Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.28-39 | Page No: 28-39 | Section: Article

# Eavesdropper Detection using Bb84 Protocol in Quantum Cryptography

**S. Jothi** is an Assistant Professor in the Department of Computer Science at Jayaraj Annapackiam College for Women, Tamil Nadu.

**A. Vijayarega** is an Assistant Professor in the Department of Computer Science at Jayaraj Annapackiam College for Women, Tamil Nadu.

**Abstract**

The recent application of the principles of quantum mechanics to cryptography has led to a remarkable new dimension in secret communication. Quantum Cryptography uses the principles of Quantum Mechanics to implement a cryptographic system. The key problem which is solved by using quantum techniques is that of eavesdropping detection. Conventional secret-key cryptography techniques require the communication of a secret key prior to message exchange. Quantum principles can be used to detect eavesdropping probabilistically when it occurs. The bits are represented as qubits, physically modeled by photons, and communicated over a quantum channel. The polarization states of photons represent 0's and 1's. As a result of these new developments, it is now possible to construct cryptographic communication systems which detect unauthorized eavesdropping should it occur, and which give a guarantee of no eavesdropping should it not occur.

**Keywords**: Secret communication, Eavesdropping, Photons, Qubits, Quantum channel, Communication Channel, one-time pad, BB84 protocol.

## Introduction

A quantum computer is a computational device modeled on the quantum mechanical concepts like superposition and entanglement. These devices use some quantum phenomenon (like polarization of light) to represent the bits and operate on them using principles of quantum mechanics to manipulate the state space. The state space in a quantum computer is probabilistic in nature and hence has the potential to cover exponential number of states while doing computation. This opens an avenue for computational speed ups using a quantum computer. Similarly, quantum cryptography technique make extensive use of underlying principles of quantum mechanics for ensuring secure cryptography, which is not only resistant to eavesdropping (again due to probabilistic nature of it), but also has the potential to inform the communicating parties if a conversation has been compromised. Conventional cryptosystems have always relied on the difficulty of working with large numbers.

## Quantum Algorithms

### *Qubit*

A qubit or a quantum bit is the basic unit of computation in a quantum computer. Physically, a qubit can be thought of as an electron in a Hydrogen atom. There are two possible states an electron in a hydrogen atom can be in: the ground and the excited state. The ground state corresponds to the value of the qubit being 0, and the excited state corresponds to 1. We represent the ground state as $|0 >$ and excited state as $|1 >$. By the basic principles of quantum mechanics, the general state (denoted $|a >$) of an electron is given by a superposition of these two states.

$$|a> = a_0|0 > + a_1 \; |1 >$$

where $a_1$, $a_2$ € an and $|a_1|_2 + |a_2|^2 = 1$. By this we mean that if a measurement is made on the state of the electron. We find it to be $|0 >$ with probability $|a_1|^2$ and $|1 >$ with probability $|a_2 \;|_2$

**Entanglement**

If we have two electrons then we have four possible states that the electrons can be in (00, 01, 11, 10), each of these states has some probability, and joint state is represented as :

$$|a > = a_{00}|00 > + a_{01}|01> + a_{10} \; |10 > + a_{11}|11 >$$

**a01** **a11**

$$\mathbf{|a > = -------------- \; | \; 01 > + -------------- \; |11 >}$$

where

$$|a_{00}| \; |+ \; |a_{01}| \; |+ \; |a_{10} \; | \; |+ \; | \; a_{11}| \; ^2 =1$$

In general we can not specify the state of each individual electron alone. The electrons are said to be entangled. If we measure the value of one of the qubits, then the joint states are restricted to the ones the qubit measured has the value measured. In the new state the values of the coefficients scale up so that the sum of the squares of the coefficients adds up to 1. In the above equation, if we measure the value of the second qubit, and its value is 1, then the new joint state is: to see the power of this concept, consider the case when the coefficients in the equation above are $a_{00} = a_{11} = 0$, $a_{01} = a_{10} =1/(2)1/2$. If the two electrons are generated in a joint state of this form, then they will be so forever. Consider two electrons that were generated together with this joint state. Now even if we separate these two electrons to distances far away, the joint state is still maintained, and if we measure the value of the second qubit, then the value of the first qubit gets fixed as its complement. If we get the value 1, then $|a = |01$. This happens even though the electrons may be large distances away. Thus quantum information travels faster than the speed of light.

## Quantum cryptography

Quantum cryptography[1] involves the use of quantum techniques to further secure conventional cryptographic processes. One aspect in which quantum principles find good use is in key exchange. In Symmetric key cryptography to send a secret message by using

### *Brute force method*

Put the message in a safe and send the unlock key which is a copy of the lock key. Make sure the receiver gets the package and the receiver can open the safe and no one else.

*Informational method: encrypt (code) and decrypt (decode)*

M = Set of possible messages, K is set of keys

E: M×K  M encryption function

D: M×K  M decryption function

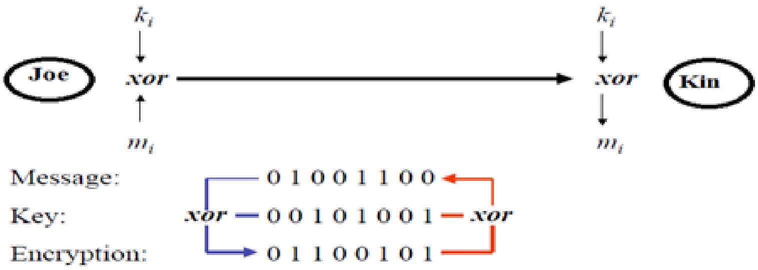
M′ = E(M,k) is n message M encrypted with key k

D (M′,k) =D(E(M,k),k) =M.

M′ should give as little information on M as possible if k is unknown.

Conventional secret-key cryptography requires the exchange of a mutual "one-time pad" to be perfectly secure. The term "one-time pad" refers to any method of encryption where each byte of the plaintext is enciphered using one byte of the key stream, and each key byte is used one time then never used again. The key stream for a one-time pad must be a true-random stream, meaning that every key byte can take any of the values 0 to 255 with equal likelihood, and independently of the values of all other key bytes.

## One Time Pad:



The encrypted message (ciphertext) is the same as before, even though the message is completely different. An opponent who intercepts the encrypted message but knows nothing about the random standard text gets no information about the original

[1] A. Ekert, "What is quantum cryptography", 1995. Cfr. URL: http:// www.qubit.org/index.html. (accessed on 25/Jan/2013).

message, whether it might be **ATTACK** or **GIVEUP** or any other six-letter message. Given any message at all, one could construct a standard text so that the message is encrypted to yield the cipher text RJUORC. An opponent intercepting the cipher text has no way to favor one message over another. It is in this sense that the one-time pad is perfect.

Step 1: Encryption and decryption function:

- M ÍK = {0,1}n, P[k] = 1/2n
- E(M,k) =M + k
- D(M′,k) =M′+ k

Step 2 : Properties

- D(E(M,k),k) = (M + k) + k =M + (k + k) =M + 0n =M
- P[M|M′] =1/|M|.
- Knowledge ofM? gives no information onMif k is unknown.

Step 3 : We could also useK =M is a subset of {0,1}n.

Step 4 : Or M =K is a subset of G (group), E(M, k) =Mk and D(M′,k) =M′k$^{-1.}$

Step 5 : This is the only provably unconditionally secure protocol known.

In example of One - Time Pad, one uses RQBOPS as the standard text, assuming these are 6 letters chosen completely at random, and suppose the message is the same. Then encryption uses the same method as with the Beale Cipher, which is a random string of letters.

| | | |
|---|---|---|
| Standard text (random key) | : | **RQBOPS** |
| Message | : | **ATTACK** |
| Encrypted message | : | **RJUORC** |

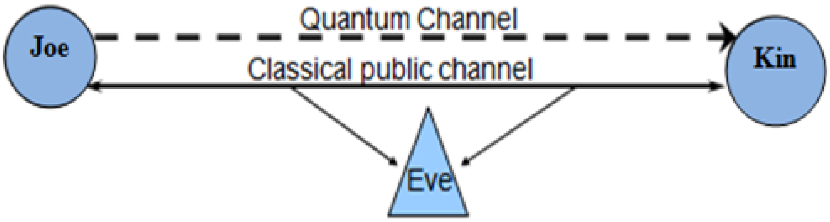
So, for example, the third column uses the letter B, representing a rotation of 1, to transform the plaintext letter T into the ciphertext letter U. The receiver must have the same random string of letters around for decryption: **RQBOPS** in this case. As the important part of this discussion, I want to show that this method is perfect as long as the random standard text letters are kept secret. Suppose the message is GIVEUP instead of **ATTACK**. If one had started with random letters **LBYKXN** as the standard text, instead of the letters **RQBOPS**, then the encryption would have taken the form:

```
Standard text (random key): LBYKXN
Message:                    GIVEUP
Encrypted message:          RJUORC
```

This can be practically achieved using quantum channels. A quantum channel is a communication channel where a bit is represented by the state of a two-state quantum system. There have been multiple algorithms developed to harness this advantage and establish the secure exchange of a key [BB84]. We look at one of these algorithms, developed by Bennett and Brassard

## The BB84 protocol

The key exchange according to this method can be divided into two stages, where the communication happens over a quantum channel and over a classical public channel respectively. The biggest advantage of this protocol is that it detects eavesdropping if it has occurred, with very high precision.



BB84 protocol was proposed by Bennett and Brassard (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 and also over free space for a distance of over one hundred meters. 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. The following describes the BB84 protocol in terms of the polarization states of a single photon:

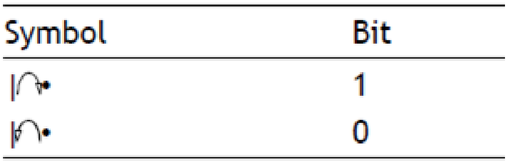
## Underlying Quantum Principles

Joe and Kin use a quantum system in which quantum bits are represented by the polarization state of photons. The photons can have one of two polarization states in either of two bases. The basis states are orthogonal in the quantum state space. Two orthonormal bases are:

(1) Circularly Polarized (2) Linearly Polarized.

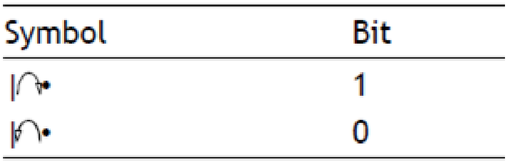
Let H be the two dimensional Hilbert space whose elements represent the polarization states of a single photon. We can make use of two different orthogonal bases of H, namely circular polarization basis and linear polarization basis. The circular polarization basis consists of the right and left circular polarization states, respectively. The linear polarization basis consists of the vertical and horizontal linear polarization states, respectively. The BB84 protocol utilizes any two incompatible orthogonal quantum alphabets in the Hilbert space H. Let Au be the circular polarization quantum alphabet and Ar be the linear polarization quantum alphabet, as shown in Table 1 and Table 2, respectively.

Table 1: Circular Polarization Quantum Alphabet $A^u$



| Symbol | Bit |
|---|---|
| \|↷• | 1 |
| \|↶• | 0 |

Table 2: Linear Polarization Quantum Alphabet $A^r$



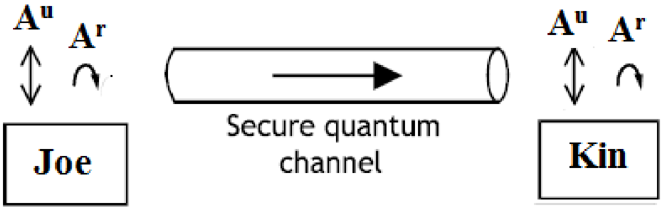
| Symbol | Bit |
|---|---|
| \|↷• | 1 |
| \|↶• | 0 |

Let us suppose that a key exchange is going to take place between two parties namely Joe and Kin and this communication is threatened by eavesdropper.

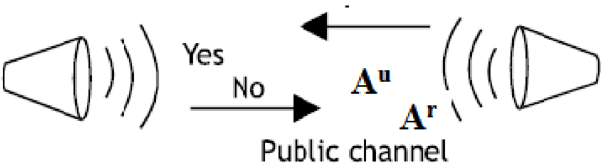
The idea is that measuring a photons polarization in the wrong basis gives no information about the encoded bit, and furthermore destroys it. The bases are related in this fashion: Measuring a photon's polarization requires choosing a measuring device which can distinguish between the two basis states of any one basis. If we have photons encoded in the linear basis and we try to measure with a detector for circularly polarized light, we measure vertical and horizontal polarization with equal probability, both 1/2. In this way, the information is obscured if one measures using the incorrect basis. The above phenomenon is fundamental to the correct operation of the BB84 protocol.

*Stage 1: Over a quantum channel*

To assure the detection of eavesdropping, Bennett and Brassard require Joe and Kin to communicate in two steps, the first step over a one way quantum communication channel from Joe to Kin, the second step over a two way public communication channel.



The first attempt at communicating the key occurs over a quantum channel. Joe generates a large random bit string where each bit is equally likely to be 0 or 1. This is then sent to Kin over the quantum channel by encoding each bit in one of the two bases, choosing either basis with equal probability for each bit.



Kin makes measurements on received photons, by randomly choosing a basis on his known (with equal probability) for each bit. Note that due to this, Kin may choose a different basis than the one in which Joe originally encoded it. These incorrect measurements are taken care of in the next stage of the protocol.

Example: The Players

- Joe and Kin: they want to share a key
- Joe can prepare qubits which he can send them to Kin via a quantum channel
- Kin can apply H or not and measure a qubit (we assume he can also memorize qubits). They also use a good public classical channel.
- Eve (the eavesdropper) wants to know the key and can do whatever quantum mechanics allows
- Read all data on the classical channel, catch the qubits sent by Joe, attach them a probing device

**The Bb84 States**

Those are the states Joe sends to Kin

They are: |0›, |1›, H|0›, H|1›

H|0›= |+› = 1/ 2½ [ |0›+ |1› ] and

H|1› = |-› = 1/ 2½ [ |0› - |1› ]

Measuring in the standard basis { |0›, |1›}

state |0› gives 0 with probability 1

state |1› gives 1 with probability 1

state |+› gives a randombit [p(0) = 1/2,p(1) = 1/2]

state |-› gives a randombit [p(0) = 1/2,p(1) = 1/2]

H|+› = |0› and H|-› = |1›

*A First Protocol:*

Notations

H0 = I, H1 =H

H**b** =H*b*1 + . . . + H*b*2*n* if **b** = *b*1 . . .*b*2*n*.

Joe selects randomly i,b belongs to {0,1}2*n* and s belongs to {0,1}2*n* with |s| = *n*.

She sends Kin H**b** |i›

When Kin has themall, she announces publicly **b** and **s**

Kin applies H**b** to his state andmeasures

If there is no noise he recovers **i**

Kin and Joe publicly check for errors on the bits with b*j* = 0

The key is the parity of the bits i *j* for which bj = 1

Joe randomly selects, each time he sends a bit, one of the two orthogonal alphabets $A^u$ or $A^r$ with equal probability. Since no measurement operator of $A^u$ is compatible with any measurement operator of $A^r$, it follows from the Heisenberg uncertainty principle that no one, not even Kin, can receive Joe's transmission with an accuracy of greater than 75%, i.e. the minimum error rate is ¼. The measurement that distinguishes linear photons will disturb circular photons. Similarly, a measurement that distinguishes circular photon a will disturb linear photons. This shows that $A^u$ and $A^r$ are incompatible and because of this incompatibility, there is no simultaneous measurement operator for both $A^u$ and $A^r$. Since one has no knowledge of Joe'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 Joe's choice and 50% of the time (i.e., with probability ½) one will guess incorrectly. A correct guess means Joe's transmitted bit is received with probability 1. On the other hand, an incorrect guess means Joe's transmitted bit is received correctly with probability ½. Thus in general, the probability of correctly receiving Joe's transmitted bit is

$$P = \tfrac{1}{2} \cdot 1 + \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{3}{4}$$

Let . be the probability of Eve's eavesdropping, 0 . . . 1. Therefore, if Eve is not eavesdropping, then the probability will be 1 - .. Thus, if . = 1, Eve is eavesdropping on each transmitted bit and if . = 0, Eve is not eavesdropping at all. As discussed earlier, both

Omer and Eve have no knowledge of Joe's choice of alphabet. Also, the measurement operators they choose are stochastically independent of each other. Therefore Eve's eavesdropping has an immediate and detectable impact on Kin's received bits. Eve's eavesdropping causes Kin's error rate to jump from ¼ to ¼ (1 - .) + (3/8) = ¼ +./8 Thus, if Eve eavesdrops on every bit, i.e., if . = 1, then Kin's error rate jumps from ¼ to 3/8, a 50% increase.

*Stage 2: Raw key generation*

The purpose of this stage is to identify and eliminate those bit positions where Joe and Kin used different bases. This is done over a public channel. Kin tells Joe which basis he used for each position, and Joe in turn replies telling him which ones were incorrect. These positions are then discarded by both. Note that no information about the actual values of the bits is exchanged. If there has been no eavesdropping nor transmission errors due to noise, the remaining bit strings, called the raw key, at both locations are the same.

*Stage 3: Eavesdropping detection*

However, if an eavesdropper Eve has been at work, she may have introduced inconsistencies in the raw key. A measurement by Eve works in the same way as a measurement by Kin. Therefore, if the measurement made by Eve is in the incorrect basis, it may change the encoded bit that Kin measures when he gets the photon. Eavesdropping is detected as follows: A random subset, say of length m, of the raw key is agreed upon by Joe and Kin, and those bits are compared publicly. If any two corresponding bits differ, this indicates the presence of an eavesdropper and so Joe and Kin return to Stage 1. If not, the exchanged bits are discarded and the rest of the raw key is used as the final secret key.

If Eve eavesdrops on every bit with an independent probability each, the probability that she goes undetected is (1- lamda/4)m . This can be proved as follows Each basis is chosen with probability ½ . In the correct basis, there is no way of measuring wrongly. In the incorrect basis, a measurement may give an incorrect bit value with: 0.1/2 + ½.1/2 = ¼.

For a bit to be measured wrongly in the presence of eavesdropping, the following must occur: Eve decides to eavesdrop (lamda and chooses the incorrect basis, and Kin gets an incorrect measurement on the photon he receives. The probability of this happening is therefore(lamda/4) implying that the probability of eavesdropping going undetected for m bits is then (1-lamda/4)m. The entire preceding discussion assumes the absence of noise in the quantum channel. In the case of noise, further steps have to be taken to verify that the key is the same at both ends. These steps involve parity-checking of various subsets and binary searching to pin down and eliminate the erroneous bit. We have implemented from the bottom-up a simulation of the

BB84 protocol to exchange keys. It is coded in C++ and simulates the above stages as described.

### Equivalence to the BB84 protocol

1. Joe creates random bits.
2. Joe chooses a random For each bit, she creates a state in the basis(when the corresponding bit of b is 0) or in the B1 basis (when the corresponding bit of b is 1).
3. Joe sends the resulting qubits to Kin.
4. Kin receives the qubits, measuring each in B0 or B1 at random.
5. Joe announces and Kin discard any result where his basis doesn't coincide with Joe's one. With high probability, there are at least 2n bits left (if not, abort the protocol). Joe decides randomly on a set of 2n bits to use for the protocol, and chooses at random n of these to be check bits.
6. Joe and Kin announce the values of their check bits. If too few of these value agree (high error rate), they abort the protocol.
7. Joe announces u + v, where v is the string consisting of the remaining non-check bits, and u is a random codeword in C1.hannel
8. Kin substracts u + v from his own remaining non-check bits v + $^{2}$ (where $^{2}$ represents errors), and corrects the result u + $^{2}$ in order to obtain u, a codeword in C1.
9. Joe and Kin use the co set of u in C1=C2 as the secret key.

### Limitations of Quantum Cryptography Techniques

In spite of all the powers that Quantum methods have, these systems are very vulnerable to decoherence. Qubits can get corrupted or flipped due to perturbations from the surroundings. Also like any other signal, there is a problem of attenuation over distance. But in case of quantum, the matter is worse. Current techniques of Quantum Cryptography face the limitation of non-existence of devices that can be used to clone the signal. To clone a particular signal, measurements are required to be made, which by the very nature of quantum cryptography will destroy the original signal because the cloning device does not know the correct order of basis that was used. Also, if we make amends in the protocol to allow for a device like router to make correct measurements and then further clone and amplify signal, then the same technique can be used for eavesdropping thereby losing the whole point of quantum cryptography. Therefore, this amounts to saying that a quantum system should have direct-dedicated point to point links between any two entities that wish to communicate. These raise a lot of serious questions on the feasibility of quantum devices.

## Current status and breakthroughs

Despite these limitations, there have been attempts to apply quantum methods, at a much scaled down level though. Teams from Harvard, Boston University and BBN Technologies are trying to build DARPA (Defense Advanced Research Projects Agency) quantum network, of which the first link has been laid and functional since December 2002. In addition to these teams at Geneva, Los Alamos and IBM are performing QKD through telecom fibers. There are systems that that can support distances upto 70 km through fiber, though at very low bit rates. Also, teams from Los Alamos and Qinetiq are performing free-space Quantum Cryptography, both through day and night skies upto a distance of 23 km.

## Eavesdropping

Various eavesdropping strategies have been developed, such as opaque and translucent eavesdropping. Opaque eavesdropping involves the capture, measurement, and retransmission of photons. Translucent eavesdropping is a technique wherein the photon is very gently disturbed in order to glean some information from it.[2] This can be accomplished by letting a photon pass through a bi-refringent crystal and then measuring the recoil of the crystal due to momentum conservation. If the width of the crystal is set appropriately, the resultant photon is only slightly depolarized. Cloning is possible only when it is known that the photon is in one of a definite set of orthonormal states. If a set of non-orthogonal states is used, this gives us the opportunity to detect any eavesdropping attempt by measuring an unusual error rate in exchanged bits, beyond the expected statistical error rate.

## BB84 Simulation

We have implemented a simulation of the BB84 protocol in C++ using the STL Library. The salient features of this implementation are the following:

- We use vector<bool> to represent the keys and the basis. We represent the two (circular and vertical) polarizations as 0 and 1.
- We input the desired size of the key (n), and the number of verification bits (m). We generate A's key and basis randomly using the function genRan dom (vector<bool>) which fills up a boolean vector with 0's and 1's randomly.
- The measure (a_ key, a _basis, b_ key, b_ basis, lambda) function measures a's key with b's basis.

- The values obtained are saved in B's key vector. The basis for the input vector is then modified.

[2] Artur K. Eckert et. al., "Eavesdropping on quantum-cryptographical systems",Physics, Rev. A 50, 1047105, 1994.

- This function works just like an actual measurement would. Once basis is used to measure a certain key entry, the key value gets fixed at that value.

- The same function is used for both B and C. Like in the theory given above, the lambda is the probability that C will eavesdrop at any given bit. If the function is being called by B, we set lambda = 1.

- We simulate A and B's basis comparison over the public channel by comparing the ith values of the two vectors 'a' basis and 'b' basis, to generate a raw key. If the size of this raw key is less than the number of verification bits, then we have an error and exit.
- We then pick up 'm' random bits from 'a' key and 'b' key and check their values. If we find any error (i.e. the values of the vectors do not match at the random indices) then we signal eavesdropping. Else we output the remaining bits and exit.

## Conclusion

Based on what have read and learnt about the field of Quantum Cryptography in general, there a few important issues that we feel need to be tackled before Quantum technology can emerge from the researcher's laboratory into the mainstream and become a security technology. The most severe limitation of quantum computers at their current stage of development is the fact that they are large and expensive, and are custom-built by researchers in a very controlled laboratory environment. It remains to be seen whether quantum computers of a reasonable size (say comparable to personal computers 20 years ago) can be built and packaged in a form amenable to mass-production.