2008

Enhancing security in quantum cryptography

Partha Basuchowdhuri
Louisiana State University and Agricultural and Mechanical College

ENHANCING SECURITY IN QUANTUM CRYPTOGRAPHY

A Thesis
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in
The Department of Electrical and Computer Engineering

by
Partha Basuchowdhuri
B.E., Bengal Engineering College, 2003
May, 2008

Acknowledgements

I am very grateful to those people who have made this thesis possible and to those who have made my experience in the graduate school one that I will always remember fondly.

I want to deeply thank my major professor Dr. Subhash Kak for his patient guidance throughout the period of my Master's study. Without his encouragement, expertise, this work would not have been possible. He challenged me to do my best in learning, thinking, writing, research and personal growth and his support provided me with the motivation and determination to complete this degree.

My committee members Dr. Xue-Bin Liang and Dr. Hsiao-Chun Wu deserve my deepest thanks and appreciation for their time and willingness to endure this long journey with me.

Table of Contents

List of Tables

List of Figures

Abstract

Quantum Key Distribution was named as one of the top ten emerging technologies by Technology Review Journal in 2003 in their annual edition. The growth in quantum cryptography since the beginning of the millennium has been expedited by new theories and ideas. The introduction of practical quantum cryptosystems offered by USA based company MagiQTech and its European rival idQuantique has changed the face of cryptography. With active experimental research in USA, Europe, Japan and Singapore, the scope of quantum cryptography seems to be growing daily. When Bennett and Brassard proposed their BB84 protocol in Bangalore in 1984, no one would have guessed the quantum revolution they had launched. Since then, new protocols have been proposed and new theories developed, but BB84 remains the simplest and probably the easiest to implement. Now that the practical implementation of basic quantum cryptography has been achieved, one can be almost certain that new protocols will sooner or later be tested for the efficiency they could provide. We have developed a Classical Authentication Aided (CAA) protocol, which merges the classical authentication policies with quantum transmission to make it even more secure. With the complexities of the authentication policies and the bit to qubit conversion, our system becomes a complex one. We also discuss the possibilities of free space quantum transmission of the protocol instead of only through optical fiber.

1 Introduction

This part describes the basic ideas of quantum computing, which form the background to the development of quantum cryptography.

1.1 Overview of Quantum Information and Quantum Computing

In this section we discuss the reasons why quantum computing has attracted so much academic attention and what are the prospects for the building of quantum computers. Basically, the field of quantum information science has arisen from a desire to apply the concept of information to quantum systems. Quantum algorithms that have been proposed can solve certain problems faster than any classical machine; therefore it represents a new area of opportunity in the study of the very concept of computation.

1.1.1 Purpose of a Quantum Computer

A quantum computer is a device for computation that would be able to utilize theories of quantum mechanics on suitable information or data. The structure and features of data that could be used for quantum mechanical phenomena are different from what is used in classical computers.

If a classical task is assigned to a quantum computer, there is no guarantee that the quantum computer will outperform a classical computer in terms of efficiency. So the core idea is to make use of the quantum characteristics present in the data. For quantum computers, instead of using classical data or the bits, we use a special format of data called qubits. We will discuss theoretical details in the later sections.

The distinctly visible advantages of quantum computing can mainly be listed as:

1. When performed quantum operations on suitable quantum data, a classical problem can be solved in a much time efficient manner.

2. Due to quantum mechanical properties a qubit can be used for multiple problems and hence performs multiple tasks at the same time. This is not possible for classical bits.

3. No-cloning property of a qubit can work as an advantage if the message sent through the qubit is secret and making a copy of it is undesirable.

4. Whenever a state of a qubit or its superposition is measured, the state collapses. This issue can be used to maintain privacy of a message.

1.1.2 Present Applications of Quantum Computing

At present, realization of quantum computing is still confined with in the theoretical boundaries of quantum mechanics. Although theoretically established, the practical implementation of a quantum computer has not been successfully done.

According to publications like "The Economist", D-Wave Systems, a start-up company in Burnaby, British Columbia, demonstrated "the world's first commercial quantum computer" on 13th February, 2007 [1]. It demonstrated solution for two problems. The first one was to search a protein from a database, which implies application of quantum search. The other problem was optimality testing with quantum computer while finding solutions for Sudoku problems. There were insufficient explanation of how the system worked and D-Wave provided no proof to back up their claims. As a result, theoretical computer scientists dismissed their claims and were critical of D-Wave for misleading the people. As the claims of the "first quantum computer" goes into oblivion with the present controversy, nearly 30 years after Richard Feynman proposed the idea of the quantum computer, it still continues to lure the quantum scientists.

The only application of quantum computing that has been successfully implemented is quantum cryptography. Till date the longest distance to demonstrate quantum key distribution through optical fiber is 148.7 km (achieved by Los Alamos/NIST) [2] and through free space, it is 144 km (achieved by a European collaboration) [3]. Experiments also suggest that due to lower atmospheric density in higher altitudes, it might be possible to transmit to the satellites as well.

The most known quantum network, DARPA Quantum Network, is a 10-node quantum cryptography network that has been running since 2004 in Massachusetts, USA. It was developed by BBN Technologies, Harvard University, Boston University and QinetiQ.

Presently there are three companies offering commercial quantum cryptographic security systems: id Quantique (Geneva), MagiQ Technologies (New York) and SmartQuantum

(France). Several other companies are also spending resources and have active research programs on quantum cryptographic security systems, including Toshiba, HP, IBM, Mitsubishi, NEC and NTT (Nippon Telegraph and Telephone, Japan).

In 2004, for the first time a bank transfer was carried out using quantum cryptography in Vienna, Austria [4]. An important cheque, which needed absolute security, was transmitted from the Mayor of the city to an Austrian bank. This work was carried out by scientists from the University of Vienna and ARC Seibersdorf Research in Austria and Ludwig-Maximillians University, Germany. The fibers were installed by WKA (Wienkanal).

On October 21, 2007 quantum cryptography was successfully used to protect Swiss federal election for the state of Geneva [5], against hacking or accidental data corruption. The vendor for this occasion was the local company id Quantique.

1.2 Basic Principles of Quantum Computing

This part will describe the basic principles of quantum computing on which the principles of quantum cryptography or quantum error-correction are built. The first application of quantum ideas to physical systems occurred in the 1970s and 1980s [6],[7],[8]. Feynman described how quantum mechanical problems could be simulated on a computer in [9]. For a recent overview of quantum information and entropy, see [40].

1.2.1 Quantum Bits and Quantum Operations

In classical information, digital signals are denoted by classical bits. These classical bits, or as we say "bits", can obtain two states 0 and 1 to give rise to 2^n number of bit vectors for a vector length of *n*. Similarly, two possible states for quantum bits or qubits are $|0\rangle$ and $|1\rangle$. The difference between qubits and bits is that qubits can obtain states, which is also a superposition of $|0\rangle$ and $|1\rangle$ states. A superposition $|\psi\rangle$ can be described as,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{, where } \alpha \text{ and } \beta \text{ are complex numbers.}$$

So, qubit can be interpreted as a complex two-dimensional vector space, with $|0\rangle$ and $|1\rangle$ as basis states, which form an ortho-normal basis for the vector space.

A classical bit's idea can be depicted by a coin toss. The idea of a 0 or a 1 is same as getting a "Head" or a "Tail" every time a coin is tossed. But qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$ until it is observed. When measured a qubit can be in a state $\alpha|0\rangle+\beta|1\rangle$, which when measured gives $|0\rangle$ with a probability of $|\alpha|^2$ and $|1\rangle$ with a probability of $|\beta|^2$. When $\alpha=\frac{1}{\sqrt{2}}$ and $\beta=\frac{1}{\sqrt{2}}$, $|\psi\rangle$ can be denoted by $|+\rangle$ and similarly when $\alpha=\frac{1}{\sqrt{2}}$ and $\beta=-\frac{1}{\sqrt{2}}$, $|\psi\rangle$ can be denoted by $|-\rangle$.

If there were *n* classical bits, then there would be 2^n possible states. For example, a two qubit system has four computational basis states denoted by $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. So the superposition of the basis states for the two qubit systems can be described as, $|\psi\rangle=\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle$, where α is a complex coefficient which denotes the amplitude for each basis vector.

Quantum gates are analogous to what logic gates are to classical information. Since a single qubit is a vector $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ parameterized by two complex numbers α and β, which satisfies $|\alpha|^2+|\beta|^2=1$, all operations on a qubit should be described by 2×2 unitary matrices.

Four useful matrices, which are often used for quantum operations, are the *Pauli matrices* [10].

$$I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \qquad X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$$Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Three other quantum gates, which are frequently used in quantum operations, are Hadamard gate (H), Phase gate (S) and $\frac{\pi}{8}$ gate (T).

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \quad S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} = \exp(i\pi/8) \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix}$$

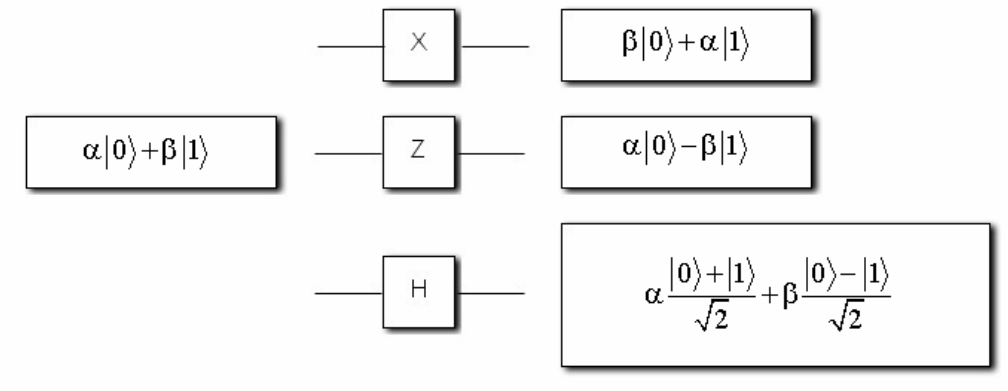

Figure 1: Explaining Pauli-X, Pauli-Z and Hadamard gates

Bloch's Theorem: It states that for solid body rotations in three dimensions, any arbitrary 2×2 unitary matrix can be written as:

$$U = e^{i\gamma} \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{bmatrix} = e^{i\gamma} e^{i\alpha\sigma_z} e^{i\theta\sigma_x} e^{i\beta\sigma_z},$$

where $\sigma_x, \sigma_y, \sigma_z$ are Pauli-X, Pauli-Y and Pauli-Z matrices.

Controlled gates: Say, U is a gate that operates on single qubits with matrix representation $U = \begin{bmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{bmatrix}$. Then, the controlled-U gate would be a gate that operates on two qubits in such a way that the first qubit serves as a control qubit and the others are called target qubit.

$$|00\rangle \to |00\rangle, \qquad |01\rangle \to |01\rangle,$$

$$|10\rangle \to |1\rangle U |0\rangle = |1\rangle(x_{00}|0\rangle + x_{10}|1\rangle), \qquad |10\rangle \to |1\rangle U |1\rangle = |1\rangle(x_{01}|0\rangle + x_{11}|1\rangle)$$

Thus the matrix of a controlled U-gate is $U(C) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{bmatrix}$

Figure 2: Controlled U-gate (left) and uncontrolled U-gate (right)

For uncontrolled U-gates there is not control bit.

$I \otimes U$ is defined as $|00\rangle \to |0\rangle U |0\rangle$, $|01\rangle \to |0\rangle U |1\rangle$, $|10\rangle \to |1\rangle U |0\rangle$, $|11\rangle \to |1\rangle U |1\rangle$, and is represented by the unitary matrix $\begin{bmatrix} x_{00} & x_{01} & 0 & 0 \\ x_{10} & x_{11} & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{bmatrix}$.

One of the most important controlled gate is CNOT gate and is denoted by

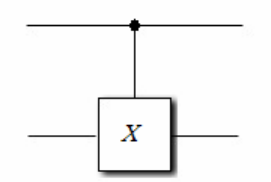

Figure 3: Representation of CNOT gate

Hence, the CNOT is represented by the unitary matrix $U(CNOT) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$.

1.2.2 Can Qubits Be Copied?

A classical CNOT gate may be used to copy a bit and is shown by the circuit in the Figure 4. Let us assume that we try to copy a qubit in an unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ in the same manner as in Figure 4. The input state of the two qubits may be written as,

$$\left[a|0\rangle + b|1\rangle\right]|0\rangle = a|00\rangle + b|10\rangle$$

The CNOT changes the second qubit when the first qubit is one. So the output becomes $|out\rangle = a|00\rangle + b|11\rangle$. If $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$, then it is possible to copy classical 0 and 1 bits encoded as $|0\rangle$ and $|1\rangle$. However, a more generalized view gives,

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

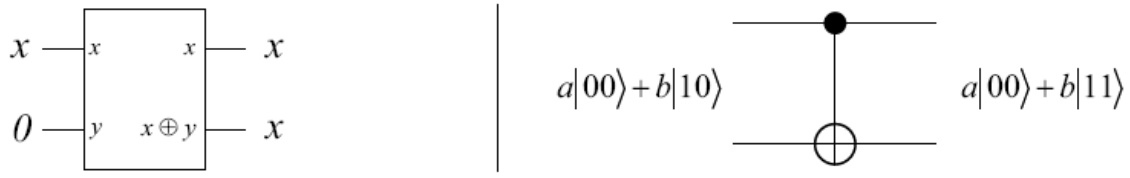

Figure 4: Classical and quantum circuits to copy an unknown bit

So we see that unless ab=0, we can not have $a|00\rangle + b|11\rangle$. So it can be said that it is not possible to make a copy of an unknown quantum state.

1.2.3 Bell States or EPR Pairs

A quantum circuit (as shown in Fig 5), which has the Hadamard gate followed by a CNOT, transforms the four computational basis states according to the Table 1. For an example, the Hadamard gate takes the input $|00\rangle$ to $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$, and then CNOT turns it to $(|00\rangle + |11\rangle)/\sqrt{2}$. The Hadamard transform puts the top qubit in a superposition and then it acts as a control input to the CNOT. The target gets inverted when the control is 1.

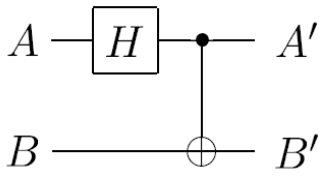

Figure 5: Quantum circuit to create EPR pairs

These output states $|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$, $|\phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$, $|\psi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$ and $|\phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ are known as Bell states or sometimes EPR (Einstein, Podolsky, Rosen) states or EPR pairs. Einstein, Podolsky, and Rosen (EPR), in their famous 1935 paper [21],[10], claimed to have found a quantum mechanical "paradox".

Table 1: Quantum "truth table" for EPR circuits

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\psi^+\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\phi^+\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\psi^-\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\phi^-\rangle$

They proposed existence of physically separated pairs of particles, called EPR pairs, whose states are correlated in such a way that the measurement of a chosen observable *A* of one automatically determines the result of the measurement of *A* of the other, irrespective of the physical distance between them. 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".

2 Quantum Cryptography

This part is the core to this thesis. It starts by describing the basic ideas of quantum cryptography and discusses its difference with classical cryptography. Then it describes the popular quantum cryptography protocols and after that the new classical authentication aided protocol and its modifications are discussed.

2.1 Brief Overview

Here we will discuss the basic principles of quantum cryptography and how it differs from classical cryptography.

Quantum cryptography is a method that utilizes principles of quantum mechanics to device a cryptosystem, which helps two parties share random strings of qubits that can be used as key to encrypt and decrypt message transmitted between them.

The most important feature of the quantum cryptography is to detect whether a third party was trying to intercept the key. As quantum bits can not be copied, if Alice sends the key to Bob and an eavesdropper Eve tries to gain knowledge of the key, then Eve has to corrupt the qubits because according to quantum mechanics a quantum system can not be measured without disturbing the system.

Say an eavesdropper Eve is trying to intercept the message being transmitted between Alice and Bob. Quantum key distribution is effective because of the no-cloning theorem. If Eve tries to differentiate between two non-orthogonal states, it is not possible to achieve information gain without collapsing the state of at least one of them.

This is clear from considering $|\psi\rangle$ and $|\varphi\rangle$ to be the non-orthogonal quantum states Eve is trying to know about. If these states interact with a standard state $|u\rangle$,

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle$$

$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle|v'\rangle$$

Eve would want $|v\rangle$ and $|v'\rangle$ to be different, to know the identity of the state. However inner products are preserved under unitary transformations and

$\langle v | v' \rangle \langle \psi | \varphi \rangle = \langle u | u \rangle \langle \psi | \varphi \rangle$ or, $\langle v | v' \rangle = \langle u | u \rangle = 1$

So $| v \rangle$ and $| v' \rangle$ must be identical and Eve will need to disturb one of the two states in order to acquire any information.

2.1.1 Differences with Classical Cryptography

Secured classical cryptosystems have been tested for past few decades and sufficient work has been done to implement them for security of communication. Although RSA, El-Gamal, ECC cryptosystems [13] are in use, it can be proved that theoretically each of these systems can be hacked. Some of these algorithms are secured in terms of the amount of large computational effort, which is restricted by capabilities of present hardware. But if the message is tapped and stored, may be with the rise of new technologies we will have sufficient computational power to decrypt those messages. But with quantum cryptography decryption of the quantum key is not possible. The central idea of security differs in the fact that, in classical cryptography the security of the system depends on the computational power and in quantum cryptography the security of the system depends on a basic principle of quantum mechanics, which states that a qubit can not be measured without collapsing it and hence corrupting the key.

Another differences between classical and quantum cryptography is that, in quantum cryptography transmission of the qubits is continuous, because qubits cannot be copied and stored. But in classical cryptography the encrypted message does not need to be continuous. It can be stored and transmitted in parts or in any desired way, which may not be true for quantum cryptography. Quantum repeaters have been invented during 1990s to store the states of the photon and it has also been further improved to exhibit increased reliability. But it has not been applied practically in wide range and is still a subject of speculation.

2.1.2 Prospects of Quantum Cryptography

Although classical cryptosystems are still most widely in use, if their quantum counterparts offered by companies like MagiQtech and idQuantique become successful then it is most likely that many companies or agencies, who needs secure transmission, will opt for quantum cryptosystems.

Let us take for example an important issue needed for successful cryptosystems, that is generation of random numbers. Classical computers can only generate pseudo-random numbers. But a quantum random generator can use the process of splitting a beam of photons on a beam splitter, which is a quantum mechanical source of true randomness.

NIST has already produced a notable enhancement in quantum-key generation field. They have tested keys that were generated at a rate of 1 Mbit/second [12]. These keys would be fast enough to encrypt multimedia streams. This indicates that quantum encryption may ultimately be faster than other conventional approaches.

As we have already mentioned in section 1.1.2, a few experiments have been made in Europe that has established the efficiency of quantum cryptography applications that are commercially available at present. Other than the companies we have mentioned another European company named Elsag plc has developed a commercial quantum key distribution scheme. Singapore has emerged as a competitor to Europe in entanglement based quantum cryptography, where Christian Kurtsiefer and his team are building and testing QKD at NUS with help of researchers from NIST. More recently, Japan has also appeared as a strong competitor using considerable manpower to quantum key distribution systems. The companies are NEC, Mitsubishi, Toshiba and NTT among others.

2.2 Literature Study And Comparing Existing Protocols

In this section the most popular quantum cryptography protocols will be discussed. This includes Bennett and Brassard's BB84 protocol [11], B92 protocol [14], the EPR protocol [15] and Kak's three-stage protocol [16].

2.2.1 BB84 Protocol

In 1984, Bennett and Brassard published their BB84 protocol, which is now the most popular QKD method. BB84 and its variants use quantum bits in one pass and this is followed by two additional passes of classical data transmission (that are potential weak links). Kak's protocol, on the other hand, uses quantum information transmission in all its steps to ensure that there is no weak link in the process. The weakness of the classical data links of the BB84 is apparent from the fact that single photons are not easy to produce, and the duplicate photons can be used by the eavesdropper to reconstruct the key.

The BB84 QKD protocol can be generally stated as follows:

1. Alice chooses a random $(4+\delta)n$ data bits.
2. Alice or the sender first chooses a random $(4+\delta)n$ bit string and encodes each data bit as $\{|0\rangle, |1\rangle\}$, if the corresponding bit of the string is 0 or $\{|+\rangle, |-\rangle\}$ if the bit is 1.
3. Alice sends the resulting states to Bob.
4. Bob receives it and announces it. Then Bob measures the qubit based of *X* or *Z* basis at random.
5. Alice then announces the bit string.
6. Alice and Bob discard all the bits for which Bob used a different basis than Alice. With a high probability there will be more than *2n* bits will be left and *2n* of them are chosen. If there are less than *2n* bits then the protocol is aborted.
7. To ensure no interference from Eve, Alice selects a subset of *n* bits as check bits and informs Bob about that.
8. Alice and Bob announce and check those *n* bits and if the number of matches is not above a threshold then the process is aborted.
9. With the remaining *n* bits Alice and Bob perform information reconciliation and privacy amplification to get a shared key of *m* bits

It can be further explained with a simple example. Say, Alice and Bob both have two polarizers. The first polarizer denotes 0/90 degrees ($+$) for which, 1 is assigned to the symbol $\updownarrow$ and 0 is assigned to the symbol $\leftrightarrow$. The second one denotes with 45/135 degrees ($\times$) for which, 1 is assigned to the symbol $\nwarrow\!\!\searrow$ and 0 is assigned to the symbol $\nearrow\!\!\swarrow$.

BB84 protocol can be viewed as a three stage protocol as said below:

Step 1: Alice randomly chooses polarizers to generate photons and sends them to Bob.

The main problem for BB84 is that generating single photon is not easy. In most

industrial applications weak laser beam is used to send the bits needed for the key.

Table 2: Preparation of photons by Alice

Say polarizers chosen by Alice are:	+ × × + + × +
Say photons sent by Alice are:	↔ ⤡ ⤢ ↕ ↕ ⤢ ↔

Step 2: Bob receives those photons with randomly chosen polarizers.

Table 3: Measurement of photons by Bob

Photons sent by Alice are:	↔ ⤡ ⤢ ↕ ↕ ⤢ ↔
Say polarizers chosen by Bob are:	+ + × + × × +
Bob's resulting measurement is:	↔ ↕ ⤢ ↕ ⤡ ⤢ ↔

Step 3: Alice and Bob matches their bases and discard the data for un-matched polarizers.

Table 4: Generation of the key

So final measurement should be:	↔ ↕ ⤢ ↕ ⤡ ⤢ ↔
So the resultant bit representation will be:	0 - 0 1 - 0 0

Usually the laser pulses generate two or more photons which remain in the same quantum state. In a beam-splitting attack [13] Eve could split the beam and use the spilt photon to detect the bit and could only let pass the multiple photon beams to Bob. In this way Eve can eventually determine all the key bits and also remain undetected.

2.2.2 B92 Protocol

The B92 protocol can be described in terms of any quantum system represented by a two dimensional Hilbert space *H*, which represents the polarization states of a single photon. B92 can be implemented in terms of any non-orthogonal basis. Let us take the bases as $|\phi\rangle$ and $|\bar{\phi}\rangle$, which denote the kets representing the polarization states of a photon linearly polarized at an angle ϕ and an angle $-\phi$ with respect to the vertical, where $0 < \phi < \frac{\pi}{4}$. $|\phi\rangle$ is represented by 1 and $|\bar{\phi}\rangle$ is represented by 0. Similarly to BB84, in B92 Alice

and Bob communicate the first over a one-way quantum channel and then over a two-way public channel.

The B92 protocol can be summarized as below:

1. Alice sends her random binary sequence to Bob.

2. Bob chooses any strategy to measure it. One of them could be the projection operators suggested by Bennett, $P_{\neg\phi} = 1 - |\phi\rangle\langle\phi|$ and $P_{\neg\bar{\phi}} = 1 - |\bar{\phi}\rangle\langle\bar{\phi}|$. Another measure could be positive operator value method (POVM) [15], as suggested by Ekert et al [20], using the operators $A_{\phi} = \frac{P_{\neg\phi}}{1 + \| \langle\phi|\bar{\phi}\rangle \|}$ and $A_{\bar{\phi}} = \frac{P_{\neg\bar{\phi}}}{1 + \| \langle\phi|\bar{\phi}\rangle \|}$.

3.

   a. For Bennett's method, with Alice transmitting randomly chosen "0"s and "1"s and Bob randomly choosing $P_{\neg\phi}$ and $P_{\neg\bar{\phi}}$ as its bases to measure those incoming bits, the probability of Bob's correctly detecting Alice's transmission is $\frac{1 - \| \langle\phi|\bar{\phi}\rangle \|^2}{2}$ and probability of receiving an ambiguous result is $\frac{1 + \| \langle\phi|\bar{\phi}\rangle \|^2}{2}$, where $\| \langle\phi|\bar{\phi}\rangle \| = \cos(2\phi)$ and where $0 < \phi < \frac{\pi}{4}$. With this arrangement Bob receives more than 50% ambiguous results.

   b. Ekert's measurement process for Bob has been known to be even more efficient. It says that Bob base his experiment on positive operator value method (POVM) consisting of operators $A_{\phi} = \frac{P_{\neg\phi}}{1 + \| \langle\phi|\bar{\phi}\rangle \|}$, $A_{\bar{\phi}} = \frac{P_{\neg\bar{\phi}}}{1 + \| \langle\phi|\bar{\phi}\rangle \|}$ and for ambiguous results $A_{amb} = 1 - A_{\phi} - A_{\bar{\phi}}$. With this more efficient detection method, the probability of an inconclusive result $\| \langle\phi|\bar{\phi}\rangle \| = \cos(2\phi)$ and where $0 < \phi < \frac{\pi}{4}$.

4. Bob publicly announces time-slots when he received correct measurements from Alice. Bits in those time-slots become the raw key for Alice and Bob.

5. If there is an unusual error rate in Bob's raw key, it is assumed that an eavesdropper Eve is present and hence the transmission is aborted.

2.2.3 EPR Protocol

Section 1.2.3 has already discussed the basic idea of EPR pairs. This protocol [15] shows that instead of key bits being generated by Alice, it can be developed from a fundamentally random process involving the properties of entanglement.

EPR pairs can exist due to several reasons:

1. Alice or Bob could prepare the pair and send a half to the other.

2. A third party could prepare the EPR and distribute to Alice and Bob.

3. Alice and Bob could have met long time ago and shared the pair, which might have been stored till present.

In order to generate key bits for EPR protocol, Alice and Bob performs identical tasks on their qubits. It can not be said for sure that which one among Alice and Bob has generated the key. Rather the key is truly random. Let us say that Alice prepares a random classical bit b and according to it, measures half of her EPR pairs with either bases $|0\rangle$ and $|1\rangle$ or with $|\pm\rangle$ and obtains a. Bob also random chooses his bases b' and obtains a'. Then Alice and Bob communicates over a pubic classical channel to announce b and b', and the key is made from $\{ a, a' \}$ where $b=b'$. The key is only determined when Alice or Bob makes a measurement on their half of the EPR pair.

2.2.4 Kak's Three Stage Protocol

This protocol can be summarized as follows:

Step 1: Alice applies a unitary transformation U_A on quantum information X and sends the qubits to Bob.

Step 2: Bob applies U_B on the received qubits U_A, which gives $U_B U_A(X)$ and sends it back to Alice.

Step 3: Alice applies $U_A^\dagger$ (transpose of the complex conjugate of U_A) on the received qubits to get $U_A^\dagger U_B U_A(X) = U_A^\dagger U_A U_B(X) = U_B(X)$ and sends it back to Bob.

Bob then applies $U_B^\dagger$ on $U_B(X)$ to get the information X.

Here U_A and U_B must be commutative to each other, which means that $U_B U_A(X) = U_A U_B(X)$.

With n number of qubits present in the message, the transformations U_A and U_B both must be of 2^n dimension. It has been observed that the (2 × 2) rotation operator, Pauli-X, Pauli-Y and Pauli-Z can be used as commutative transformations in 1-qubit system as all of these are 2 × 2 matrices.

In order to find transformations for an n-qubits system we can randomly pick any of these 2×2 matrices and tensor multiply it with another randomly picked one (may be itself) and keep on tensor multiplying for n times, which will eventually produce a $2^n \times 2^n$ matrix. The commutativity of the rotation operator can be shown as below:

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$R(\theta).R(\phi) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} = \begin{pmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{pmatrix}$$

For a 2-qubit system:

$$R_2(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 & 0 \\ \sin\theta & \cos\theta & 0 & 0 \\ 0 & 0 & \cos\theta & -\sin\theta \\ 0 & 0 & \sin\theta & \cos\theta \end{pmatrix}$$

where "*" denotes tensor product.

Keeping the practical implementations in view information exchange in three-stage protocol does not restrict to single photon. Even if the laser pulse produces multiple photons and as long as all the photons are in the same phase the transformation and their complex conjugate transformation will have same effect on them. So irrespective of how many photons are used three-stage protocol is bound to succeed and is not prone to beam-splitting attack.

But, theoretically, the three-stage protocol can be subjected to the man-in-the-middle attack [22]. The next section explains how it can affect functionality of three-stage protocol and how the protocol can be modified to perform better.

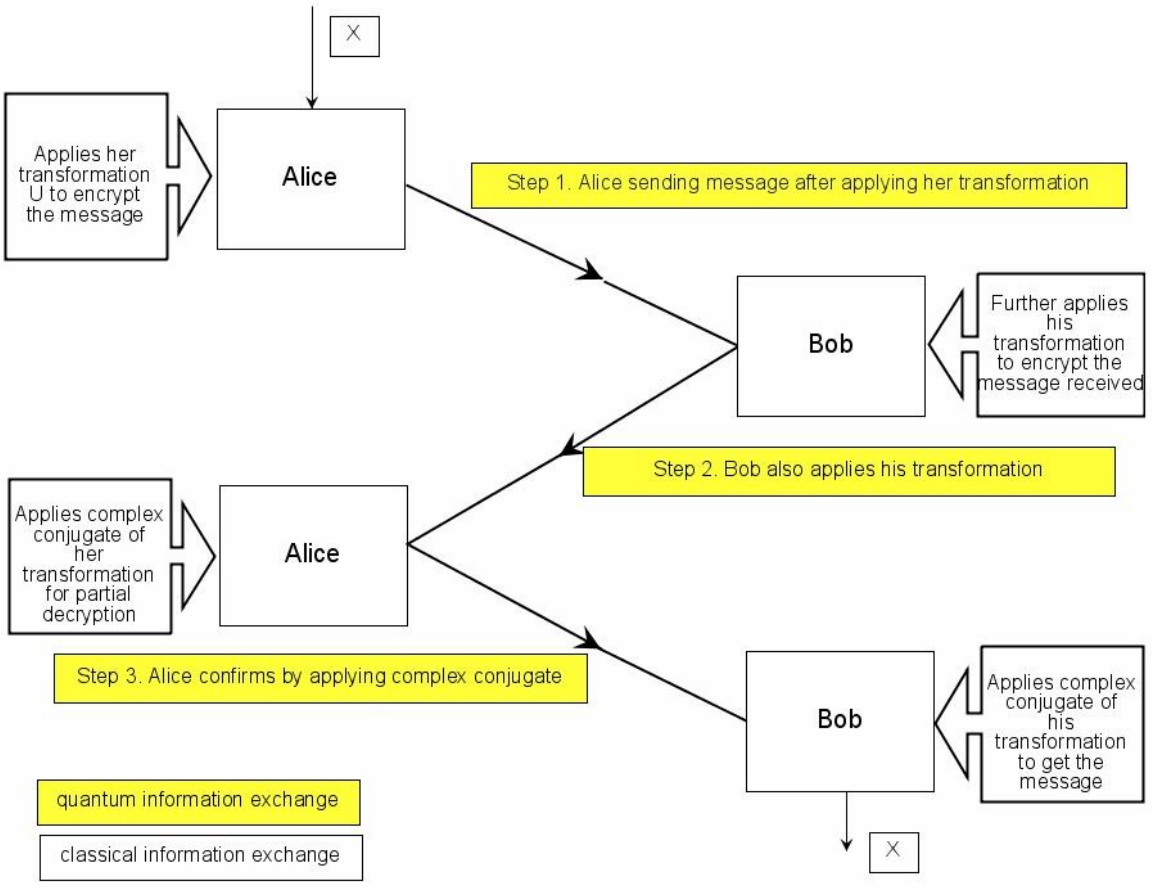

Figure 6: Kak's three-stage protocol

2.3 Classical Authentication Aided (CAA) Protocol

This section will describe the kind of attacks that can affect the efficiency of the previously explained quantum key distribution protocols. Then a protocol will be proposed which will try to avoid those attacks and will improve with help of classical authentication methods.

2.3.1 Types of Attacks Possible for QKD Protocols

There are many existing attacks for quantum cryptosystems like,

1. Photon Number Splitting (PNS) Attack.
2. Beam-splitting attack.
3. Random Number Generator Attack.
4. Side-channel Attack.
5. Man-in-the-Middle Attack.

Here we will discuss man-in-the-middle attack because the other attacks are mainly directed towards the implementation of the protocol rather than targeting the protocol itself.

The Man-in-the Middle or the Bucket-Brigade attack is a form of popular eavesdropping where Eve makes independent connections with the Alice and Bob and relays messages between them, making them believe that they are communicating directly to each other, whereas the communication is controlled by Eve. Also, Eve must be able to intercept all messages going between Alice and Bob and resend new ones, which is straightforward in most circumstances. Man-in-the-Middle attack works best when Eve can impersonate each endpoint to the satisfaction of the other. Hence most cryptographic protocols include some form of endpoint authentication specifically to prevent the Man-in-the-Middle attack. We will also introduce classical authentication methods in the modified Kak's three-stage protocol to enhance its security [23].

2.3.2 Man-in-the-middle Attack for Three-stage Protocol

Man-in-the-middle attack can affect both classical and quantum channels. Here Eve can pretend to be Bob to Alice and vice-versa. From reference to section 2.2.4, instead of U_B Eve selects U_C (which is also commutative) and fakes a response which looks similar to what Bob would have done. Eve pretends as Alice to Bob with the transformation U_D, which is commutative to U_B and instead of X sends a gibberish Y. So from interaction

with Alice he acquires value X and sends a junk Y to Bob and hence disables the protocol.

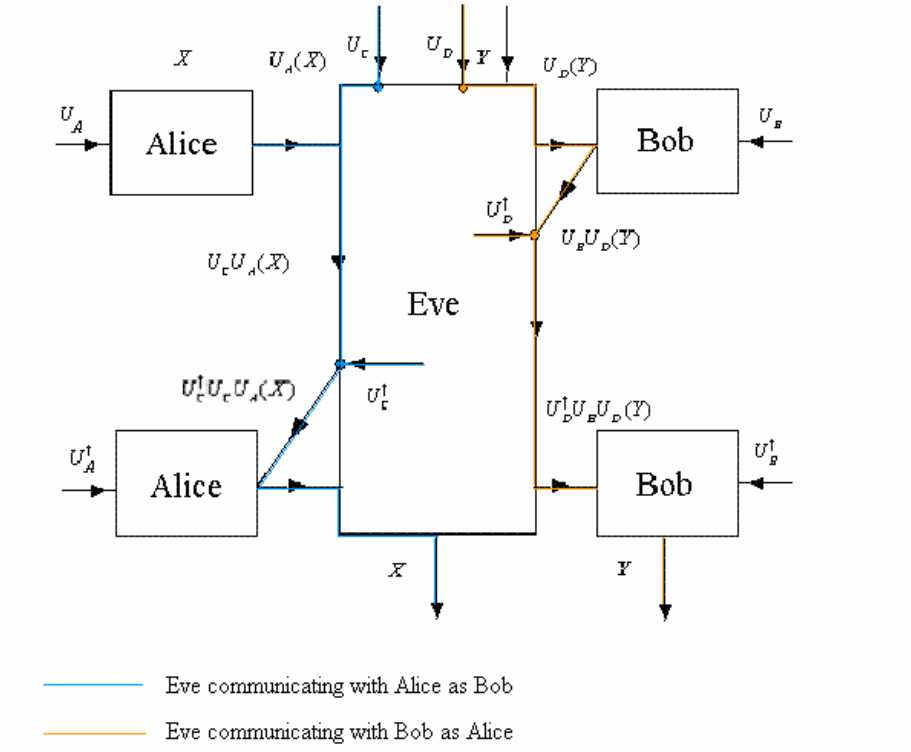

Figure 7: Three-stage protocol under Man-in-the-middle attack

EPR pairs can be used for a possibly secure three-stage protocol that can avoid man-in-the-middle attack. But while distributing the EPR pairs, they might get corrupt during the transit. So if the EPRs are not matched then the process will be aborted and this might cause delay. So in order to ensure security from man-in-the-middle attack and avoid the uncertainty regarding EPR pairs this paper proposes a hybrid model that uses classical authentication protocols to ensure security in three-stage quantum protocol.

2.3.3 Description of the Classical Authentication Aided Protocol

Here, we use modified version of the protocols proposed by Denning-Sacco [24] and Kehne et al [25], as the authentication protocol, alongside the qubits sent in each stage. It takes help from a central Key Distribution Center (KDC), which assigns the session key and work as the central authority for authentication.

Firstly, as this protocol uses classical bit sequence, we have to transform the bit sequence into qubits. A bit sequence of 01101… can be transformed into $|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle\ldots$, even; to increase the amount of reliability we can map 0 and 1 into more than one photon. Now what we are doing in each step is that we are sending a series of photon as in usual three-stage protocol and still using the authentication protocol. Each time Alice or Bob (or the KDC) gets the stream of photons; they convert the authentication part to classical information, then process it and again transform it into quantum information before transmitting. Say, $Q(.)$ is the function used to denote conversion of classical bits to quantum qubits. $Q^{-1}(.)$ is also used to get the classical bits inside the Alice, Bob and KDC units and are not shown in the protocol.

The protocol can be described as follows:

1. $A \rightarrow B$: $\quad Q(ID_A \| N_a) \| U_A(X)$

Alice sends quantum information of the nonce N_a and the ID along side the message to Bob.

2. $B \rightarrow KDC$: $\quad Q(ID_B \| N_b \| E_{K_b}[ID_A \| N_a \| T_b]) \| U_B U_A(X)$

Bob also sends his ID and nonce and encrypts Alice's ID, nonce and his timestamp using shared key between Bob and KDC. This initiates KDC to assign a session key.

3. $KDC \rightarrow A$: $\quad Q(E_{K_a}[ID_B \| N_a \| K_s \| T_b]) \| E_{K_b}[ID_A \| K_s \| T_b]) \| N_b) \| U_B U_A(X)$

KDC assigns a session key and prepares packages for Alice and Bob which include their own ID, session key and Bob's timestamp. Alice's nonce is encrypted inside Alice's package but Bob's nonce is kept open. Alice gets back his nonce and Alice is assured of its timeliness by the session key and ensured that it's not a replay. This block also verifies that Bob has received Alice's earlier message with help of Bob's ID.

4. $A \rightarrow B$: $\quad Q(E_{K_b}[ID_A \| K_s \| T_b]) \| E_{K_s}[N_b]) \| U_A^{\dagger} U_A U_B(X)$

Session key authenticates that the message came from Alice and is not a replay.

5. Once the string of qubits reaches Bob, he knows how many qubits are used for the authentication purpose. He checks those bits to verify the ID of Alice, which means that

Alice had received Bob's earlier message. He also gets back his nonce to make sure that it is not a replay message. Also the time-stamp and session key verifies the message. Then $U_B^\dagger$ can be applied on $U_B(X)$ to get X.

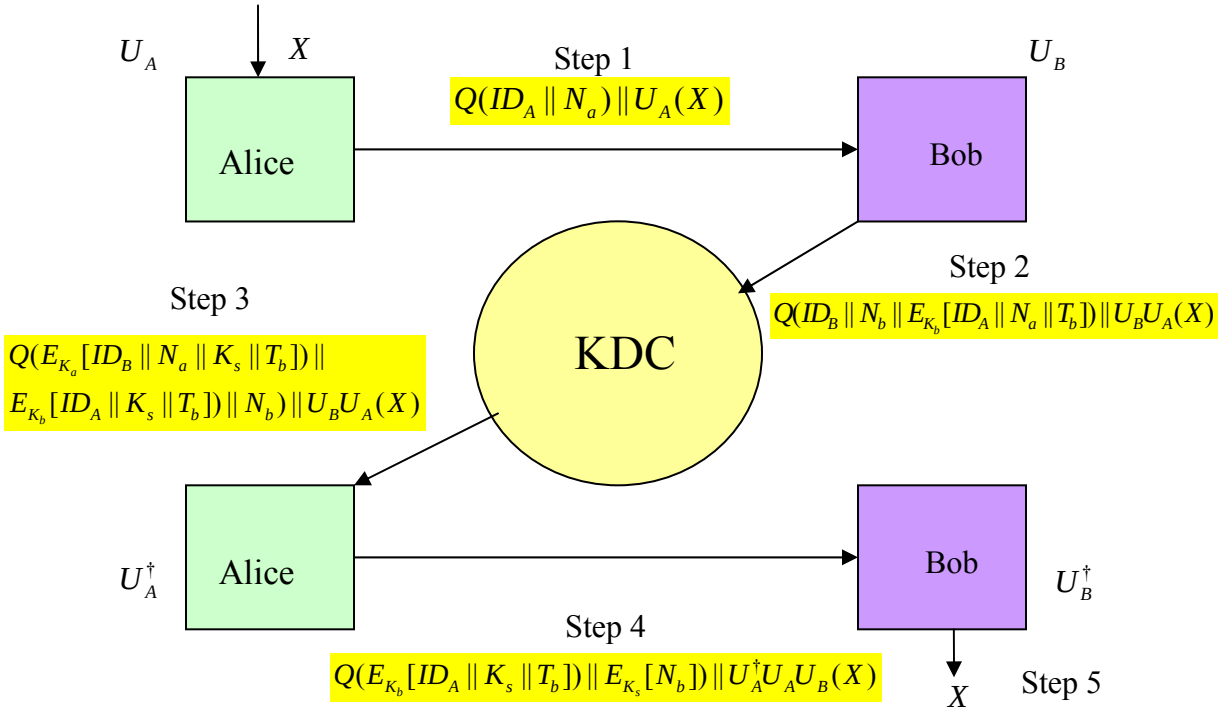

Figure 8: Classical Authentication Aided Three-stage Quantum Protocol

There are many inherent advantages of the proposed system. For, example, the KDC can't see the message in this system. Neither Bob nor Eve is capable of modifying or forging the message. Alice cannot disavow sending that message and simultaneously Bob cannot deny receiving the message later on. The transmission is quantum and hence non-reproducible. Synchronization throughout the network is not needed as the time-stamp is provided by Bob and hence will correspond to Bob's clock only. Suppress-reply attacks can be avoided because the nonces the recipients will choose are unpredictable to the sender. We will consider a few situations for this protocol and study what will happen under those circumstances.

- Case I:

What happens if transmitted bits are entangled?

By using an EPR pair Alice and Bob can share information known to themselves and avoid Eve reading the bit. But more complex situations can arise where entanglement might enable Eve to perform an attack. One of them can be performed if the secret key or the encryption system is made of entangled bits. Kuhn showed cases where an attacker could use quantum entanglement of photons to extract information without being detected [27].

Say, Alice and Bob share an EPR pair among themselves. If any one of them prepares the EPR pair it would enable one of them to know about which is the correct basis. Say, Alice prepares the EPR pair then she will send the bits to Bob and will also let Bob know about the basis in which she wants Bob to measure the qubits to make the encryption system perform successfully. She stores the quantum state of the first photon and delays measuring it. Suppose that when the time comes for Alice to open the commitment, she decides she would like the committed bit to read 0, which requires her to specify a state in the rectilinear basis. Because of the entanglement, Alice knows that if she and Bob measure in the same basis, they will get opposite results. Therefore, she can measure her photon in the rectilinear basis and tell Bob he has the opposite polarization, and she will always be right.

If Alice instead wishes the committed bit to read 1, she needs a state in the diagonal basis. But (|↔↕ 〉 - |↕↔ 〉)/√2 = (|↗↖ 〉 - |↖↗ 〉)/√2. So Alice can measure her particle in the diagonal basis and again be sure that Bob's measurement outcome will be opposite to hers. Quantum cheating allows Alice to change her mind at the last minute without being caught by Bob, thus totally defeating the purpose of bit commitment [22]. This phenomenon is called quantum cheating and can happen in the situation we have described, if the transmitted bits are entangled.

However, we can also use a third party to prevent this situation and protect the privacy of this communication. A trusted third party could be introduced, who will create an EPR pair and distribute the photons to Alice and Bob. So neither Alice nor Bob will have the upper hand to know what basis should be chosen to get the right results. Also, knowing the qubits of Alice and Bob, the third party authority could generate a string of qubits of same length. This string should be generated based on a certain function Γ, where Γ applied on Alice's qubit string, Bob's qubit string and the third party generated string would result in some pre-determined string. If Alice and Bob get a match, the protocol will go ahead or else it will be aborted.

An example of similar method but more specific has been described by Perkins [28]. The third party chosen bit string, which can also be called a master key, can be operated on the bit strings of Bob and Alice. Say the Γ is taken to be XOR here and the master key is 10011.

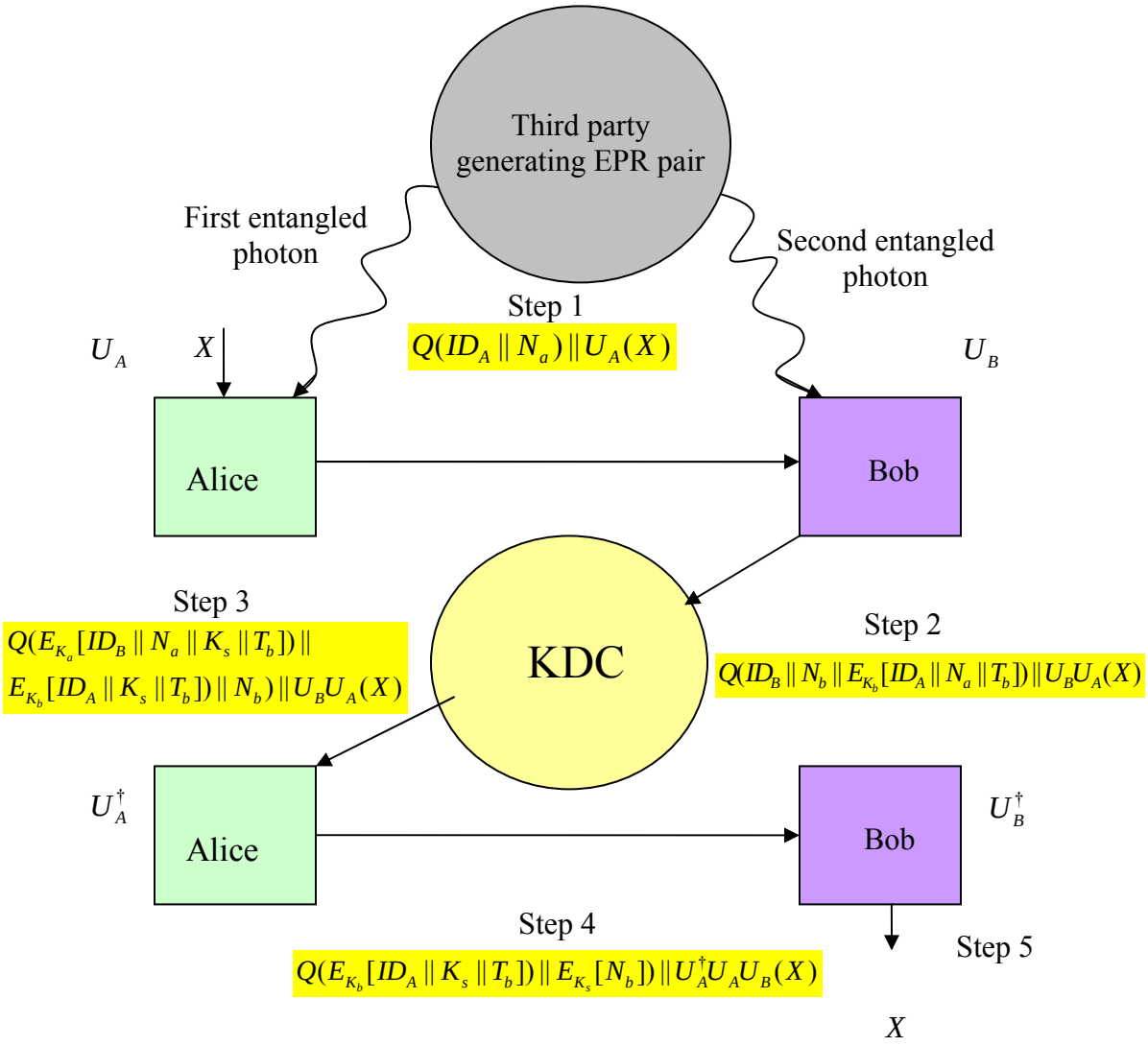

Figure 9: Authentication Aided Protocol with an EPR pair generating third party

Say entangled bit string for Alice reads as 11000. Then in order to produce a 5-bit zero string, Bob's entangled bit string should read 01011. If Alice's string remains same and Bob's string changes or vice versa then the function Γ will not produce an all-zero string, indicating tampering. Hence, the protocol will not proceed.

10011	Master Key	10011	Master Key	10011	Master Key
11000	Alice's string	11000	Alice's string	11001	Alice's string
(XOR) 01011	Bob's string	(XOR) 01111	Bob's string	(XOR) 01010	Bob's string
00000	Authentic	00100	Not authentic	00000	Authentic

- Case II:

What if there is noise?

In this section, by noise, we do not mean deliberate noise or noise from the attacks. We have discussed attacks in another section. So, we will mainly discuss about the channel noise or the noise coming from the medium.

There is no other way than usual error correction methods to discard noise. In fact Eve could disguise herself by posing as noise.

Dense wavelength-division multiplexing (DWDM) revolutionized data transmission technology by increasing the capacity signal of embedded fiber and is used for practical implementation of QKD network [25]. The generation of spontaneous anti-Stokes Raman noise (SASRN) in fiber places constraint on both the filtering requirements as well as the wavelength selection for QKD implementation through DWDM networking. The QKD wavelength must reside far enough (experimentally tested to be 1310 nm) outside both the DWDM spectrum and also the SASRN spectrum.

As in classical communication, successful QKD also depends on the signal-to-noise ratio (SNR). In classical communication signal power can be increased or the noise of the environment can be decreased to improve the SNR, but QKD uses a single photon as a qubit to carry the information and no pulse is allowed to contain more than one photon, so the only way to improve the SNR is to decrease the noise.

The SNR is defined as the average number of signal photons to the number of noise photons per pulse. With channel noise being similar to an attack, we have to eliminate it only by means of error-correction. But for satellite-to-ground communication through atmosphere, there could be a few other noise sources. Two of the main noise sources are dark counts and background light [30]. To improve the system by reducing the noise light and increasing the SNR, we can use the following filters.

1. Time-gate filter.

2. Frequency (wavelength) filter.

3. Spatial filter.

Error-correction methods for noise and anomalies caused by attacks are discussed in the next chapter.

3 Quantum Error-correction

Error-correction coding is essential both for transmission of classical information and for quantum information. During information transmission through a channel there is always a possibility that information is distorted because of the noise and assuming absence of noise in a channel is only an ideal situation. All quantum protocols are prone to errors to combat which one needs error-correction. Here we consider quantum errors and their correction methods for the Kak quantum cryptography protocol [16], [23] using the techniques of Shor and Steane [31], [32], [33].

Error-correction in quantum information is more complex than its classical counterpart. Efficacy of unconstrained error-correction has previously been questioned [34], [35]. The state of a qubit with redundancy may be described by the following equation:
$|\psi\rangle = a|0\rangle + b|1\rangle$
$(|000\rangle - |111\rangle)\sqrt{2}$, where a and b are complex numbers.

Quantum cryptography protocols like BB84 and its advanced versions have been tested with error-correction codes and different simulation results regarding it has also been published [36]. Here we present a possible error-correction method for the three-stage quantum cryptography protocol and analyze its security.

3.1 Principles of Quantum Error-correction

Generation of quantum errors can be contributed mainly by two prime factors:

1. Interaction of the information with environment, and
2. Erroneous behavior or wrong use of hardware.

Interaction with environment could lead to decoherence, as said earlier.

The second issue could give rise to different situations like:

1. There could be errors while preparing the initial states. Once there is an error in the initial state, it could propagate exponentially through the next steps. If the evolution of the state is characterized by a Hamiltonian $\hat{H}$, then the final state $|\psi_f\rangle$ can be denoted by $|\psi_f\rangle = e^{-i\hat{H}t}|\psi_i\rangle$, where the initial state is $|\psi_i\rangle$. If there is

an error of ε, in the k-th qubit of the state, then there will be a term $\sqrt{1-\varepsilon^2}$ multiplied to the $|\psi_i\rangle$ and in $|\psi_f\rangle$ also, the factor will remain unchanged due to the linearity in quantum mechanics.

2. Some times errors are contributed by hardwares. These are called unitary errors as the error term $\hat{\eta}$ is accumulated to the noiseless Hamiltonian $\hat{H}_0$ to produce $\hat{H}_\eta$ i.e, $\hat{H}_\eta = \hat{\eta} + \hat{H}_0$.

   So transformation of $|\psi_i\rangle$ gives us $e^{-i(\hat{\eta}+\hat{H}_0)t}|\psi_i\rangle = e^{-i\hat{\eta}t}.e^{-i\hat{H}_0 t}|\psi_i\rangle \equiv e^{-i\hat{\eta}t}.|\psi_f\rangle$, which can be expanded to its series form $(1-i\hat{\eta}t)|\psi_f\rangle$ to show that error probability grows in time.

3. Errors also happen while interpreting the outputs from a quantum system.

As quantum errors are dissimilar to the classical errors the problems encountered while correcting quantum errors are different from classical error correction.

1. Unlike classical errors, quantum error is continuous. Due to superposition, there may be errors in the magnitudes of the coefficients a and b, which is called amplitude decoherence and errors in the phase of the coefficients, which is called phase decoherence.

2. Unlike classical error correction, inserting redundancy is not a possibility in quantum error correction as a qubit can not be copied.

3. If we want to correct quantum errors, we need to measure the state of the system and measurement of a quantum state will result to its collapse.

3.2 Literature Study and Existing Error-correction Codes

The basic error correction codes for quantum computation are,

1. Bit-flip code and

2. Phase-flip code.

The bit flip code changes the qubit(s) of a corrupted state to correct the errors in bits and the phase flip changes the phase of a state to correct an erroneous phase of a state.

Shor [32] came up with an algorithm that consisted of both the bit flip and phase flip codes and worked as a more generalized form. In this process $|0\rangle$ and $|1\rangle$ are first encoded as $|+++\rangle$ and $|---\rangle$ respectively, using phase flip code. Then each $|+\rangle$ and $|-\rangle$ is encoded as $(|000\rangle+|111\rangle)\sqrt{2}$ and $(|000\rangle-|111\rangle)\sqrt{2}$ respectively, using bit flip code.

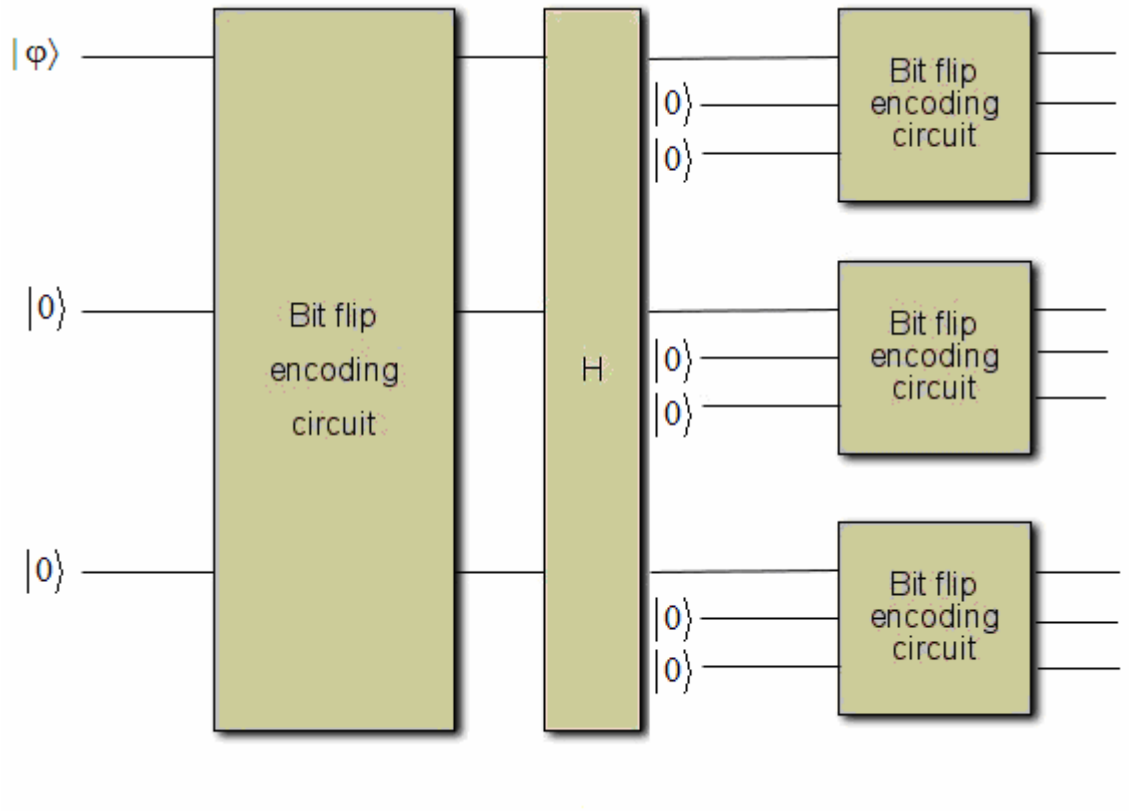

Figure 10: Encoding circuit for Shor code

CSS (Calderbank-Shor-Steane) [31] codes are quantum codes that help us to detect and correct large qubit errors. CSS codes are derived from classical linear codes.

Say, there are two classical linear codes, $C_1[n, k_1]$ and $C_2[n, k_2]$ such that $C_2 \subset C_1$. The code encodes $(k_1 - k_2)$ logical qubits in n physical qubits, so this code is $[n, k_1 - k_2]$. A quantum $[n, k_1 - k_2]$ code CSS(C_1, C_2) is capable of correcting errors on t qubits, where C_1 and $C_2^{\perp}$ both correct t errors. The encoding is a vector space spanned by all states constructed by taking a codeword $x \in C_1$ and then adding to it the whole of C_2:

$|x +_2 C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x +_2 y\rangle$, where $|C_2|$ is the number of elements in C_2.

If we take the $C_1[7,4]$ Hamming code and its $C_2[7,3]$ dual then CSS(C_1, C_2) is going to be [7,1] code. The code words of $C_1[7,4]$ are spanned by the columns of the generator matrix G, where

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

The code words of $C_2[7,3]$ are spanned by the rows of the parity check matrix H, where

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

From G and H, CSS(C_1, C_2) can be constructed and the elements are calculated to be,

$$|0\rangle_L = (|0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle + |0111100\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle)/\sqrt{8}$$

$$|1\rangle_L = (|1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle + |1000011\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle)/\sqrt{8}$$

This seven qubit encoding is named after its inventor as the Steane Code [33].

3.3 New Error-correction Codes

The following section will discuss how we propose to correct errors in Kak's three stage protocol and Classical Authentication aided protocol.

3.3.1 Error-correction for Kak's Protocol

Some of the earlier papers on the three-stage quantum cryptography protocol [16],[23] did not consider the question of random errors. We have already discussed Kak's three stage protocol in 2.2.4, so with reference to that we further extend on it.

Now, we have to be sure that the X, which is being encoded by U_A is same as the one we get at the last step, after decoding the message by U_B. There could be errors caused by the channels or the hardware and hence we have to find a way to eliminate the errors, if needed.

Say, X has been modified to X', then we can check the errors in the message by sending it back to Alice. In no other quantum cryptographic protocol, error correction can be made by sending the key back to Alice. Here the quantum key can be sent back to Alice in the opposite order that has been described in the protocol.

Step 1: Bob applies a unitary transformation U_B on quantum information X' and sends the qubits to Alice.

Step 2: Alice applies U_A on the received qubits U_B, which gives $U_A U_B(X')$ and sends it back to Bob.

Step 3: Bob applies $U_B^\dagger$ (transpose of the complex conjugate of U_B) on the received qubits to get $U_B^\dagger U_A U_B(X') = U_B^\dagger U_B U_A(X') = U_A(X')$ and sends it back to Alice.

Alice then applies $U_A^\dagger$ on $U_A(X')$ to get the information X'.

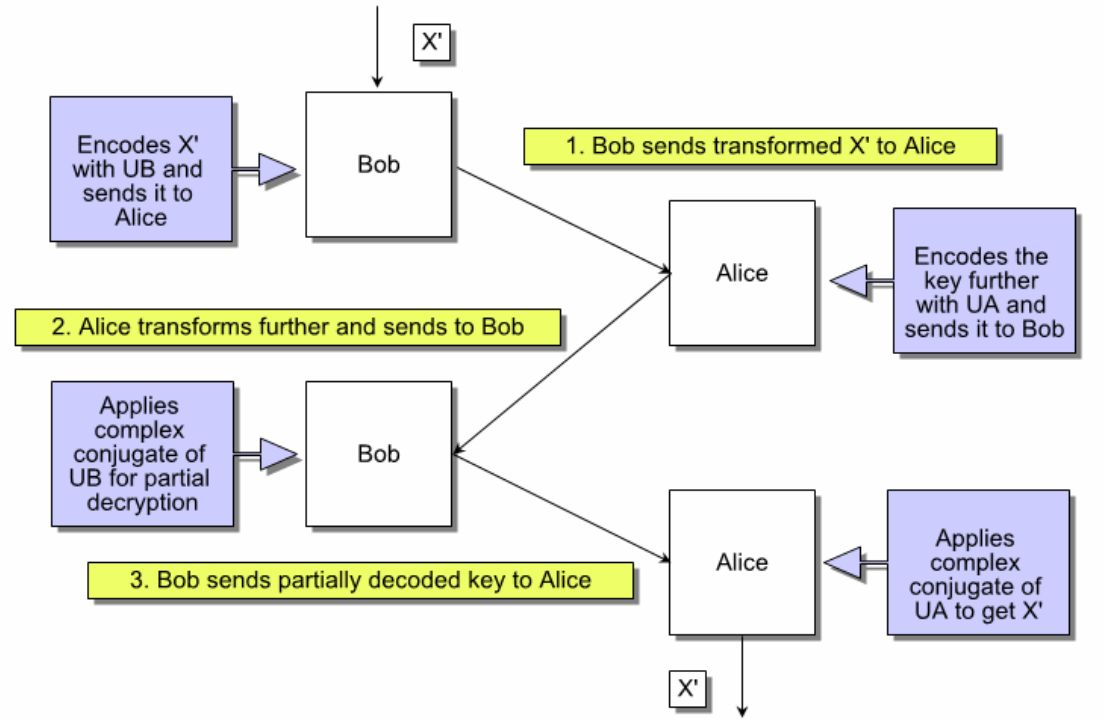

Figure 11: Sending the message with error to Alice

Once Alice gets X' she can compare it with X and create a transformation, which when applied to the information with error will give rise to X. Such hardware can be installed inside Bob's unit so that X' can be corrected to X. Each time the communication channel is changed the transformation function needs to be recalculated and hence the circuit in Bob's unit needs to be changed as well.

- Error Control Method:

In order to achieve error control, as described in the previous section, one merely requires that Bob send back the bits he has received (which represent the key) to Alice, using transformations in exactly the same way as they were carried out in the forward transmission of the key. This is shown in Figure 12.

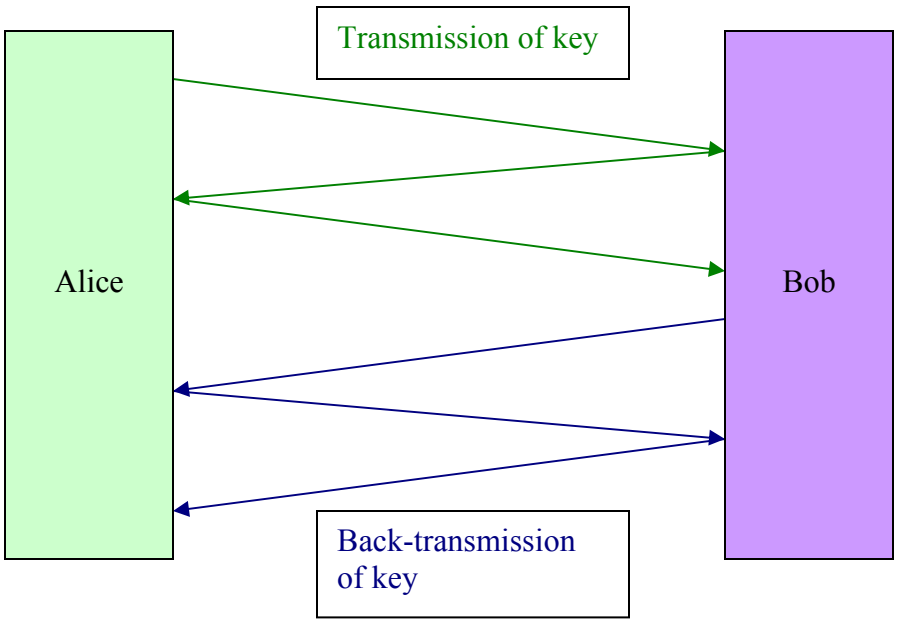

Figure 12: The Back-transmission of the Secret Key

Alice needs to check what she has received with what had been transmitted. If there are random errors or malicious distortions, Alice would know that quite readily.

3.3.2 Error-correction for Classical Authentication Aided Protocol

In CAA transmission of quantum super-positions is undesired and it is also the same in BB84 or in Kak's protocol. Given that CSS codes are used freely to correct BB84, CAA

protocol will also be able to make use of it. Low Density Parity Check (LDPC) [37] algorithm is known for little interactive communication and hence used to produce a CSS code that will make the error corrections.

Construction of the CSS code based on LDPC codes [38] can be done in following way:

1. For code C_1 any LDPC code is chosen, which is defined by a $M \times N$ parity-check matrix H_1.

2. H_1 is arranged based on ascending order of column weights and an $M \times (N-M)$ matrix H_1' is separated from it.

3. The row vectors of the matrix H_1', which is of length $N-M$, will act as encode bits. They will be encoded to code words in C_1 and generate $M \times N$ parity-check matrix H_2 by the set of the code words in C_1.

4. The code $C_2^{\perp}$ can be defined by H_2.

As the parity-check matrix H_2 has the code words from C_1, it can be said $H_1 H_2^T = 0$. Hence, C_1 and C_2 satisfies the main criterion for CSS, $C_1 \supset C_2$. Any arbitrary LDPC code can be used for this purpose. It pseudo randomly creates C_2, by only choosing C_1.

One disadvantage of using LDPC is that it uses a pessimistic lower bound estimate of the error rate. Privacy amplification, at a later stage, removes information disclosed during the error correction process. Implementation of this error-correction requires that Alice and Bob both generate the same random factor graph. Once Alice and Bob comes to know the number of bits they will correct and the measured error rate, they seed a pseudo random number from their one-time pad to generate a factor graph and assume that Eve will not know which one among the (say, 2^{256}) factor graphs they are using.

4 Implementation Ideas and Related Costs

In the absence of proper laboratory, equipments and facilities we could not perform experimental testing and all of the work has been done theoretically. But from other literatures on practical implementation of BB84, we have found out information on practical implementation and base our hypothesis on that.

Duligall et al [39] presented a low cost QKD system that is aimed at protecting consumer transactions. A little compromise on the performance is made while retaining the high security associated with quantum protocols. The design is based on a future hand-held e-credit/debit card, which communicates with consumer outlets (say, ATM) using free space optics. This device then also acts as storage for secrets shared only with the bank (or some central database) which can be used to protect online transactions. With quantum key distribution protecting the interface between the ATM and the user's handheld device, there is no possibility of an eavesdropper gaining key information via 'skimming' attacks where the key and card details are read using a so-called 'false front' on the ATM itself.

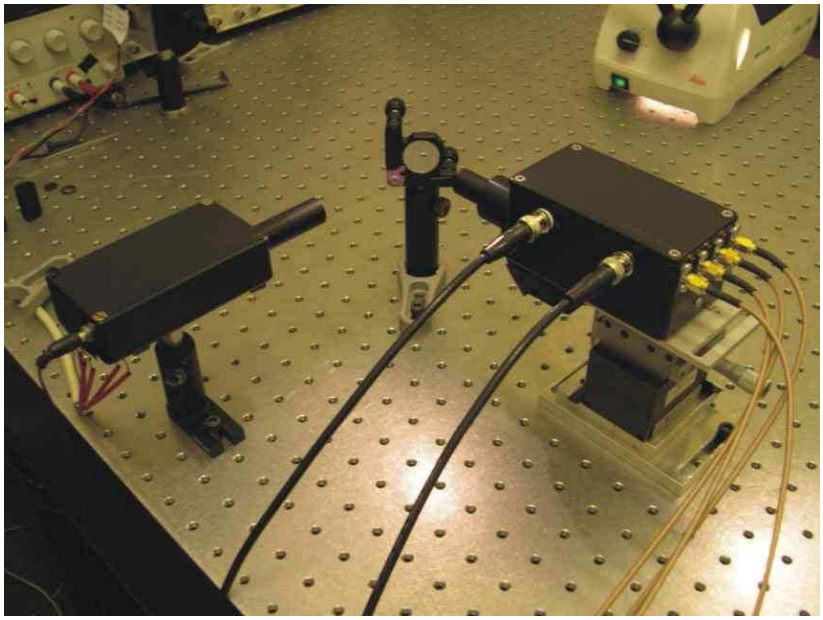

Figure 13: The quantum cryptography kit (photograph)

The system described here is based on the BB84 protocol and instead of dedicated optical fiber communication it uses free space communication, which is a very practical and

emerging form of communication for QKD. The error rate threshold is set to be 11%, so whenever the error rate exceeds 11% the process is aborted or the data is discarded.

- Alice Module for BB84

The Alice module uses the IC components in a driver circuit which produces sub-5ns pulses. The driver pulses and output from a digital input/output card (NuDAQ, Adlink PCI-7300A) are then ANDed and passed to one of four AlInGaP, miniature, red-orange LEDs (Agilent, HLMA-QH00). An external oven-stabilized clock (C-MAC Frequency Products, CFPO-6) regulates the output from the NuDAQ card and a random bit string, generated by a quantum random number generator (QRNG), (idQuantique, Quantis) is passed to the Alice module, which triggers LED to glow as it is recorded. The driver pulses are reproduced at a rate of 5MHz.

The LEDs are attached to a holder, with dichroic sheet polarizer, orientated in each of the four polarization states, 0^0, 45^0, 90^0 and 135^0, placed over each output. Alice and Bob communicate via internet but can be replaced by an IrDA infra red communication channel.

- Bob Module for BB84

Bob module contains four silicon avalanche photodiodes (Perkin Elmer, C30902S) which are cooled down to - 10^0 C and maintained by a temperature controlling circuit. Since the detectors operate at a relatively high voltage, DC-DC converter (EMCO, Q03-5) for high voltage was included so that the Bob module can run off a low voltage supply. A discriminator circuit takes the output from the detectors and converts it to a readable positive pulse. Time of arrival information is recorded by a time interval analyzer card (TIA, GuideTech, GT653).

In a similar setup to the Alice module, the dichroic sheet polarizer was placed in front of each detector orientated in the four polarization directions with the diffraction grating in place. In addition to this arrangement, a 632.8 ± 3 *nm* filter was included to reduce the background count and a 50mm focal length lens to collect the beams from Alice and focus it down onto the detectors.

The bit error rate (BER) for each channel was estimated from data taken during key exchange.

$BER = \frac{N_{wrong}}{N_{total}}$, where N_{wrong} is the number of bits in error and N_{total} is the number of bits received in total.

Table 5. BER values at 0^0, 45^0, 90^0 and 135^0

Channel	*Bit Error Rate* (%)
0^0	1.32
45^0	2.54
90^0	2.20
135^0	4.75

- Modifications for Classical Authentication Aided Protocol

In the setup explained above Alice and Bob module has been constructed based on the BB84 protocol, where Bob only needs the detector module but for both Kak's protocol and CAA protocol Alice also needs the detectors. So the set of four Silicon Avalanche photodiodes along with the discriminator circuit to get the output pulses from the detectors will also be needed inside the Alice module.

For Kak's protocol, the number of times qubit communication is made between Alice and Bob is three, which in case of BB84 protocol is one. So error-correction overheads for qubit transmission has to be considered three times, compared to one in BB84.

For CAA protocol, an extra Key Distribution Center (KDC) module has to be introduced. We have some bit to qubit conversions in all the modules as CAA protocols takes help of classical authentication and yet translates the bits into qubits for quantum transmission. So Alice, Bob and KDC, all of them, will need the driver circuit, the NuDAQ and the four set of AlInGaP LEDs. All of them should be able to prepare string of qubits based on digital inputs through NuDAQ. Added to that, Alice should also have the QRNG module to generate the random string of qubits before staging the first step of the protocol. Also all of Alice, Bob and KDC module need the detectors and the output module to get the

output pulses. In CAA, the number of quantum transmission becomes four with introduction of KDC.

5 Conclusions and Future Work

The Classical Authentication Aided protocol works on the basic principle of Kak's protocol and modifies its security with classical authentication algorithms.

The difficulty of generating single photons makes CAA protocol more secure than other QKD protocols like BB84, which require use of single photons. Since all the photons, be it a single photon or multiple photons, go through private transformations in the Kak protocol or the CAA protocol, the information remains protected until the complex conjugate transformation is applied. In contrast, beam-splitting can easily break the inherent quantum security in BB84 and in order to avoid it measures may be taken that consume both time and money. Thus CAA protocol may be used with greater confidence in its unbreakability than BB84.

Although CAA protocol is secure against beam-splitting it can be successfully subjected to man-in-the-middle attack. To deal with such an attack timestamps, IDs, session keys, nonces and encryption keys are used for verification. If the authentication process detects any problem, the process is aborted. In this protocol we are dependent on the KDC and we need the KDC to be trustworthy.

There are many inherent advantages of the system. It includes all the advantage that comes with the authentication methods but makes it more complex and more expensive in terms of practical implementation. The Key distribution centre can not see the message. Alice and Bob both exchange their IDs, so later none of them can disavow receiving the message. Synchronization is not needed because time stamp is already provided by Bob. Introduction of nonce will help avoiding suppress-reply attack.

As the LDPC code is a code that allows data transmission very close to the Shannon limit (which is the maximum), the CSS code explained is also expected to be and suitable to enhance performance of CAA protocol.

However, the practical implementation section was based on knowledge of quantum cryptography related equipments by other groups. We could not implement the discussed systems due to unavailability of proper infrastructure and facilities. So until the CAA model is tested in the proposed way, there is no other way to know how efficiently it works. Also even if it works efficiently, optimizing its cost might pose a challenge and it remains to be seen whether it can be commercially used at a later stage.

Bibliography

[1] http://www.nytimes.com/2007/04/08/business/yourmoney/08slip.html?pagewanted=print

[2] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller and J. E. Nordholt, "Long-distance quantum key distribution in optical fibre." arXiv: quant-ph/0607177

[3] Tobias Schmitt-Manderbach, HenningWeier, Martin Furst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km." Phys. Rev. Lett. 98, 010504 (2007)

[4] http://www.newscientist.com/channel/fundamentals/quantum-world/dn4914

[5] http://spectrum.ieee.org/oct07/5634

[6] S. Kak, "On quantum numbers and uncertainty." Nuovo Cimento, vol. 33B, 1976, pp. 530-534.

[7] S. Kak, "On quantum numbers and uncertainty II." Nuovo Cimento, vol. 41B, 1977, pp. 1-6.

[8] S. Kak, "On information associated with an object." Proc. Indian National Science Academy, vol. 50, 1984, pp. 386-396.

[9] R. P. Feynman, "Simulating physics with computers." Int. Journal of Theoretical Physics, vol. 21, 1982, pp. 467-488.

[10] M.A Nielsen, I.L. Chuang, "Quantum computation and Quantum information." Cambridge University Press, 2000.

[11] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public-key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179.

[12] http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

[13] William Stallings, "Cryptography and Network Security". Third edition. Pearson Education, 2003.

[14] Bennett, Charles H.,"Quantum cryptography using any two non-orthogonal states", Physical Review Letters, Vol. 68, No. 21, 25 May 1992, pp 3121 - 3124.

[15] Ekert, Artur K., "Quantum cryptography based on Bell's theorem", Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661 – 663

[16] Subhash Kak, "A Three-Stage Quantum Cryptography Protocol." Foundations of Physics Letters 19, 293, 2006; arXiv: quant-ph/0503027.

[17] M. Dusek, N. Lutkenhaus, and M. Hendrych, Progress in Optics, Vol. 39, 381, Edt. E. Wolf, Elsevier (2006), ArXiv: quant-ph/0601207.

[18] Samuel J. Lomonaco, Jr., "A Quick Glance at Quantum Cryptography", arXiv: quant-ph/9811056

[19] Busch, Paul, Pekka J. Lahti, and Peter Mittelstaedt, "The Quantum Theory of Measurement," Springer-Verlag, New York (1991).

[20] Ekert, Artur K., Bruno Huttner, G. Massimo Palma, and Asher Peres, "Eavesdropping on quantum-cryptographical systems", Phys. Rev. A, Vol. 50, No 2, August 1994, pp 1047-1056.

[21] Einstein, A., B. Podolsky, N. Rosen, "Can quantum, mechanical description of physical reality be considered complete?" Phys. Rev. 47, 777 (1935); D. Bohm "Quantum Theory", Prentice-Hall, Englewood Cliffs, NJ (1951).

[22] K. Svozil, "Feasibility of the Interlock Protocol against Man-in-the-Middle Attacks on Quantum Cryptography." arXiv: quant-ph/0501062

[23] Partha Basuchowdhuri, "Classical Authentication Aided Three-stage Quantum Protocol." ; arXiv: cs/0605083

[24] D. Denning and G. Sacco, "Timestamps in key distribution protocols." Communications of the ACM, 24(8):533-536, August 1981.

[25] A. Kehne, J. Schonwalder, and H. Langendorfer, "A Nonce-Based Protocol for Multiple Authentications" *Operating Systems Review*, October 1992.

[26] Lo, Hoi-Kwong, and H.F. Chau, "Is Quantum Bit Commitment Really Possible?" Phys. Rev. Lett. 78, (1997), p3410-3413.

[27] http://www.commsdesign.com/showArticle.jhtml?articleID=29106041

[28] W. Perkins, "Trusted certificates in quantum cryptography." arXiv: cs/0603046

[29] P, Toliver, R.J. Runser, T.E. Chapuran, S. McNown, M.S. Goodman, J. Jackel, R.J. Hughes, C.G. Peterson, K. McCabe, J.E. Nordholt, K. Tyagi, P. Hiskett, N. Dallman, "Impact of spontaneous anti-Stokes Raman scattering on QKD+DWDM

networking" Lasers and Electro-Optics Society, 2004. LEOS 2004. The 17th Annual Meeting of the IEEE, 2004, Volume: 2, P(s): 491- 492

[30] Miao Er-long, Han Zheng-fu, Gong Shun-sheng, Zhang Tao, Diao Da-Sheng and Guo Guang-Can, "Background noise of satellite-to-ground quantum key distribution" New Journal of Physics **7** (2005) 215

[31] A.R. Calderbank and P.W. Shor, "Good quantum error-correcting codes exist." arXiv: quant-ph/9512032.

[32] P.W. Shor, "Fault-tolerant quantum computation," arXiv:quant-ph/9605011

[33] A.M. Steane, "Simple quantum error correcting codes," arXiv: quant-ph/9605021

[34] S. Kak, "General qubit errors cannot be corrected." Information Sciences, 152, 195-202, 2003; quant-ph/0206144.

[35] S. Kak, "Are quantum computing models realistic?" ACM Ubiquity, 7 (11): 1-9, 2006; arXiv:quant-ph/0110040

[36] M. Sharifi and H. Azizi, "A Simulative Comparison of BB84 Protocol with its Improved Version", Journal of Computer Science & Technology, Volume 7, No. 3, pp. 204-208, October 2007

[37] R. G. Gallager, "Low-density parity-check codes," Cambridge, MA: MIT Press, 1963; preliminary version in *IRE Trans. On Inf. Theory*, vol. 8, pp. 21-28, Jan. 1962.

[38] Maki Ohata and Kanta Matsuura, "Constructing CSS Codes with LDPC Codes for the BB84 Quantum Key Distribution Protocol." arXiv: quant-ph/0702184v3

[39] J L Duligall, M S Godfrey, K A Harrison, W J Munro and J G Rarity, "Low Cost and Compact Quantum Key Distribution" arXiv: quant-ph/0608213v2

[40] S. Kak, "Quantum information and entropy." Int. Journal of Theoretical Physics, vol. 46, pp. 860-876; arXiv:quant-ph/0605096

Vita

Partha Basuchowdhuri was born in Calcutta, India. He received his Bachelor of Engineering degree from the department of Electronics and Telecommunication Engineering of Bengal Engineering College (presently Bengal Engineering and Science University), WB (est. 1856) in 2003. He is presently pursuing a dual master's degree in Louisiana State University in the departments of Electrical & Computer Engineering and Computer Science. His research interests consist of information security (quantum and classical cryptography based) and data mining (graph mining, clustering).