easier to manipulate state expressions if we explicitly name the qubits, say A and B. We can then distinguish the kets by writing, for example, $|\psi\rangle_A$ for a state of qubit A. Now the state $|0\rangle|1\rangle$ can be written with explicit qubit names (or 'labels') as

$$|0\rangle_A|1\rangle_B = |1\rangle_B|0\rangle_A = |01\rangle_{AB} = |10\rangle_{BA} \tag{2.5}$$

Having explicit labels allows us to unambiguously reorder the states in a product of states belonging to different qubits. We say that kets for different qubits 'commute'.

So far we have seen four states of two qubits, which are the logical states that correspond to the states of two bits. As in the case of one qubit, the superposition principle can be used to get all the other pure states. Each state of two qubits is therefore of the form

$$\alpha|00\rangle_{AB} + \beta|01\rangle_{AB} + \gamma|10\rangle_{AB} + \delta|11\rangle_{AB} \tag{2.6}$$

where α, β, γ and δ are complex numbers. Again, there is a column vector form for the state:

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} \tag{2.7}$$

and this vector has to be of unit length, that is $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$

Other examples of two-qubit states in ket notation are the following:

$$|\psi_1\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A + |1\rangle_B\right)|1\rangle_B \tag{2.8}$$

$$\begin{aligned} |\psi_2\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|0\rangle_A - |1\rangle_A\right)\frac{1}{\sqrt{2}}\left(|0\rangle_B + i|1\rangle_B\right) \\ &= \frac{1}{2}\left(|00\rangle_{AB} + i|01\rangle_{AB} - |10\rangle_{AB} - i|11\rangle_{AB}\right) \end{aligned} \tag{2.9}$$

$$|\psi_3\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right) \tag{2.10}$$

$$|\psi_4\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right) \tag{2.11}$$

The first two of these states have the special property that they can be written as a product $|\phi_1\rangle_A|\phi_2\rangle_B$ of a state of qubit A and a state of qubit B. The second expression for $|\psi\rangle_2$ shows that the product decomposition is not always easy to see. Such states are called 'product' states. The last two states, $|\psi_3\rangle_{AB}$ and $|\psi_4\rangle_{AB}$ are two of the famous Bell states. They have no such representation as a product of independent states of each qubit. They are said to be 'entangled' because they contain a uniquely quantum correlation between the two qubits. Pbits can also have correlations that cannot be decomposed into product states, but the entangled states have additional properties that make them very useful. For example, if Alice and Bob each have *one* of the qubits that together are in the state $|\psi_3\rangle_{AB}$, they can use them to create a secret bit for encrypting their digital communications.

2.1.4 Processing qubits

The quantum version of the not gate for bits exchanges the two logical states. That is, using ket notation,

$$\text{not}\left(\alpha|0\rangle+\beta|1\rangle\right)=\alpha|1\rangle+\beta|0\rangle=\beta|0\rangle+\alpha|1\rangle \qquad (2.12)$$

In vector notation this equation becomes

$$\text{not}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ \alpha\end{pmatrix} \qquad (2.13)$$

Another way of expressing the effect of not is by multiplying the vector by a matrix representing not:

$$\text{not}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ \alpha\end{pmatrix} \qquad (2.14)$$

so that we can identify the action of not with the matrix $\sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. An even simpler gate is the one that does nothing. We call this the noop gate, and its matrix form is the identity matrix as shown in the following equation:

$$\text{noop}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{2.15}$$

The noop and not gates are 'reversible'. In other words, we can undo their actions by applying other gates. For example, the action of the not gate can be undone by another not gate. The action of every reversible quantum gate can be represented by matrix multiplication, where the matrix has the additional property of preserving the length of vectors. Such matrices are called 'unitary' and are characterized by the equation $A^{\dagger}A=I$, where $A^{\dagger}$ is the conjugate transpose of A and I is the identity matrix. (The conjugate transpose of a matrix is computed by flipping the matrix across the main diagonal and conjugating the complex numbers.) For gates represented by a matrix, the unitarity condition is necessary and sufficient for ensuring that pure states get mapped to pure states.

The ket notation can be extended so that we can write gates in a compact form that readily generalizes to multiple qubits. To do so we have to introduce expressions such as $\langle\psi|=\alpha\langle 0|+\beta\langle 1|$. This is called the 'bra' notation. The terminology comes from the term 'bracket': The 'bra' is the left and the 'ket' is the right part of a matched pair of brackets. From the vector point of view, $\langle\psi|$ corresponds to the row vector (α, β). Note that a column vector multiplied by a row vector yields a matrix. In the bra-ket notation, this corresponds to multiplying a ket $|\psi\rangle$ by a bra $\langle\phi|$, written as $|\psi\rangle\langle\phi|$. Since this represents an operator on states, we expect to be able to compute the effect of $|\psi\rangle\langle\phi|$ on a state $|\varphi\rangle$ by forming the product.

The simplest way of modifying the state of two qubits is to apply one of the one-qubit gates. If the gates are expressed in the bra-ket notation, all we need to do is add qubit labels so that we know which qubit each bra or ket belongs to. For example, the not gate for qubit B is written as

$$\text{not}^{(B)}=|0\rangle_B\,{}^{B}\langle 1|+|1\rangle_B\,{}^{B}\langle 0| \tag{2.16}$$

The labels for bra expressions occur as left superscripts.

2.1.5 Qubit Measurements

In order to classically access information about the state of qubits we use the measurement operation meas. This is an intrinsically probabilistic process that can be applied to any extant qubit. For information processing, one can think of meas as a subroutine or function that returns either 0 or 1 as output. The output is called the 'measurement outcome'. The probabilities of the measurement outcomes are determined by the current state. The state of the qubit being measured is 'collapsed' to the logical state corresponding to the outcome. Suppose we have just one qubit, currently in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Measurement of this qubit has the effect

$$\text{meas}\left(\alpha|0\rangle+\beta|1\rangle\right)=\begin{cases}0:|0\rangle \text{ with probability } |\alpha|^2\\ 1:|1\rangle \text{ with probability } |\beta|^2\end{cases} \tag{2.17}$$

The classical output is given before the new state for each possible outcome. This measurement behavior explains why the amplitudes have to define unit length vectors: Up to a phase, they are associated with square roots of probabilities.

For two qubits the process is more involved. Because of possible correlations between the two qubits, the measurement affects the state of the other one too, similar to conditioning for pbits after one 'looks' at one of them. As an example, consider the state

$$|\psi\rangle_{AB}=\frac{2}{3}|01\rangle_{AB}+\frac{i2}{3}|10\rangle_{AB}+\frac{1}{3}|00\rangle_{AB} \tag{2.18}$$

To figure out what happens when we measure qubit *A*, we first rewrite the current state in the form $\alpha|0\rangle_A|\phi_0\rangle_B+\beta|1\rangle_A|\phi_1\rangle_B$, where $|\phi_0\rangle_B$ and $|\phi_1\rangle_B$ are pure states for qubit *B*. It is always possible to do that. For the example of (2.18):

$$\begin{aligned}|\psi\rangle_{AB}&=\frac{2}{3}|0\rangle_A|1\rangle_B+\frac{1}{3}|0\rangle_A|0\rangle_B+\frac{i2}{3}|1\rangle_A|0\rangle_B\\&=|0\rangle_A\left(\frac{2}{3}|1\rangle_B+\frac{1}{3}|0\rangle_B\right)+|1\rangle_A\frac{i2}{3}|0\rangle_B\\&=\frac{\sqrt{5}}{3}|0\rangle_A\left(\frac{1}{\sqrt{5}}|0\rangle_B+\frac{2}{\sqrt{5}}|1\rangle_B\right)+\frac{i2}{3}|1\rangle_A\left(|0\rangle_B\right)\end{aligned} \tag{2.19}$$

so $\alpha = \frac{\sqrt{5}}{3}, \beta = \frac{\iota 2}{3}, |\phi_0\rangle_B = \frac{1}{\sqrt{5}}|0\rangle_B + \frac{2}{\sqrt{5}}|1\rangle_B$ and $|\phi_1\rangle_B = |0\rangle_B$. The last step required pulling out the factor of $\frac{\sqrt{5}}{3}$ to make sure that $|\phi_0\rangle_B$ is properly normalized for a pure state. Now that we have rewritten the state, the effect of measuring qubit A can be given as follows:

$$\text{meas}^{(A)}\ \left(\alpha|0\rangle_A|\phi_0\rangle_B + \beta|1\rangle_A|\phi_1\rangle_B\right) = \begin{cases} 0: |0\rangle_A|\phi_0\rangle_B \text{ with probability } |\alpha|^2 \\ 1: |1\rangle_A|\phi_1\rangle_B \text{ with probability } |\beta|^2 \end{cases} \tag{2.20}$$

For the example, the measurement outcome is 0 with probability $\frac{5}{9}$, in which case the state collapses to $|0\rangle_A\left(\frac{1}{\sqrt{5}}|0\rangle_B + \frac{2}{\sqrt{5}}|1\rangle_B\right)$. The outcome is 1 with probability $\frac{4}{9}$, in which case the state collapses to $|1\rangle_A|0\rangle_B$. The probabilities add up to 1 as they should.

2.2 Novel properties of quantum information

The essence of quantum cryptography can be understood by considering a single question: given a single photon in one of the four possible polarizations: horizontal, vertical, 45 degrees and 135 degrees, can we distinguish between these four possibilities with certainly? Surprisingly, the answer is no. This is due to the novel properties of quantum information. First, there is a physical law in quantum mechanics known as the quantum no-cloning theorem which states that an unknown quantum state cannot be cloned. Second, given a quantum system prepared in one of two prescribed non-orthogonal states, any attempt to distinguish between the two possibilities necessarily leads to disturbance. Third, a measurement on an arbitrary unknown quantum state is an irreversible process which introduces disturbance to the state. As a result of these three properties, passive monitoring of quantum signals is impossible. Therefore, eavesdropping on quantum channels necessarily disturbs the signal and is exceedingly likely to be detected. In what follows, we will discuss these three properties in more detail.

2.2.1 Quantum No-cloning theorem

Owing to the linearity of quantum mechanics, there is a quantum no-cloning theorem which states that an unknown quantum state cannot bc copied. Andy Steane says: "Even though one can clone a sheep, one cannot clone a single photon. The proof of this theorem is given in Appendix-A. This theorem provides the foundation of the concept that passive monitoring of quantum signals is not possible. Obviously, if one is not allowed to make copies, one will make use of original piece and, if disturbed, will remain in its state until detected by authenticated user.

2.2.2 Information gain implies disturbance

Another unusual property of quantum mechanics is that, in any attempt to distinguish between two non-orthogonal states, information gain is possible only at expense of introducing disturbance to the signal. A proof by contradiction is given in Appendix-B. These two properties—the quantum no-cloning theorem and the tradeoff between *information gain and disturbance*—imply that, given a photon in one of the four polarizations (horizontal, vertical, 45 degrees and 135 degrees), there is no way to distinguish between four possibilities with certainty.

2.2.3 Irreversibility of measurements

We might think that we make a measurement and copies the result of that measurement. But this is not possible because the measurement will disturb the state of the signal. Consequently, the result of a measurement is different from the initial state and copying will be unfaithful. To understand this point, we will consider a photon in one of its four possible polarizations. A birefringent calcite crystal can be used to detect and distinguish with certainty between horizontally and vertically polarized photons. If a horizontally polarized beam of light is passed through this crystal, then the photons pass straight through it. On the other hand, if we pass a vertically polarized beam of light, then the photons are deflected to a new path. This fact is shown in Figure. 2.2(a) and Figure. 2.2(b). Photons originally in these two polarizations are, therefore, deterministically routed. However, a beam of light polarized at some other direction experiences a different behavior. According to the law of quantum mechanics, the photons with such polarization will have some probability of going into either beam (Figure. 2.2(c)). A photon will then be repolarized according to which beam it goes into and permanently forget its original polarization. For instance, a diagonally (i.e., 45-degree or 135-degree) polarized photon is equally likely to go into either beam, revealing nothing about its original polarization.

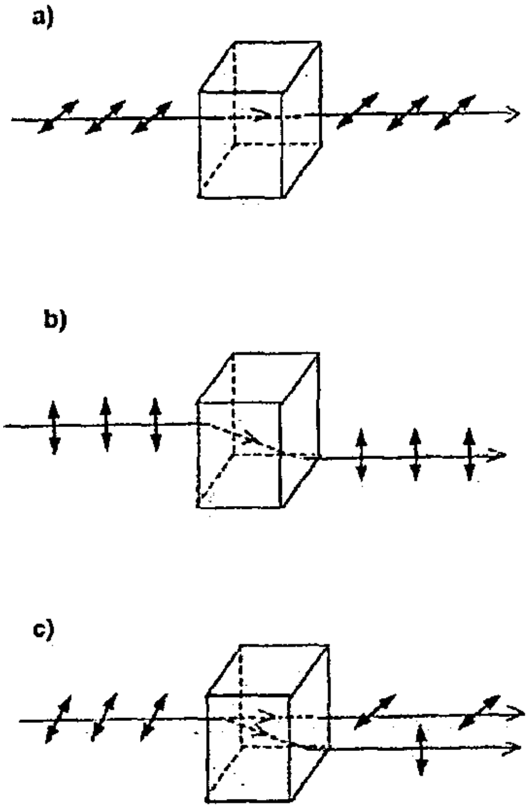


Figure 2.2 A calcite crystal is used to distinguish between horizontal and vertical photons.

(a) Horizontally polarized photons pass straight through.

(b) Vertically polarized photons are deflected to a new path.

(c) Diagonally polarized photons will have equal probability of coming our vertically or horizontally polarized.

We can setup an apparatus to distinguish rectilinear (horizontal or vertical) photons by adding two detectors, such as photomultiplier tubes that can record single photons along the two paths, to the calcite crystal. By using this apparatus, an observer can reliably distinguish between the two possibilities. This set up will, however, randomize the polarizations of diagonal (45- or 135-degree) photons, thus failing to distinguish between the two possibilities. In order to distinguish between diagonal photons, one should rotate the whole apparatus (calcite crystal and detectors) by 45 degrees. The rotated apparatus is, however, powerless in distinguishing between vertical and horizontal photons.

We can conclude from the above discussion that for a photon in one of the four polarizations (horizontal, vertical, 45-degree and 135-degree), a process of measure-and-copy will disturb the signal and fail to distinguish between the four possibilities. A measurement that distinguishes rectilinear photons will disturb diagonal photons. Similarly, a measurement that distinguishes diagonal photons will disturb rectilinear photons. This fundamental limitation in distinguishing between non-orthogonal states is due to the basic principles of quantum mechanics and thus it applies only to the particular measuring apparatus described here, but also to any measuring apparatus.

2.3 Quantum entanglement and Bell's theorem

In the world of microscopic objects described by quantum mechanics, things are not always so simple. Imagine an atom which might undergo a radioactive decay in a certain time, or it might not. We might expect that with respect to the decay, there are only two possible states here: 'decayed', and 'not decayed', just as we had two states, 'fired' and 'not fired' for the gun or 'alive' and 'dead' for the teller. However, in the quantum mechanical world, it is also possible for the atom to be in a combined state 'decayed-not decayed' in which it is neither one nor the other but somewhere in between. This is called a 'superposition' of the two states, and is not something we normally expect of classical objects like guns or tellers. Two atoms may be correlated so that if the first has decayed, the second will also have decayed, and if the first atom has not decayed, neither has the second. This is a 100% correlation. But the quantum mechanical atoms may also be correlated so that if the first is in the superposition 'decayed-not decayed', the second will be also. Quantum mechanically there are more correlations between the atoms than we would expect classically. This kind of quantum 'super-correlation' is called 'entanglement'.

The problem was brought into focus by a famous paper in 1935 by Einstein, Podolsky and Rosen, who argued that the strange behaviour of entanglement meant that quantum mechanics was an incomplete theory, and that there must be what came to be known as 'hidden variables' not yet discovered. This produced a famous debate between Einstein and Niels Bohr, who argued that quantum mechanics was complete, and that Einstein's problems arose because he tried to interpret the theory too literally.

However in 1964, John Bell pointed out that for certain experiments classical hidden variable theories made different predictions from quantum mechanics. In fact he published a theorem which quantified just how much more strongly quantum particles were correlated than would be classically expected, even if hidden variables were taken into account. This made it possible to test whether quantum mechanics could be accounted for by hidden variables. A number of experiments were performed, and the result is almost universally accepted to be fully in favor of quantum mechanics. Therefore there can be no 'easy' explanation of the entangled correlations. The only kind of hidden variables not ruled out by the Bell tests would be 'non-local', meaning they would be able to act instantaneously across a distance.

Chapter 3

Existing Work

3. Existing Work

In this chapter we briefly describe the work already done in the field of quantum cryptography.

3.1 The BB84 quantum cryptographic protocol

BB84 protocol was proposed by Bennett and Brassard [9] in 1984. It is the first well known quantum cryptographic protocol. This protocol has been experimentally demonstrated to work for a transmission over 30 km of fiber optic cable [12], and also over free space for a distance of over one hundred meters [13, 14]. Experiments for ground to satellite communication are also underway. It is speculated, but not yet experimentally verified, that the BB84 protocol should be implement able over distances of at least 100 km. We now describe the BB84 protocol in terms of the polarization states of a single photon.

Let H be the two dimensional Hilbert space whose elements represent the polarization states of a single photon. We can make use of two different orthogonal bases of H, namely circular polarization basis and linear polarization basis. The circular polarization basis consists of the kets $|\curvearrowright\rangle$ and $|\curvearrowleft\rangle$ for right and left circular polarization states, respectively. The linear polarization basis consists of the kets $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ for vertical and horizontal linear polarization states, respectively.

The BB84 protocol utilizes any two incompatible orthogonal quantum alphabets in the Hilbert space H. Let $A_{\circledcirc}$ be the circular polarization quantum alphabet and $A_{\oplus}$ be the linear polarization quantum alphabet, as shown in Table 3.1 and Table 3.2, respectively.

Table 3.1 Circular Polarization Quantum Alphabet $A_{\circledcirc}$

Symbol	*Bit*
$|\curvearrowright\rangle$	1
$|\curvearrowleft\rangle$	0

Table 3.2 Linear Polarization Quantum Alphabet $A_{\oplus}$

Symbol	*Bit*
$\lvert\updownarrow\rangle$	1
$\lvert\leftrightarrow\rangle$	0

Let us suppose that a key exchange is going to take place between two parties namely Ali and Bina, and this communication is threatened by Iblees—an eavesdropper. To assure the detection of Iblees's eavesdropping, Bennett and Brassard require Ali and Bina to communicate in two steps, the first step over a one way quantum communication channel from Ali to Bina, the second step over a two way public communication channel.

3.1.1 Communication over a quantum channel

Ali randomly selects, each time he sends a bit, one of the two orthogonal alphabets $A_{\circledcirc}$ or $A_{\oplus}$ with equal probability. Since no measurement operator of $A_{\circledcirc}$ is compatible with any measurement operator of $A_{\oplus}$, it follows from the Heisenberg uncertainty principle that no one, not even Bina or Iblees, can receive Ali's transmission with an accuracy of greater than 75%, i.e. the minimum error rate is ¼.

With the knowledge put forward earlier, a measurement that distinguishes linear photons will disturb circular photons. Similarly, a measurement that distinguishes circular photons will disturb linear photons. This shows that $A_{\circledcirc}$ and $A_{\oplus}$ are incompatible, and because of this incompatibility, there is no simultaneous measurement operator for both $A_{\circledcirc}$ and $A_{\oplus}$. Since one has no knowledge of Ali's secret choice of quantum alphabet, 50% of the time (i.e., with probability ½) one will guess correctly, i.e., choose a measurement operator compatible with Ali's choice, and 50% of the time (i.e., with probability ½) one will guess incorrectly. A correct guess means Ali's transmitted bit is received with probability 1. On the other hand, an incorrect guess means Ali's transmitted bit is received correctly with probability ½. Thus in general, the probability of correctly receiving Ali's transmitted bit is

$$P = \tfrac{1}{2} \cdot 1 + \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{3}{4} \qquad (3.1)$$

Let λ be the probability of Iblees's eavesdropping, $0 \le \lambda \le 1$. Therefore, if Iblees is not eavesdropping, then the probability will be $1 - \lambda$. Thus, if $\lambda = 1$, Iblees is eavesdropping on each transmitted bit, and if $\lambda = 0$, Iblees is not eavesdropping at all.

As discussed earlier, both Bina and Iblees have no knowledge of Ali's choice of alphabet. Also, the measurement operators they choose are stochastically independent of each other. Therefore Iblees's eavesdropping has an immediate and detectable impact on Bina's received bits. Iblees's eavesdropping causes Bina's error rate to jump from ¼ to $\tfrac{1}{4}(1 - \lambda) + (3/8)\lambda = \tfrac{1}{4} + \lambda/8$

Thus, if Iblees eavesdrops on every bit, i.e., if $\lambda = 1$, then Bina's error rate jumps from ¼ to 3/8, a 50% increase.

3.1.2 Communication over a public channel

Ali and Bina communicate in two phases over a public channel to check for Iblees's presence by analyzing Bina's error rate.

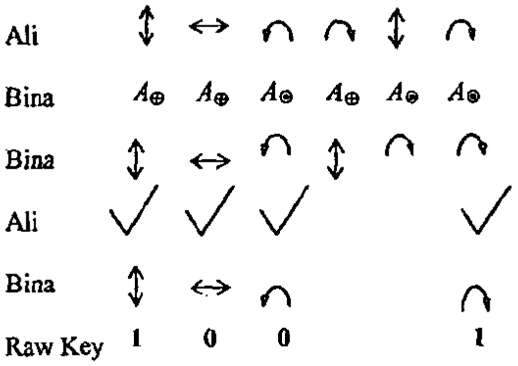


Figure 3.1 Determination of Key using BB84 protocol.

Extraction of raw key

This step is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Iblees's eavesdropping (See Figure 3.1). Bina publicly communicates to Ali which measurement operators (not the results) she used for each of the received bits. Ali then in turn publicly communicates to Bina to tell her which of her measurement operator choices were correct. After this two way communication, Ali and Bina delete the bits corresponding to the incompatible measurement choices for which they can start over again later to communicate these bits securely. The sequence of bits obtained after deletion is known as the raw key. Both Ali and Bina have their own raw key which may differ with each other.

If there is no intrusion, then Ali's and Bina's raw keys will be in total agreement. However, if Iblees has been at work, then corresponding bits of Ali's and Bina's raw keys will not agree with probability

$$0 \cdot (1 - \lambda) + \tfrac{1}{4} \cdot \lambda = \lambda/4 \tag{3.2}$$

Detection of external intrusion via error detection

This step is dedicated to check for external intrusion e.g., Iblees's presence. Ali and Bina select a publicly agreed upon random subset of m bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed. In the absence of noise, if a comparison reveals an inconsistency, then Iblees's eavesdropping has been detected, in which case Ali and Bina return to step 1 and start over. On the other hand, if no inconsistencies are uncovered, then the probability that Iblees escapes detection is:

$$P_{\text{false}} = (1 - \lambda/4)^{m} \tag{3.3}$$

For example, if $\lambda = 1$ and $m = 200$, then

$$P_{\text{false}} = (\tfrac{3}{4})^{200} \approx 10^{-25} \tag{3.4}$$

Thus, if P_{false} is sufficiently small, Ali and Bina agree that Iblees has not eavesdropped, and accordingly adopt the remnant raw key as their final secret key.

3.2 The BB84 quantum cryptographic protocol with noise

In this section, the BB84 protocol is extended to a noisy environment. Since, in a noisy environment, Ali and Bina can not distinguish between error caused by noise and error caused by Iblees's eavesdropping, they must and do adopt the assumption that all errors in raw key are caused by Iblees.

As before, there are two stages to the protocol.

3.2.1 Communication over a quantum channel

This stage is exactly the same as before, except that errors are now also induced by noise.

3.2.2 Communication over a public channel

Ali and Bina communicate over a public channel in four phases. Phase 1 is dedicated to raw key extraction, phase 2 to error estimation, phase 3 to reconciliation, i.e., to reconciled key extraction, and phase 4 to privacy amplification, i.e., extraction of final secret key.

Extraction of raw key

This stage is the same as before, except Ali and Bina also delete those bit locations at which Bina should have received but did not receive a bit. Such 'non-receptions' could be caused by Iblees's intrusion or by dark counts in Bina's detecting device. The locations of the dark counts are, of course, communicated by Bina to Ali over the public channel.

Estimation of error in raw key

Ali and Bina now use the public channel to estimate the error rate in raw key. They publicly select and agree upon a random sample of raw key, publicly compare these bits to obtain an estimate *R* of the error rate. These revealed bits are discarded from raw key. If *R* exceeds a certain threshold *RMax*, then it will be impossible for Ali and Bina to arrive at a common secret key. If so, Ali and Bina return to stage 1 to start over. On the other hand, If the error estimate *R* does not exceed *RMax* , then Ali and Bina move onto next phase.

Extraction of reconciled key

In this phase, Ali and Bina's objective is to remove all errors from what remains of raw key to produce an error free common key, called reconciled key. This phase is of course called reconciliation, and takes place in two steps.

In step 1, Ali and Bina publicly agree upon a random permutation, and apply it to what remains of their respective raw keys. Next Ali and Bina partition the remnant raw key into blocks of length *l*, where the length *l* is chosen so that blocks of this length are unlikely to contain more than one error. For each of these blocks, Ali and Bina publicly compare overall parity checks, making sure each time to discard the last bit of the compared block. Each time a overall parity check does not agree, Ali and Bina initiate a binary search for the error, i.e., bisecting the block into two sub-blocks, publicly comparing the parities for each of these sub-blocks, discarding the right most bit of each sub-block. They continue their bisective search on the sub-block for which their parities are not in agreement. This bisective search continues until the erroneous bit is located and deleted. They then continue to the next *l*-block.

Step 1 is repeated, i.e., a random permutation is chosen, remnant raw key is partitioned into blocks of length *l*, parities are compared, etc. This is done until it becomes inefficient to continue in this fashion.

Ali and Bina then move to step 2 by using a more refined reconciliation procedure. They publicly select randomly chosen subsets of remnant raw key, publicly compare parities, each time discarding an agreed upon bit from their chosen key sample. If a parity should not agree, they employ the binary search strategy of step 1 to locate and delete the error.

Finally, when, for some fixed number *N* of consecutive repetitions of step 2, no error is found, Ali and Bina assume that to a very high probability, the remnant raw key is without error. Ali and Bina now rename the remnant raw key reconciled key, and move on to the final and last phase of their communication.

Privacy amplification, i.e., extraction of final secret key

Ali and Bina now have a common reconciled key which they know is only partially secret from Iblees. They now begin the process of privacy amplification, which is the extraction of a secret key from a partially secret one.

Based on their error estimate *R*, Ali and Bina obtain an upper bound *k* of the number of bits known by Iblees of their *n* bits of reconciled key. Let *s* be a security parameter that Ali and Bina adjust as desired. They then publicly select n - k - s random subsets of reconciled key, without revealing their contents, and without revealing their parities. The undisclosed parities become the common final secret key. It can be shown that Iblees's average information about the final secret key is less than 2^{-s} / ln 2 bits.

3.2.3 Priming the pump to start authentication

Unfortunately, there is no known way to initiate authentication without initially exchanging secret key over a secure communication channel. So, quantum protocols have not entirely overcome the "catch 22" of classical cryptography. However, this secret key exchange for authentication need only be done once. Thereafter, a portion of the secure key communicated via a quantum protocol can be used for authentication.

3.3 The B92 quantum cryptographic protocol

The B92 protocol was proposed by Bennett in 1992 [15]. Like BB84 protocol, this protocol can be described in terms of any quantum system represented by a two dimensional Hilbert space. We choose the two dimensional Hilbert space H representing the polarization states of a single photon.

B92 can be implemented in terms of any non-orthogonal basis. Let $|\phi\rangle$ and $|\varphi\rangle$ be the kets representing the polarization state of a photon linearly polarized at an angle ϕ and an angle φ, respectively, with respect to the vertical, where $0 \leq \phi \leq \pi/4$.

Unlike BB84 which requires two orthogonal quantum alphabets, B92 requires only a single non-orthogonal quantum alphabet. We choose the non-orthogonal quantum alphabet A_ϕ, as described in Table 3.3.

Table 3.3 Linear Polarization Quantum Alphabet A_ϕ

Symbol	*Bit*
$\|\phi\rangle$	1
$\|\varphi\rangle$	0

As in BB84, Ali and Bina communicate in two steps, the first over a one way quantum channel, the second over a two way public channel.

3.3.1 Communication over a quantum channel

Ali generates a random sequence of photons using the quantum alphabet A_ϕ and sends it to Bina. Since $|\phi\rangle$ and $|\varphi\rangle$ are not orthogonal, there are many experiments that unambiguously distinguish between these two polarization states. Thus, Bina can use one of many possible measurement strategies. Bennett suggests the measurements be based on the two incompatible experiments corresponding to the projection operators

$$P_{\text{not}\,\phi} = 1 - |\phi\rangle\langle\phi| \text{ and } P_{\text{not}\,\varphi} = 1 - |\varphi\rangle\langle\varphi| \tag{3.5}$$

In this case, Bina either correctly detects Ali's transmitted bit, or an ambiguous result, i.e., an erasure, denoted by "?". Assuming that Ali transmits 0's and 1's at random with equal probability and that, for each incoming bit, Bina at random with equal probability chooses to base her experiment on either of the incompatible operators $P_{\text{not}\,\phi}$ or $P_{\text{not}\,\varphi}$, then the probability of Bina's correctly receiving Ali's transmission is

$$(1 - \| \langle \phi | \varphi \rangle \|^2) / 2 \tag{3.6}$$

and the probability of receiving an erasure is

$$(1 + \| \langle \phi | \varphi \rangle \|^2) / 2 \tag{3.7}$$

where $\| \langle \phi | \varphi \rangle \| = \cos(2\phi)$ and where $0 < \phi < \pi/4$. Thus, Bina receives more than 50% erasures.

On the other hand, Ekert [16] suggest a more efficient measurement process for Bina. They suggest that Omer base his experiments on the positive operator valued measure (POVM) [10] consisting of the operators

$$A_\phi = (P_{\text{not}\,\phi}) / (1 + \| \langle \phi | \varphi \rangle \|), \tag{3.8}$$

$$A_\varphi = (P_{\text{not}\,\varphi}) / (1 + \| \langle \phi | \varphi \rangle \|) \tag{3.9}$$

and $A_? = 1 - A_\phi - A_\varphi$

With this more efficient detection method, the probability of an inconclusive result is now

$$\| \langle \phi \mid \varphi \rangle \| = \cos(2\phi) \tag{3.10}$$

where again $0 < \phi < \pi/4$

3.3.2 Communication over a public channel

Bina publicly informs Ali as to which time slots she received non erasures. The bits in these time slots become Ali's and Bina's raw keys. Iblees's presence is detected by an unusual error rate in Bina's raw key. It is also possible to detect Iblees's presence by an unusual erasure rate for Bina.

However, Ekert [16] do point out that Iblees can choose eavesdropping strategies which have no effect on the erasure rate, and hence, can only be detected by unusual error rates in Bina's raw key.

3.4 EPR quantum cryptographic protocols

Ekert in [17] has devised a quantum protocol based on the properties of quantum correlated particles.

Einstein, Podolsky, and Rosen (EPR) in their famous 1935 paper [18] point out an interesting phenomenon in quantum mechanics. According to their theory, the EPR effect occurs when a pair of quantum mechanically correlated photons, called the entangled photons, is emitted from a source. The entanglement may arise out of conservation of angular momentum. As a result, each photon is in an undefined polarization. Yet, the two photons always give opposite polarizations when measured along the same basis. Since EPR pairs can be pairs of particles separated at great distances, this leads to what appears to be a paradoxical "action at a distance".

For example, it is possible to create a pair of photons (each of which we label below with the subscripts 1 and 2, respectively) with correlated linear polarizations. An example of such an entangled state is given by

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 \left|\frac{\pi}{2}\right\rangle_2 - \left|\frac{\pi}{2}\right\rangle_1 |0\rangle_2\right) \tag{3.11}$$

Thus, if one photon is measured to be in the vertical linear polarization state |0⟩, the other, when measured, will be found to be in the horizontal linear polarization state |π/2⟩, and vice versa.

Einstein then state that such quantum correlation phenomena could be a strong indication that quantum mechanics is incomplete, and that there exist "hidden variables", inaccessible to experiments, which explain such "action at a distance".

In 1964, Bell [19] gave a means for actually testing for locally hidden variable (LHV) theories. He proved that all such LHV theories must satisfy the Bell inequality. Quantum mechanics has been shown to violate the inequality.

The EPR quantum protocol is a 3-state protocol that uses Bell's inequality to detect the presence or absence of Iblees as a hidden variable. We now describe a simplified version of this protocol in terms of the polarization states of an EPR photon pair.

As with the BB84 and B92, there are two steps to the EPR protocol, the first step over a quantum channel, the second over a public channel.

3.4.1 Communication over a quantum channel

An EPR pair is created at the source. One photon of the constructed EPR pair is sent to Ali, the other to Bina. Ali and Bina at random with equal probability separately and independently measure their respective photons. Ali records his measured bit. On the other hand, Bina records the complement of his measured bit. This procedure is repeated for as many EPR pairs as needed.

3.4.2 Communication over a public channel

Ali and Bina communicate over a public channel.

Separation of key into raw and rejected keys

Ali and Bina carry on a discussion over a public channel to determine the correct bases they used for measurement. They each then separate their respective bit sequences into two subsequences. One subsequence, called raw key, consists of those bits at which they used the same basis for measurement. The other subsequence, called rejected key, consists of all the remaining bits.

Detection of Iblees's presence with Bell's inequality applied to rejected key

Unlike the BB84 and B92 protocols, the EPR protocol, instead of discarding rejected key, actually uses it to detect Iblees's presence. Ali and Bina now carry on a discussion over a public channel comparing their respective rejected keys to determine whether or not Bell's inequality is satisfied. If it is, Iblees's presence is detected. If not, then Iblees is absent.

Chapter 4

Randomized Quantum Key Distribution

4. Randomized Quantum Key Distribution

We have developed a quantum key distribution (QKD) scheme based on quantum entanglement. The polarization basis for this entanglement is selected at random. The sender generates pairs of entangled particles and sends one particle from each pair to the receiver. Both sender and receiver randomly and independently execute some unitary transformations on the particle they possess. Finally, a measurement is made on the sender's side to check for possible eavesdropping. This scheme doesn't require any classical public channel. The delicate nature of entanglement along with random selection of basis guarantees that no adversary party can get the key.

4.1 The concept

The bell states are described as:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4.1}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{4.2}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{4.3}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{4.4}$$

The state of a quantum bit (qubit) can be altered by applying any unitary quantum gate. We will make use of a set of quantum gates, commonly known as Pauli operators, described as:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix} \quad \text{and} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.5}$$

Also note that $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix.

We express the Pauli operators and the identity matrix in the bra-ket notation as [20]:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{4.6}$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{4.7}$$

$$\sigma_y = \imath\left(|1\rangle\langle 0| - |0\rangle\langle 1|\right) \tag{4.8}$$

$$\sigma_z = |0\rangle\langle 1| - |1\rangle\langle 0| \tag{4.9}$$

If we apply σ_z to 2nd qubit of $|\Phi^+\rangle$, we will get:

$$\begin{aligned}
&\sigma_z^{(B)}|\Phi^+\rangle_{AB} \\
&\quad \left(|0\rangle_B {}^B\langle 0| - |1\rangle_B {}^B\langle 1|\right) \frac{1}{\sqrt{2}} \left(|00\rangle_{AB} + |11\rangle_{AB}\right) \\
&\quad \frac{1}{\sqrt{2}}\Big(|0\rangle_A|0\rangle_B {}^B\langle 0|0\rangle_B + |1\rangle_A|0\rangle_B {}^B\langle 0|1\rangle_B \\
&\quad - |0\rangle_A|1\rangle_B {}^B\langle 1|0\rangle_B - |1\rangle_A|1\rangle_B {}^B\langle 1|1\rangle_B\Big) \\
&\quad \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} - |11\rangle_{AB}\right)
\end{aligned} \tag{4.10}$$

Applying σ_z to 1st qubit of (4.10) gives:

$$\begin{aligned}
&\left(|0\rangle_A {}^A\langle 0| - |1\rangle_A {}^A\langle 1|\right) \frac{1}{\sqrt{2}} \left(|00\rangle_{AB} - |11\rangle_{AB}\right) \\
&\quad \frac{1}{\sqrt{2}}\Big(|0\rangle_A|0\rangle_B {}^A\langle 0|0\rangle_A - |0\rangle_A|1\rangle_B {}^A\langle 0|1\rangle_A \\
&\quad - |1\rangle_A|0\rangle_B {}^A\langle 1|0\rangle_A + |1\rangle_A|1\rangle_B {}^A\langle 1|1\rangle_A\Big) \\
&\quad \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)
\end{aligned} \tag{4.11}$$

which is again $|\Phi^+\rangle$. Similarly, it can be shown that any one of the four operators described above, when applied to both qubits of $|\Phi^+\rangle$ alternatively, will give us the state

$\Phi^{+}\rangle$ as a result. It is, however, noted that applying different operators to the two qubits of $|\Phi^{+}\rangle$ does not result in $|\Phi^{+}\rangle$ again.

4.2 The Protocol

Let H be the two dimensional Hilbert space whose elements represent the polarization states of a single photon. We use two different orthogonal bases of H. The linear polarization basis consists of the kets $|\ \rangle$ and $|\quad\rangle$ for vertical and horizontal polarization states, respectively, whereas the circular polarization basis consists of the kets $|\curvearrowright\rangle$ and $|\curvearrowright\rangle$ for right and left circular polarization states. The encoding of classical bits over these states is represented in Table 4.1.

Table 4.1 Encoding of classical bits over quantum states

Symbol	*Bit*
$\|\ \rangle$	0
$\|\rangle$	1
$\|\curvearrowright\rangle$	0
$\|\curvearrowright\rangle$	1

The state of the entangled photon pair along the linear basis is represented as:

$$|\varphi_{HV}\rangle \quad \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle|\leftrightarrow\rangle \;\mid\; |\updownarrow\rangle|\updownarrow\rangle) \tag{4.12}$$

and for the pair along circular basis:

$$|\varphi_{LR}\rangle \quad \frac{1}{\sqrt{2}}(|\curvearrowleft\rangle|\curvearrowleft\rangle \;\mid\; |\curvearrowright\rangle|\curvearrowright\rangle) \tag{4.13}$$

Let M be the set of unitary operators where

$$M = \{I, \sigma_x, \iota\sigma_y, \sigma_z\} \tag{4.14}$$

We assume that a quantum communication is going to take place between two legitimate parties 'Ali' and 'Bina'. A third adversarial party 'Iblees' is ready to eavesdrop this communication. The protocol proceeds as follows:

1. Ali selects a polarization basis, linear or circular, at random with equal probability. He generates a pair of entangled photons along the chosen basis. We call it as bipartile system. The state of this system is either $|\phi_{HV}\rangle$ or $|\phi_{LR}\rangle$, however, it corresponds to the Bell state $|\Phi^{+}\rangle$. This step is repeated until he accumulates n pairs (n may be disclosed in public).

2. Ali keeps one photon from each pair, let it be $|u\rangle$, while sends the other to Bina, let it be $|v\rangle$. We call the sequence of $|v_j\rangle$ photons as seed, where $0 \leq j < n$.

3. Bina randomly and independently selects a unitary operator from M and applies it to the received photon. The state of the bipartile system is transformed into:

$$M_i|\phi_{HV}\rangle \rightarrow |\phi'_{HV}\rangle \tag{4.15}$$

or

$$M_i|\phi_{LR}\rangle \rightarrow |\phi'_{LR}\rangle \tag{4.16}$$

where $i = 0, 1, 2, 3$.

Bina repeats this step for n photons she receives and records i each time, which we call as passcode. Note that 2 bits are needed to represent the value of i. So, the length of passcode will be $2n$.

4. Bina returns n photons back to Ali.

5. Ali randomly and independently selects a unitary operator from M and applies it to the photon he retains in step 2. The state of the bipartile system now becomes:

$$M_i|\phi'_{HV}\rangle \rightarrow |\phi''_{HV}\rangle \tag{4.17}$$

or

$$M_i|\phi'_{LR}\rangle \rightarrow |\phi''_{LR}\rangle \tag{4.18}$$

where again $i = 0, 1, 2, 3$.

As in step 3, Ali repeats this step for all the n photons, recording the 2-bit value of i each time, thereby, producing a $2n$ bit passcode.

6. Ali combines every $|u_j\rangle$ photon with the $|v_j\rangle$ photon, where $0 \leq j < n$, forming the pairs (in other words, he will attempt to form original entangled pairs as in step 1). Finally, he performs the Bell state measurement on each pair. If

$$\left|\phi''_{HV}\right\rangle\left(\text{or } \left|\phi''_{LR}\right\rangle\right) = \left|\Phi^{+}\right\rangle \tag{4.19}$$

then the protocol succeeds. Otherwise, failure is reported.

In order to inform Bina about the success or failure of the protocol, Ali may create an m-qubit string. To represent failure, the qubits are initialized to 0, in which case both Ali and Bina will move back to step 1. To represent success, the qubits are initialized to 1, in which case they will consider the passcodes as their final keys.

4.3 Eavesdropping strategies and intrusion detection

In this section we discuss some eavesdropping strategies that may be adopted by Iblees, and the security of our protocol against these strategies along with intrusion detection.

4.3.1 The intercept-resend strategy

In intercept-resend, Iblees intercepts the photons and reads them in basis of his choosing. Then he fabricates and sends a photon of the same polarization as he detected. We consider the following three cases.

First, we consider the case when Iblees intercepts transmission from Ali. Since, the intercepted photon may be from one of two possible polarization bases, Iblees will have to make intelligent guess with probability ½ for the correct basis. If he guesses incorrectly, this process of measurement will randomize the photon's basis of polarization. As a result the bipartile system will no longer remain entangled and, therefore, intrusion will be detected upon Bell state measurement by Ali. On the other hand, if Iblees guesses correctly, he will safely record the result of his measurement and will send to Bina another photon polarized according to the result he obtained. However, this partial information is in no way useful since passcodes are independent of seed and that they are never communicated.

Next, we consider the case when Iblees intercepts the photons returned by Bina. This case is similar to the one discussed above. We can simply say that monitoring this sequence of photons will be useless for Iblees in any manner.

Lastly, we consider the case when Iblees intercepts the signal in both directions. Suppose Ali sends a qubit $|0\rangle$ to Bina. It is noted that Iblees's choice of measurement basis should remain consistent throughout one round of transmission for a single photon. Assuming Iblees's choice of basis is compatible with the traveling photon, his measurement will give him $|0\rangle$, for which he will create another qubit in the same state and send it to Bina. Then, Iblees intercepts and measures the qubit returning from Bina, and get either $|0\rangle$ or $|1\rangle$. This means that Iblees can differentiate with probability ½ between the sets $\{I, \sigma_z\}$ and $\{\sigma_x, \iota\sigma_y\}$, but he cannot differentiate between the operators within the sets. Therefore, this partial information will be useless to him.

We have discussed the intercept-resend strategy for a single photon. If Iblees make use of a wrong basis of polarization, his actions are likely to be detected. In all three cases described above, the probability that Iblees escapes detection is assumed to be ½. Since, our protocol utilizes *n* photons at a time, this count reduces to $(½)^n$, which can be made too small to imagine.

4.3.2 Beam splitting

This strategy depends on the fact that the transmitted light pulses are not pure single-photon states. To carry out this attack, Iblees uses a partly-silvered mirror or equivalent device to divert a fraction of the original beams intensity to himself, letting the remainder pass undisturbed to Bina. This way, Iblees will have complete copy of transmitted bit sequence, though unmeasured yet.

Even BB84 protocol is vulnerable to this attack [21]. In [22] the authors have discussed Conditional Beam Splitting which is more disastrous to quantum key distribution schemes. It is believed that by using beam splitting, Ibleess actions will certainly go undetected. However, our protocol offers some degree of protection against this strategy. Since, no classical communication is involved, Iblees can never know with certainty the choice of polarization basis taken by Ali. Moreover, assuming Iblees correctly obtains exact copy of transmission, he wont be able to extract fruitful information as discussed in section 4.3.1.

4.3.3 EPR man-in-the-middle attack

D. Richard [23] has pointed out a security loophole in some QKD schemes. Here we discuss the vulnerability of our protocol against this type of attack.

Ali creates a two-qubit system in Bell state $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, sending the second qubit to Bina. Iblees captures the qubit, creates his own two qubit system, then forwards to Bina one qubit of this system in EPR state $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$. Bina applies her choice of unitary operator on the received qubit and returned it to Iblees, thinking it is being returned to Ali. Iblees combines the received qubit with the one he retained from the EPR pair that he created, then executes a Bell state measurement on the pair. Depending on the result he obtains, he records the operator index. Taking the qubit he captured previously from Ali, he executes the operator identified by the index he obtained and returns the qubit back to Ali.

At first it appears that Iblees will have a complete copy of Bina's passcode. However, the scheme cannot work because of the reason that a random selection is made for the basis of polarization. Intrusion detection will be carried out as discussed in section 4.3.1. Even if Iblees coincides his passcode with that of Bina, this information will be useless since, when a disturbance is made to the signal, the passcodes of both Bina and Iblees are always different from the one possessed by Ali.

Chapter 5

Simulation Software

5. Simulation Software

We have developed a simulation software to test and verify our research. This chapter is dedicated to illustrate all phases of software development paradigm we used to develop the software.

5.1 Analysis

At a technical level, software engineering begins with a series of modeling tasks that lead to a complete specification of requirements and a comprehensive design representation for the software to be built. The Analysis model, actually a set of models, is the first technical representation of a system. Over the years many methods have been proposed for analysis modeling. However two now dominate the analysis modeling landscape. The first, *structured analysis* is a classical modeling method and the other approach is *object oriented* method. We have used the later modeling technique for the analysis of our simulation software.

5.1.1 Use case diagrams

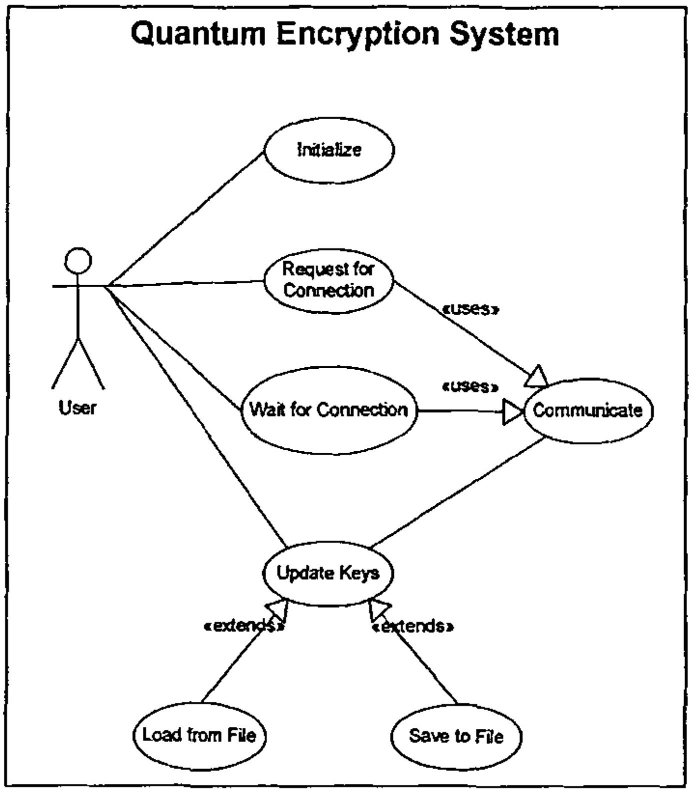


Figure 5.1 Use case diagram for Quantum Encryption System (QES).

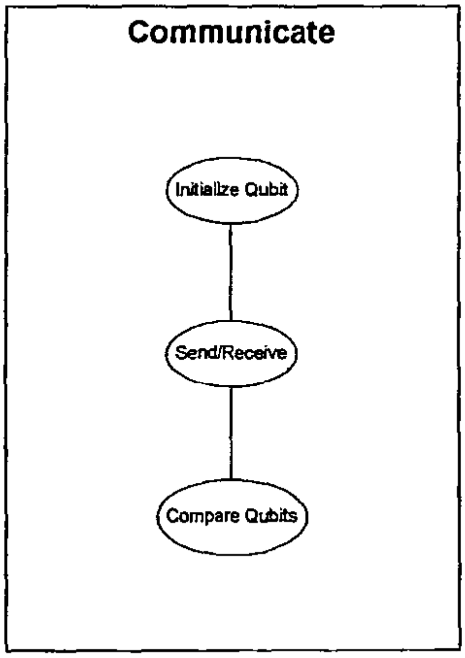


Figure 5.2 Use case diagram for Communication use case.

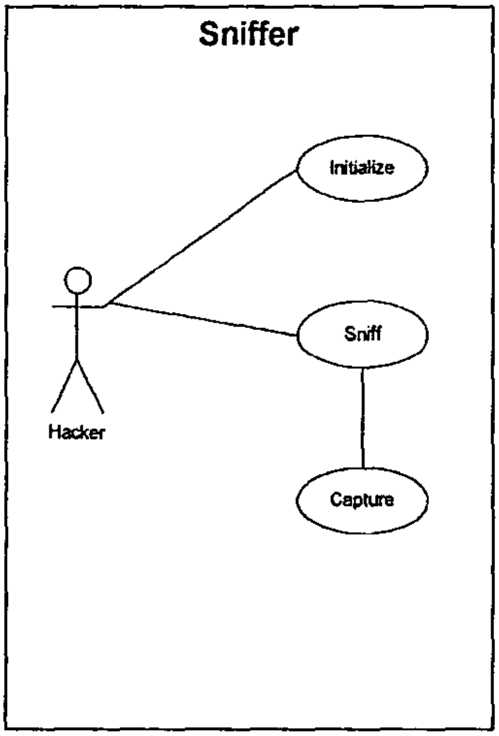


Figure 5.3 Use case diagram for Sniffer module.

5.2 Design

During an iterative development cycle it is possible to move to a design phase, once the use cases are complete. During this step a logical solution based upon the object-oriented paradigm is developed. The designer's goal is to produce a model or representation of an entity that will later be built. The process by which the model is developed combines intuition and judgment based on experience in building similar entities, a set of principles and/or heuristics that guide the way in which the model evolves, a ultimately leads to a final design representation.

5.2.1 Class diagrams

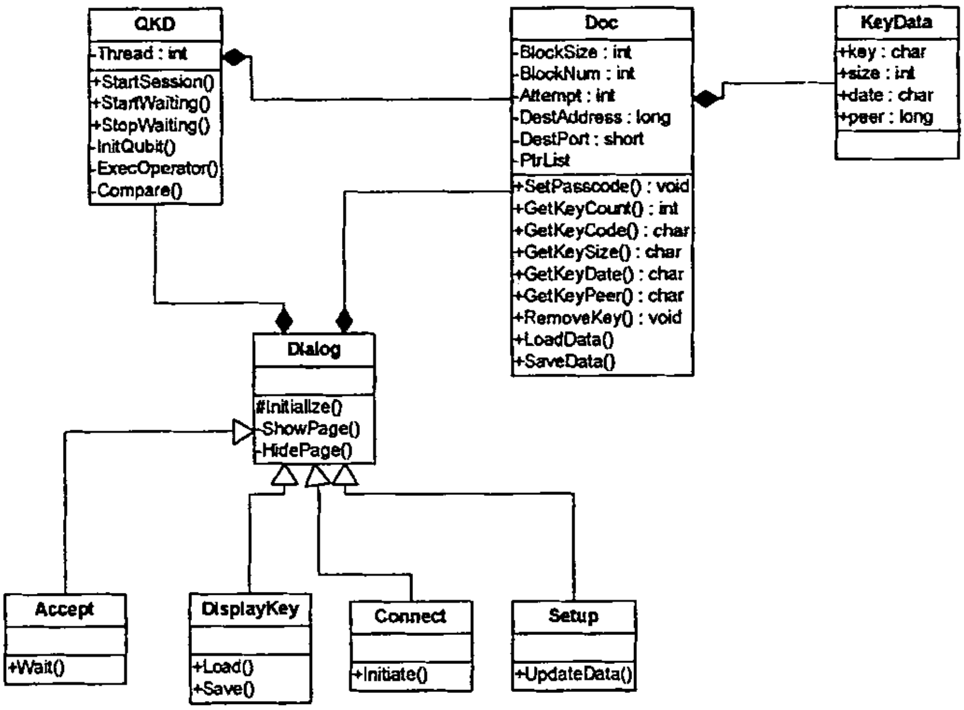


Figure 5.4 Class diagram of QES.

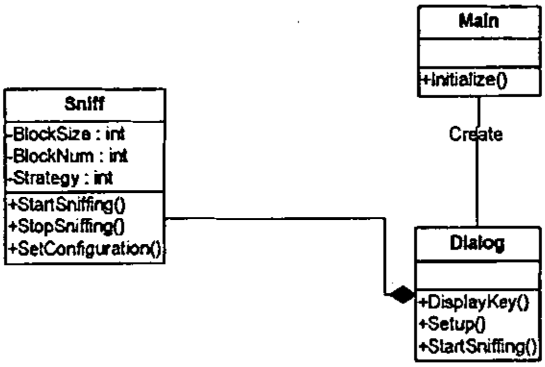


Figure 5.5 Class diagram for Sniffer module.

5.2.2 Activity diagrams

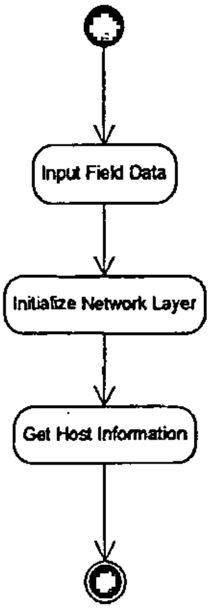


Figure 5.6 Activity diagram for 'Initialize' use case.

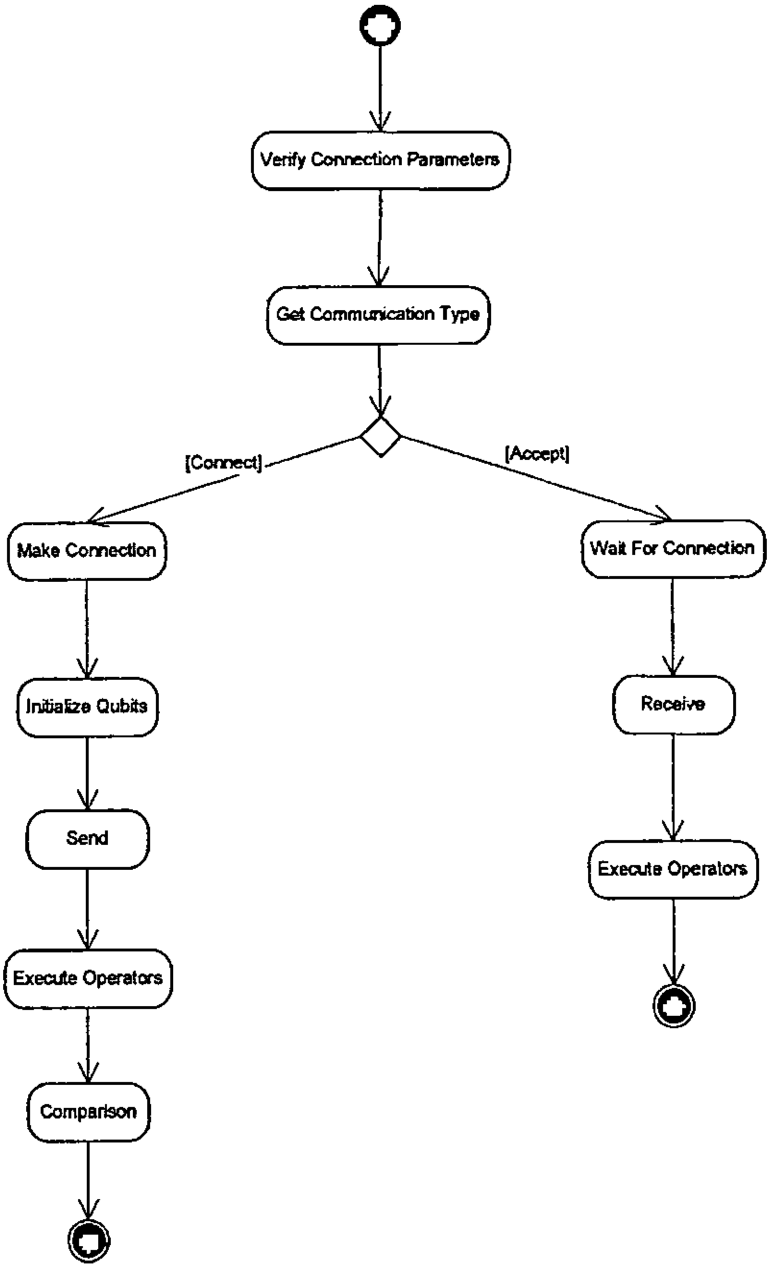


Figure 5.7 Activity diagram for 'Communicate' use case.

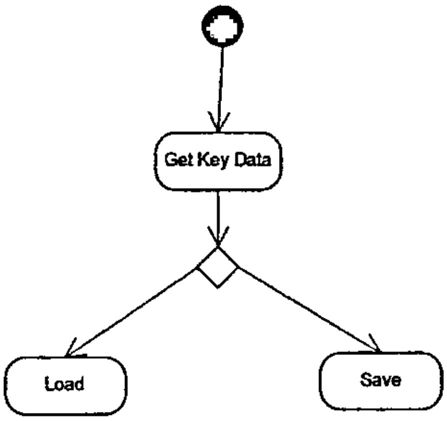


Figure 5.8 Activity diagram for 'Update keys' use case.

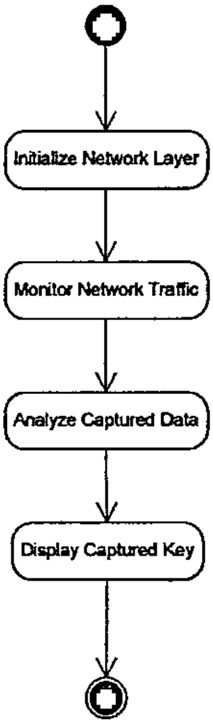


Figure 5.9 Activity diagram for 'Sniff' use case.

5.2.3 Sequence diagrams

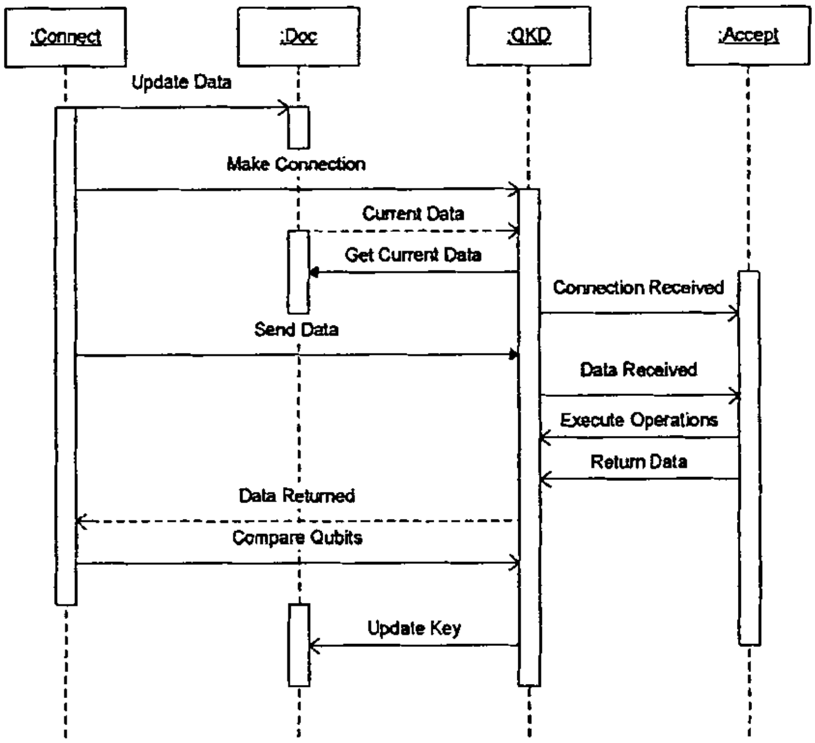


Figure 5.10 Sequence diagram for 'Communicate' use case

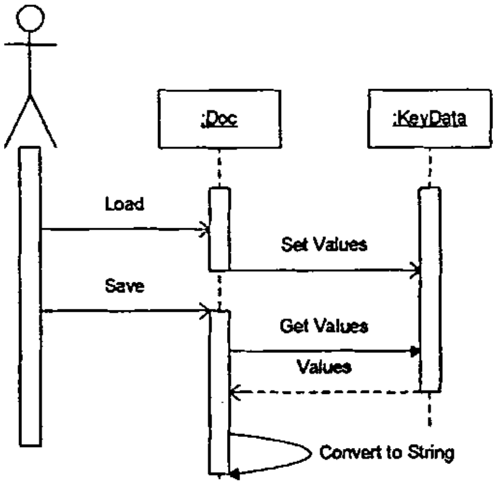


Figure 5.11 Sequence diagram for 'Update Keys' use case

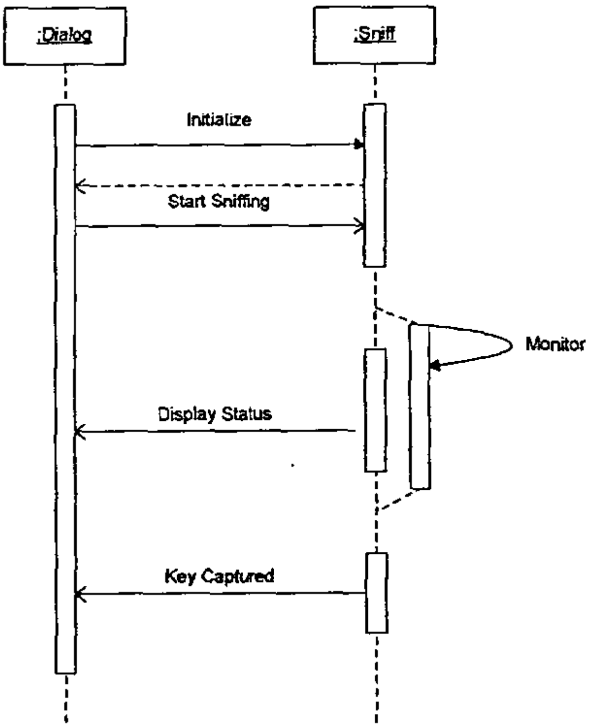


Figure 5.12 Sequence diagram for 'Sniff' use case.

5.3 Implementation

We have used Microsoft Visual C++ .NET for the development of this simulation. In order to fully grab quantum mechanical properties, we have made use of bitwise operations and system level tasks. A skinning interface is provided to show a beautiful look and feel. In this section, we introduce major components of the program along with their brief explanation.

Class Doc

SetPasscode. When keys are communicated successfully, then this function is called to update the key set.

GetKeyCount. Returns the number of keys currently holding by the Doc class.

GetKeyCode. Returns the code of a given key.

GetKeySize. Returns the size of a given key in bits.

GetKeyDate. Returns the date when the given key was shared with the remote user.

GetKeyPeer. Returns the IP address of the remote user who sharing the given key.

RemoveKey. Remove the given key from the list of keys.

LoadKeyData. Load keys from a file. The list of keys is emptied before loading new keys and updated as necessary.

SaveKeyData. Save the active list of keys to a specified file.

EmptyKeyList. Remove all keys from the list.

Class QKD

ThdAccept. A thread function used to perform several function. The thread, after creation, initializes the Microsoft Winsock Architecture and makes a local socket to wait for incoming connections. When a connection is arrived, it is accepted and communication is started. The function sits in a loop to read incoming data, perform local operations and send the modified data back to where it came from. The loop exits upon remote user's request, and results are displayed.

ThdConnect. A thread function used to perform several function. The thread, after creation, initializes the Microsoft Winsock Architecture and makes a socket to connect to remote user. When the connection is established, two similar lists of qubits is prepared and sent to the remote user. The function now waits to receive back the qubits. When received, a comparison is made between the list received and the one retained. The results are then displayed to the user.

GetDoc. This function returns a pointer to the current open document.

StartSession. Creates a new thread for connection process.

StartWaiting. Creates a new thread for acceptance process.

StopWaiting. If the user wishes to stop the acceptance process, he can initiate this function to stop the thread from waiting.

InitQubit. Initializes a qubit to some random values, for example, the polarization basis, polarization direction, classical bit value etc. The qubit is actually represented as one byte. Bits 0-4 are used for control operations like success or failure indication, terminate connection etc. Bits 5-8 are used to set quantum values.

ExecOp. Executes a local operator. It either one of Pauli operators or the identity operator. 2 bits are reserved to describe the operator executed.

CompareQubits. A comparison between two qubits. Returns true if comparison succeeds, returns false otherwise.

Class Sniff

StartSniffing. Starts the sniffing process.

StopSniffing. Stops the sniffing thread and returns resources to the system.

SetConfiguration. Sets system required configuration like block size, number of blocks etc.

GetPasscode. If passcode is successfully captured, it is converted a character string and displayed to the user.

ThdSniffer. Thread function to perform sniffing operations. This function receives data from source user and send it to the destination user unaltered. Now it waits to receive data back from the destination user. When received, this function performs local operations based on the specified eavesdropping strategy. When done, it sends the modified data back to the source user.

ThdMessage. Prompt the user about different events taking place during sniffing process.

ExtractInfo. Reads the captured qubit and analyze about possible local operations performed by the destination user. Then perform its own local operations based the result obtained.

Appendix-A

The No-cloning theorem

Appendix-A The No-cloning theorem

In this appendix, we prove that there can be no device that produces exact replicas or copies of a quantum system. If such a 'quantum copier' existed, then Iblees could eavesdrop without detection. This proof is taken from [10].

It is an amazingly simple application of the linearity of quantum mechanics (See also [11] for a proof using the creation operators of quantum electrodynamics). Let us assume that there exists a quantum replicator initially in state $|\Psi\rangle$ which duplicates quantum systems via a unitary transformation U.

Let $|u\rangle$ and $|v\rangle$ be two arbitrary states such that

$$0 < \left\| \langle u | v \rangle \right\| < 1$$

Then the application of the quantum replicator to $|u\rangle$ and $|v\rangle$ yields

$$\begin{aligned} |\Psi\rangle|u\rangle &\mapsto U|\Psi\rangle|u\rangle = |\Psi'\rangle|u\rangle|u\rangle \\ |\Psi\rangle|v\rangle &\mapsto U|\Psi\rangle|v\rangle = |\Psi''\rangle|v\rangle|v\rangle \end{aligned}$$

where $|\Psi'\rangle$ and $|\Psi''\rangle$ denote the states of the quantum replicator after the two respective duplications.

Thus,

$$\langle u|\langle\Psi|U^{\dagger}U|\Psi\rangle|v\rangle = \langle u|\langle\Psi|\Psi\rangle|v\rangle = \langle u|v\rangle$$

because of the unitarity of U and because $\langle\Psi|\Psi\rangle = 1$. On the other hand,

$$\langle u|\langle u|\langle\Psi'|\Psi''\rangle|v\rangle|v\rangle = \langle\Psi'|\Psi''\rangle\langle u|v\rangle^{2}$$

As a result, we have the equation

$$\langle u|v\rangle = \langle\Psi'|\Psi''\rangle\langle u|v\rangle^{2}$$

But this equation cannot be satisfied since $\left\|\langle\Psi'|\Psi''\rangle\right\| \le 1$ and $|u\rangle$ and $|v\rangle$

were chosen so that $0 < \left\|\langle u|v\rangle\right\| < 1$.

Hence, a quantum replicator cannot exist.

Appendix-B

Proof that an eavesdropper can get no information from non-orthogonal states

Appendix-B Proof that an eavesdropper cannot get any information from non-orthogonal states

In this appendix we prove that an undetectable eavesdropper obtains no information from non-orthogonal states. The proof is taken from [7].

Let $|a\rangle$ and $|b\rangle$ denote the two non-orthogonal states. Thus,

$$\langle a|b\rangle \neq 0$$

Let U be the unitary transformation performed by Iblees's detection probe, which we assume is initially in state $|\Psi\rangle$.

Since Iblees's probe is undetectable, we have

$$|\Psi\rangle|a\rangle \mapsto U|\Psi\rangle|a\rangle = |\Psi'\rangle|a\rangle$$
$$|\Psi\rangle|b\rangle \mapsto U|\Psi\rangle|b\rangle = |\Psi''\rangle|b\rangle$$

where $|\Psi'\rangle$ and $|\Psi''\rangle$ denote the states of Iblees's probe after the detection of $|a\rangle$ and $|b\rangle$ respectively. Please note that, since Iblees is undetectable, his probe has no effect on the states $|a\rangle$ and $|b\rangle$ So $|a\rangle$ appears on both sides of the first equation, and $|b\rangle$ appears on both sides of the second equation.

Thus,

$$\langle a|\langle\Psi|U^{\dagger}U|\Psi\rangle|b\rangle = \langle a|\langle\Psi|\Psi\rangle|b\rangle = \langle a|b\rangle$$

because of the unitarity of U and because $\langle\Psi|\Psi\rangle = 1$. On the other hand,

$$\langle a|\langle\Psi'|\Psi''\rangle|b\rangle = \langle\Psi'|\Psi''\rangle\langle a|b\rangle$$

As a result, we have the equation

$$\langle a|b\rangle = \langle\Psi'|\Psi''\rangle\langle a|b\rangle$$

But $\langle a|b\rangle \neq 0$ implies $\langle\Psi'|\Psi''\rangle = 1$. Since $|\Psi'\rangle$ and $|\Psi''\rangle$ are normalized, this implies that $|\Psi'\rangle = |\Psi''\rangle$. It follows that Iblees's probe is in the same state no matter which of the states $|a\rangle$ and $|b\rangle$ is received. Thus, Iblees obtains no information whatsoever.

Appendix-C

Glossary of Terms

Appendix-C Glossary of Terms

Algorithm. A set of instructions to be executed by a computing device. What instructions are available depends on the computing device. Typically, instructions include commands for manipulating the contents of memory and means for repeating blocks of instructions indefinitely or until a desired condition is met.

Amplitude. A quantum system with a chosen orthonormal basis of "logical" states $|i\rangle$ can be in any superposition $\sum_i \alpha_i |i\rangle$ of these states, where $\sum_i |\alpha_i|^2 = 1$. In such a superposition, the complex numbers α_i are called the amplitudes. Note that the amplitudes depend on the chosen basis.

Ancillas. Helper systems used to assist in a computation involving other information systems.

Bell basis. For two qubits *A* and *B*, the Bell basis consists of the four states $\frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB})$ and $\frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB})$.

Bell states. The members of the Bell basis.

Bit. The basic unit of deterministic information. It is a system that can be in one of two possible states, 0 and 1.

Bit sequence. A way of combining bits into a larger system whose constituent bits are in a specific order.

Bit string. A sequence of 0's and 1's that represents a state of a bit sequence. Bit strings are the words of a binary alphabet.

Black box. A computational operation whose implementation is unknown. Typically, a black box implements one of a restricted set of operations, and the goal is to determine which of these operations it implements by using it with different inputs. Each use of the black box is called a "query". The smallest number of queries required to determine the operation is called the "query complexity" of the restricted set. Determining the query complexity of sets of operations is an important problem area of computational complexity.

Bloch sphere. The set of pure states of a qubit represented as points on the surface of the unit sphere in three dimensions.

Bra. A state expression of the form $\langle\psi|$, which is considered to be the conjugate transpose of the ket expression $|\psi\rangle$.

Bra-ket notation. A way of denoting states and operators of quantum systems with kets (for example, $|\psi\rangle$) and bras (for example, $\langle\psi|$).

Circuit. A combination of gates to be applied to information units in a prescribed order. To draw circuits, one often uses a convention for connecting and depicting gates. See also "network".

Circuit complexity. The circuit complexity of an operation on a fixed number of information units is the smallest number of gates required to implement the operation.

Classical information. The type of information based on bits and bit strings and more generally on words formed from finite alphabets. This is the information used for communication between people. Classical information can refer to deterministic or probabilistic information, depending on the context.

Computation. The execution of the instructions provided by an algorithm.

Computational states. See the entry for "logical states".

Computer. A device that processes information.

Density matrix or operator. A representation of pure and mixed states without redundancy. For a pure state $|\psi\rangle$, the corresponding density operator is $|\psi\rangle\langle\psi|$. A general density operator is a probabilistic combination $\sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$, with $\sum_i \lambda_i = 1$.

Deterministic information. The type of information that is based on bits and bit strings. Deterministic information is classical, but it explicitly excludes probabilistic information.

Distinguishable states. In quantum mechanics, two states are considered distinguishable if they are orthogonal. In this case, a measurement exists that is guaranteed to determine which of the two states a system is in.

Efficient computation. A computation is efficient if it requires at most polynomially many resources as a function of input size. For example, if the computation returns the value $f(x)$ on input x, where x is a bit string, then it is efficient if there exists a power k such that the number of computational steps used to obtain $f(x)$ is bounded by $|x|^k$, where $|x|$ is the length (number of bits) of x.

Entanglement. A non-classical correlation between two quantum systems most strongly exhibited by the maximally entangled states such as the Bell states for two qubits, and considered to be absent in mixtures of product states (which are called "separable" states). Often states that are not separable are considered to be entangled. However, nearly separable states do not exhibit all the features of maximally entangled states. As a result, studies of different types of entanglement are an important component of quantum information theory.

Gate. An operation applied to information for the purpose of information processing.

Global phase. Two quantum states are indistinguishable if they differ only by a global phase. That is, $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ are in essence the same state. The global phase difference is the factor $e^{i\phi}$. The equivalence of the two states is apparent from the fact that their density matrices are the same.

Hilbert space. An n-dimensional Hilbert space consists of all complex n-dimensional vectors. A defining operation in a Hilbert space is the inner product. If the vectors are thought of as column vectors, then the inner product $\langle x, y\rangle$ of x and y is obtained by forming the conjugate transpose $x^\dagger$ of x and calculating $\langle x, y\rangle = x^\dagger y$. The inner product induces the usual squared norm $|x|^2 = \langle x, x\rangle$.

Information. Something that can be recorded, communicated, and computed with. Information is fungible; that is, its meaning can be identified regardless of the particulars of the physical realization. Thus, information in one realization (such as ink on a sheet of paper) can be easily transferred to another (for example, spoken words). Types of information include deterministic, probabilistic and quantum information. Each type is characterized by "information units", which are abstract systems whose states represent the simplest information of each type. The information units define the "natural" representation of the information. For deterministic information the information unit is the bit, whose states are symbolized by 0 and 1. Information units can be put together to form larger systems and can be processed with basic operations acting on a small number of them at a time.

Inner product. The defining operation of a Hilbert space. In a finite dimensional Hilbert space with a chosen orthonormal basis $\{e_i : 1 \leq i \leq n\}$, the inner product of two vectors $x = \sum_i x_i e_i$ and $y = \sum_i y_i e_i$ is given by $\sum_i \bar{x}_i y_i$. In the standard column representation of the two vectors, this is the number obtained by computing the product of the conjugate transpose of x with y. For real vectors, this agrees with the usual "dot" product. The inner product of x and y is often written in the form $\langle x, y \rangle$. Pure quantum states are unit vectors in a Hilbert space. If $|\phi\rangle$ and $|\psi\rangle$ are two quantum states expressed in the ket-bra notation, there inner product is given by $(|\phi\rangle)^\dagger |\psi\rangle = \langle\phi|\psi\rangle$.

Ket. A state expression of the form $|\phi\rangle$ representing a quantum state. Usually $|\phi\rangle$ is thought of as a superposition of members of a logical state basis $|i\rangle$. One way to think about the notation is to consider the two symbols "|" and "⟩" as delimiters denoting a quantum system and as a symbol representing a state in a standard Hilbert space. The combination $|\phi\rangle$ is the state of the quantum system associated with in the standard Hilbert space via a fixed isomorphism. In other words, one can think of $\phi \leftrightarrow |\phi\rangle$ as an identification of the quantum system's state space with the standard Hilbert space.

Linear extension of an operator. The unique linear operator that implements a map defined on a basis. Typically, we define an operator U on a quantum system only on the logical states $U : |i\rangle \mapsto |\psi_i\rangle$. The linear extension is defined by $U(\sum_i \alpha_i |i\rangle) = (\sum_i \alpha_i |\psi_i\rangle)$.

Logical states. For quantum systems used in information processing, the logical states are a fixed orthonormal basis of pure states. By convention, the logical basis for qubits consists of $|0\rangle$ and $|1\rangle$. For larger dimensional quantum systems, the logical basis is often indexed by the whole numbers, $|0\rangle$, $|1\rangle$, $|2\rangle$, ... The logical basis is often also called the "computational" basis, or sometimes, the "classical" basis.

Network. *In the context of information processing,* a network is a sequence of gates applied to specified information units. We visualize networks by drawing horizontal lines to denote the time line of an information unit. The gates are represented by graphical elements that intercept the lines at specific points. A realization of the network requires applying the gates to the information units in the specified order (left to right).

Operator. A function that transforms the states of a system. Operators may be restricted depending on the system's properties. For example, in talking about operators acting on quantum systems, one always assumes that they are linear.

Oracle. An information processing operation that can be applied. A use of the oracle is called a "query". In the oracle model of computation, a standard model is extended to include the ability to query an oracle. Each oracle query is assumed to take one time unit. Queries can reduce the resources required for solving problems. Usually, the oracle implements a function or solves a problem not efficiently implementable by the model without the oracle. Oracle models are used to compare the power of two models of computation when the oracle can be defined for both models. For example, in 1994, D. Simon showed that quantum computers with a specific oracle O could efficiently solve a problem that had no efficient solution on classical computers with access to the classical version of O. At the time, this result was considered to be the strongest evidence for an exponential gap in power between classical and quantum computers.

Overlap. The inner product between two quantum states.

Pauli operators. The Hermitian matrices $\sigma_x, \sigma_y, \sigma_z$ acting on qubits, which are two-level quantum systems.

Probabilistic bit. The basic unit of probabilistic information. It is a system whose state space consists of all probability distributions over the two states of a bit. The states can be thought of as describing the outcome of a biased coin flip before the coin is flipped.

Probabilistic information. The type of information obtained by extending the state spaces of deterministic information to include arbitrary probability distributions over the deterministic states. This is the main type of classical information to which quantum information is compared.

Product state. For two quantum systems *A* and *B*, product states are of the form $|\psi\rangle_A|\phi\rangle_B$. Most states are not of this form.

Program. An algorithm expressed in a language that can be understood by a particular type of computer.

Projection operator. A linear operator *P* on a Hilbert space that satisfies $P^2 = P^\dagger P = P$. The projection onto a subspace *V* with orthogonal complement *W* is defined as follows: If $x \in V$ and $y \in W$, then $P(x+y) = x$.

Pseudo-code. An semi-formal computer language that is intended to be executed by a standard "random access machine", which is a machine model with a central processing unit and access to a numerically indexed unbounded memory. This machine model is representative of the typical one processor computer. Pseudo-code is similar to programming languages such as BASIC, Pascal, or C, but does not have specialized instructions for human interfaces, file management, or other "external" devices. Its main use is to describe algorithms and enable machine-independent analysis of the algorithms' resource usage.

Pure state. A state of a quantum system that corresponds to a unit vector in the Hilbert space used to represent the system's state space. In the ket notation, pure states are written in the form $|\psi\rangle = \sum_i \alpha_i |i\rangle$, where the $|i\rangle$ form a logical basis and $\sum_i |\alpha_i|^2 = 1$.

Quantum information. The type of information obtained when the state space of deterministic information is extended by normalized superpositions of deterministic states. Formally, each deterministic state is identified with one of an orthonormal basis vector in a Hilbert space and normalized superpositions are unit-length vectors that are expressible as complex linear sums of the chosen basis vectors. It is convenient to extend this state space further by permitting probability distributions over the quantum states . This extension is still called quantum information.

Qubit. The basic unit of quantum information. It is the quantum extension of the deterministic bit, which implies that its state space consists of the unit-length vectors in a two dimensional Hilbert space.

Read-out. A method for obtaining human-readable information from the state of a computer. For quantum computers, read-out refers to a measurement process used to obtain classical information about a quantum system.

Reversible gate. A gate whose action can be undone by a sequence of gates.

Separable state. A mixture of product states.

States. The set of states for a system characterizes the system's behavior and possible configurations.

Subspace. For a Hilbert space, a subspace is a linearly closed subset of the vector space. The term can be used more generally for a system *Q* of any information type: A subspace of *Q* or, more specifically, of the state space of *Q* is a subset of the state space that preserves the properties of the information type represented by *Q*.

Superposition principle. One of the defining postulates of quantum mechanics according to which if states $|0\rangle$, $|1\rangle$, $|2\rangle$, ... are distinguishable then $\sum_i \alpha_i |i\rangle$ with $\sum_i |\alpha_i|^2 = 1$ is a valid quantum state. Such a linear combination is called a normalized superposition of the states $|i\rangle$.

System. An entity that can be in any of a specified number of states. An example is a desktop computer whose states are determined by the contents of its various memories and disks. Another example is a qubit, which can be thought of as a particle whose state space is identified with complex, two dimensional, length-one vectors. Here, a system is always associated with a type of information that determines the properties of the state space. For example, for quantum information the state space is a Hilbert space. For deterministic information, it is a finite set called an alphabet.

Unitary operator. A linear operator U on a Hilbert space that preserves the inner product. That is, $\langle Ux|Uy\rangle = \langle x|y\rangle$. If U is given in matrix form, then this expression is equivalent to $U^{\dagger}U = I$.

Universal set of gates. A set of gates that satisfies the requirement that every allowed operation on information units can be implemented by a network of these gates. For quantum information, it means a set of gates that can be used to implement every unitary operator. More generally, a set of gates is considered universal if for every operator *U*, there are implementable operators *V* arbitrarily close to *U*.

Appendix-D

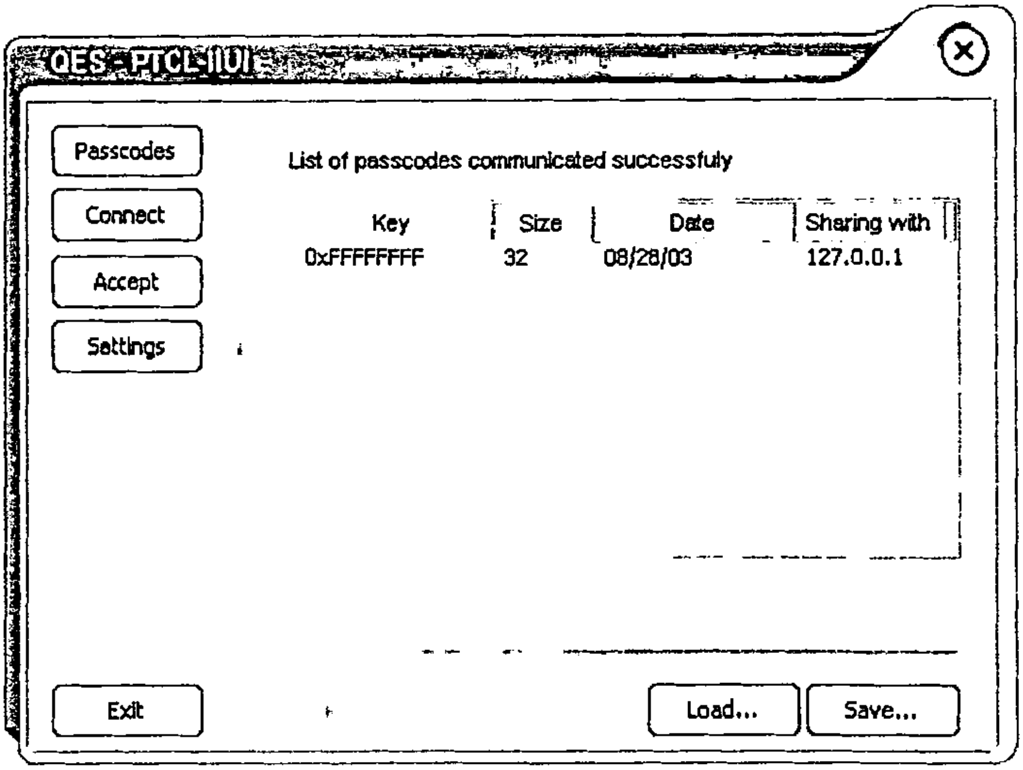
User Manual

Appendix-D User Manual

Overview

This software is built as a simulation to describe a Quantum Key Distribution process. The software uses network features of a system to communicate between multiple instances. The simulation also includes a Sniffer component which describes different eavesdropping strategies that may be adopted by a hacker. The vulnerability of our scheme against such type of attacks is tested. This appendix is dedicated to describe different user interface components that we have prepared for the user.

Main window (Passcodes)



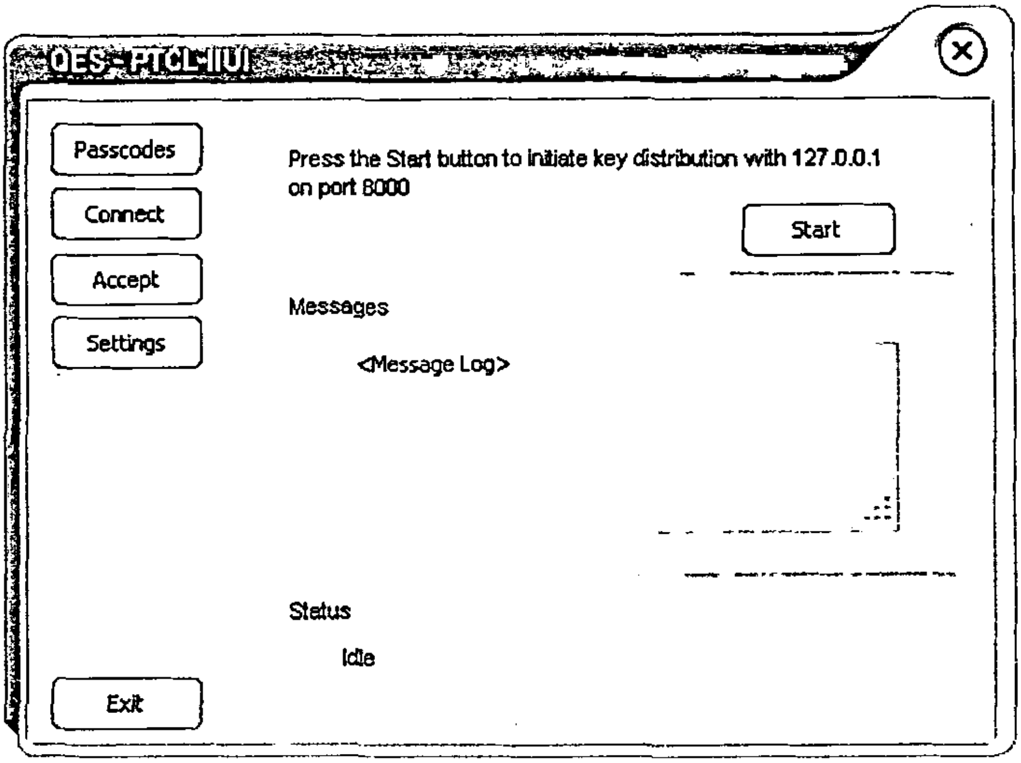
List of passcodes communicated successfuly

Key	Size	Date	Sharing with
0xFFFFFFFF	32	08/28/03	127.0.0.1

Figure 1 Main window

The main window (Passcodes) displays a list of passcodes that are communicated successfully. The list shows the key (in hexadecimal numbers), the size of key in bits, the date when this key was shared and the remote user address who is sharing this key. The user has the option to Load or Save the contents of the list from a file. Any selected key can also be removed, if desired.

Connect window



Press the Start button to initiate key distribution with 127.0.0.1 on port 8000

Messages

<Message Log>

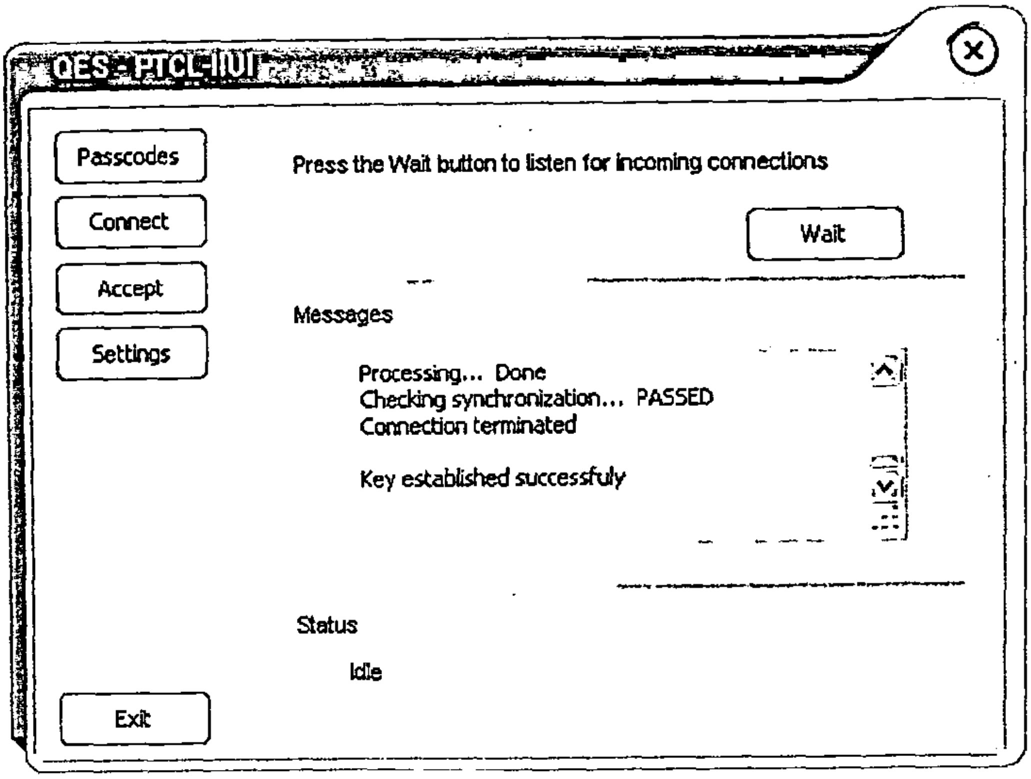
Status

Idle

Figure 2 Connect window.

This window enables the user to initiate a connection with the remote user. The Start button starts the communication. Notification messages are displayed on the Messages box. The Status describes the important tasks the system is doing at the moment or have been done successfully.

Accept window



Press the Wait button to listen for incoming connections

Messages

Processing... Done
Checking synchronization... PASSED
Connection terminated

Key established successfuly

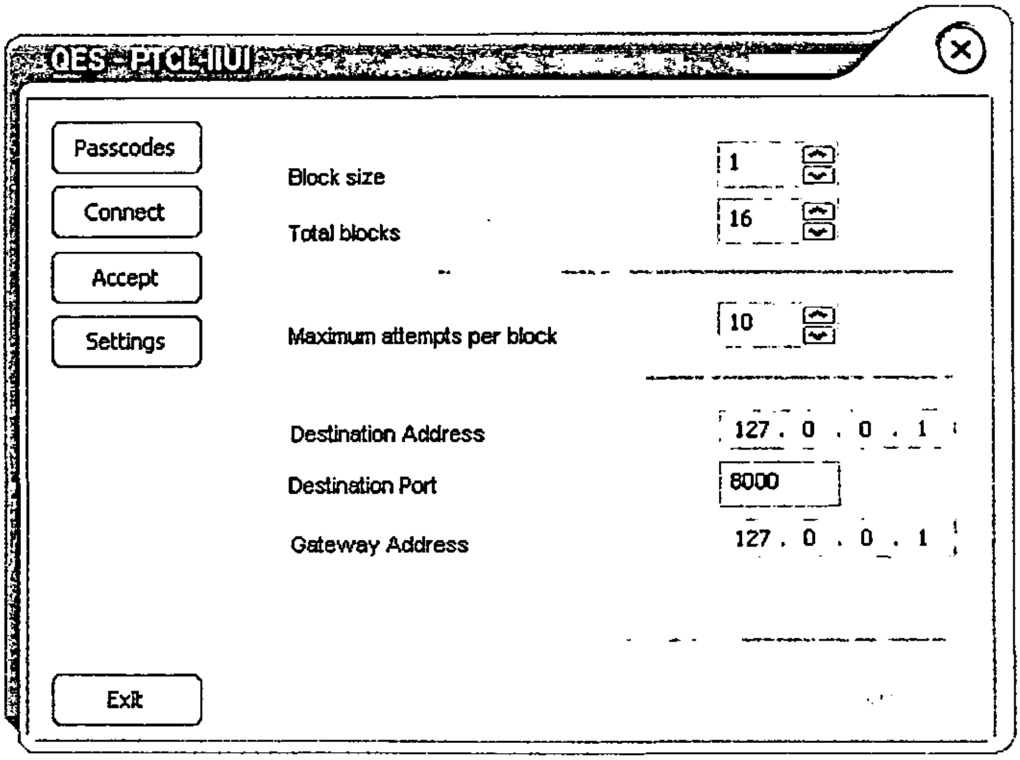
Status

Idle

Figure 3 Accept window.

This window enables the user to wait for incoming connections from the source user. The Wait button starts the listening process. Notification messages are displayed on the Messages box. The Status describes the important tasks the system is doing at the moment or have been done successfully.

Setting window



Block size 1

Total blocks 16

Maximum attempts per block 10

Destination Address 127 . 0 . 0 . 1

Destination Port 8000

Gateway Address 127 . 0 . 0 . 1

Figure 4 Settings window

This window enables the user to enter the settings used by the system.

Block size: Number of qubits in a block.

Total Blocks: Maximum number of blocks that should be communicated.

Maximum attempts per block: Number of attempts that the system will make to transfer one block of data. When the maximum limit is reached and the system still experience failures, the transmission of that block is aborted.

Destination address: Address of the destination user machine.

Destination port: Socket port of the destination user machine.

Gateway address: Address of the gateway machine.

Reset: Resets the values to factory default.

Apply: Save the modified values to configuration settings.

Bibliography and References

Research Papers

1. W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22, no. 6, (1976), 644-654.

2. P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Press, 1994, pp. 124-134.

3. P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Computing, vol. 26, (1997), pp. 1484-1509.

4. S. Wiesner, "Conjugate coding", Sigact News, vol. 15, no. 1, (1983), pp. 78-88, manuscript written in about 1970.

5. D. Dieks, "Communication by EPR devices", Phys. Lett. vol. A92, (1982), pp.271-273.

6. W. K. Wootters and W. Zurek, "A single quantum can not be cloned", Nature, vol. 299, (1982), pp. 802-803.

7. C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", Phys. Rev. Lett., vol. 68 (1992), 557-559.

8. Shor, Peter W., Polynomial-Time Algorithms for Prime Fac- torization and Discrete Logarithms on a Quantum Compute, SIAM J. Computing 26 (1997) pp 1484 - . (See also quant-ph/9508027). An extended abstract of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20--22, 1994

9. C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and tossing", in Proceedings of IEEE International conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, (IEEE Press, 1984), pp. 175-179.

10. Peres, Asher, ``Quantum Theory: Concepts and Methods," Kluwer Academic Publishers, Boston, (1993).

11. Wootters, W.K., and W.H. Zurek, A single quantum cannot be cloned, Nature, Vol. 299, 28 October 1982, pp 982 - 983.

12. Phoenix, Simon J., and Paul D. Townsend, 1995. Quantum cryptography: how to beat the code breakers using quantum mechanics, Comtemporay Physics, vol. 36, No. 3.

13. Jacobs, B.C. and J.D. Franson, 1996. Quantum cryptography in free space, Optics Letters, Vol. 21.

14. Franson, J.D., and H. Ilves, 1994. Quantum cryptography using polarization feedback, Journal of Modern Optics, Vol. 41, No. 12.

15. Bennett, Charles H., 1992. Quantum cryptography using any two nonorthogonal states, Physical Review Letters, Vol. 68, No. 21.

16. Ekert, Artur K., Bruno Huttner, G. Massimo Palma, and Asher Peres, 1994. Eavesdropping on quantum-cryptographical systems, Phys. Rev. A, Vol. 50, No 2.

17. Ekert, Artur K., 1991. Quantum cryptography based on Bell's theorem, Physical Review Letters, Vol. 67, No. 6.

18. Einstein, A., B. Podolsky, N. Rosen, 1935. Can quantum, mechanical description of physical reality be considered complete?, Phys. Rev. 47, 1951. D. Bohm "Quantum Theory", Prentice-Hall, Englewood Cliffs, NJ.

19. Bell, J.S., 1964.,Physics, 1.

20. E. Knill, R. Laflamme, H. Barnum, D. Dalvit, J. Dziarmaga, J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola, and W. Zurek. "Introduction to quantum information processing". Technical Report LAUR-01-4761, Los Alamos National Laboratory, 2001.

21. Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail and John Smolin, “Experimental Quantum Cryptography”, Lecture Notes in Computer Science, 1991.

22. John Calsamiglia, Stephen M. Barnett and Norbert Ltkenhaus, “Conditional beam splitting attack on quantum key distribution”, Phys. Rev. A, 2002.

23. D. Richard Kuhn, “Vulnerabilities in Quantum Key Distribution Protocols”, quant-ph/0305076, 2003.