Review Article on Quantum Cryptography

Anuradha Singhal, Tarun Chander

***Abstract*–** Quantum cryptography is an approach to securing communications based on certain phenomena of quantum physics. Unlike traditional cryptography, which employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted messages, quantum cryptography is focused on the physics of information. The process of sending and storing information is always carried out by physical means, for example photons in optical fibers or electrons in electric current. Eavesdropping can be viewed as measurements on a physical object — in this case the carrier of the information. What the eavesdropper can measure, and how, depends exclusively on the laws of physics. Using quantum phenomena such as quantum super positions or quantum entanglement one can design and implement a communication system which can always detect eavesdropping. This is because measurements on the quantum carrier of information disturb it and so leave traces.

Index Terms*— *Cryptography , polarization,photons , quantum bit

I. INTRODUCTION

In a quantum computer, the fundamental unit of information (called a quantum bit or qubit), is not binary but rather more quaternary in nature. This qubit property arises as a direct consequence of its adherence to the laws of quantum mechanics which differ radically from the laws of classical physics. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical bit, but also in states corresponding to a blend or superposition of these classical states. In other words, a qubit can exist as a zero, a one, or simultaneously as both 0 and 1, with a numerical coefficient representing the probability for each state. This may seem counterintuitive because everyday phenomenon are governed by classical physics, not quantum mechanics -- which takes over at the atomic level. , a quantum computer manipulates qubits by executing a series of quantum gates, each a unitary transformation acting on a single qubit or pair of qubits. In applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits in some initial state. The qubits can then be measured, with this measurement serving as the final computational result. This similarity in calculation between a classical and quantum computer affords that in theory, a classical computer can accurately simulate a quantum computer. In other words, a classical computer would be able to do anything a quantum computer can. So why bother with quantum computers? Although a classical computer can theoretically simulate a quantum computer, it is incredibly inefficient, so much so that a classical computer is effectively incapable of performing many tasks that a quantum computer could perform with ease

II. PREAMBLE TO QUANTUM CRYPTOGRAPHY

The recent results in quantum cryptography are based on the Heisenberg uncertainty principle of quantum mechanics1. Using standard Dirac notation2, this principle can be succinctly stated as follows: Heisenberg Uncertainty Principle: For any two quantum mechanical observables A and B

$$\Delta A = A - \langle A \rangle \quad \text{and} \quad \Delta B = B - \langle B \rangle ,$$

$$\left\langle (\Delta A)^2 \right\rangle \left\langle (\Delta B)^2 \right\rangle \geq \frac{1}{4} \| \langle [A, B] \rangle \|^2 ,$$

$$\left\langle (\Delta A)^2 \right\rangle \text{and} \left\langle (\Delta B)^2 \right\rangle$$

are variances which measure the uncertainty of observables A and B. For incompatible observables, that is, for observables A and B such that [A;B] 6= 0, reducing the uncertainty (A2)of A forces the uncertainty (B2) Of B to increase, and vice versa..Thus the observables A and B can not be simultaneously measured to arbitrary precision. Measuring one of the observables interferes with the measurement of the other.

III. YOUNG'S DOUBLE SLIT EXPERIMENT

Young's double slit experiment is an example suggesting how Heisenberg's uncertainty principle could be used for detecting
eavesdropping in a cryptographic communications.

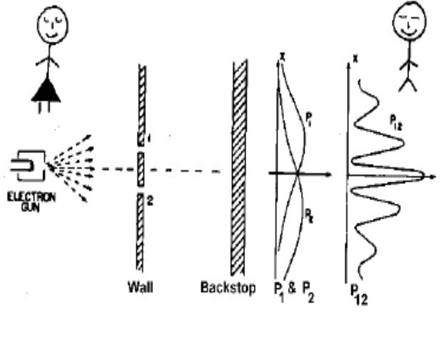


Fig 1.Young's Double slit Experiment when electron trajectories are not observed.The first of two incompatible observables is measured

Manuscript received March, 2014

***Anuradha Singhal**, Department of Computer Science , Delhi University /Deen Dayal Upadhyaya College/ Delhi , India, 09650600697*
***Tarun Chander**, Department of Computer Science, Kurukshetra University, Delhi , India , 9899880116,*

An electron gun randomly emits electrons over a fairly large angular spread. In front of the gun is a metal wall with two small slits. Beyond the wall is a backstop that absorbs the electrons that pass through the two slits. The probability density pattern of the absorbed electrons is described by the curves P1, P2, and P21 which, for the convenience of the reader, have been drawn behind the backstop. The curve P1 denotes the probability density pattern if only slit 1 is open. The curve P2 denotes the probability density pattern if only slit 2 is open. Finally, the curve P12 denotes the probability density pattern if both slits 1 and 2 are open. Thus, P12 shows a quantum mechanical interference pattern demonstrating the wave nature of electrons.

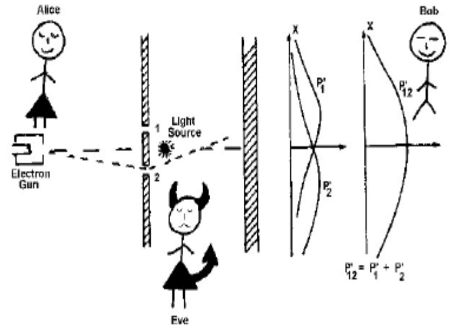


Fig 2 .Young Double Slit experiment When Electron trajectories are observed by eve.   The second of two incompatible observable is measured

Comparing this with our description of a classical cryptographic system, the electron gun can be thought of as the transmitter Alice. And the interference pattern P12 can be thought of as the message received by Bob. If however, Eve tries to eavesdrop by trying to detect through which slit each electron passes, as illustrated in Fig. 2.2, the interference pattern P12 is destroyed and replaced by the bell curve P0 12 (which is a classical superposition of curves P01 and P02) as drawn .Thus demonstrating the particle nature of the electron. As a result, Bob knows with certainty that Eve is eavesdropping in on his communication with Alice. Bob knows that, because of the Heisenberg uncertainty principle, both the wave and particle natures of the electron can not be simultaneously detected. The quantum cryptographic protocols discussed will of necessity use some encoding scheme (or schemes) which associates the bits 0 and 1 with distinct quantum states. We call such an association a quantum alphabet. Should the associated states be orthogonal, we call the encoding scheme an orthogonal quantum alphabet

IV. Quantum Cryptography Protocols

The BB84 quantum cryptographic protocol without noise The first quantum cryptographic communication protocol, called BB84, was invented in 1984 by Bennett and Brassard . 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. It is speculated, but not yet experimentally verified, that the BB84 protocol should be implementable over distances of at least 100 km. In this section we describe the BB84 protocol in a noise free environment. In the next section, we extend the protocol to one in which noise is considered.

BB84 protocol in terms of the polarization states of a single photon:-

Let H be the two dimensional Hilbert space whose elements represent the polarization states of a single photon. In describing BB84, we use two different orthogonal bases of H. They are the circular polarization basis, which consists of the keys.

$$|\curvearrowright\rangle \text{ and } |\curvearrowleft\rangle$$

for right and left circular polarization states, respectively, and the linear polarization basis which consists of the keys

$$|\updownarrow\rangle \text{ and } |\leftrightarrow\rangle$$

for vertical and horizontal linear polarization states, respectively. The BB84 protocol utilizes any two incompatible orthogonal quantum alphabets in the Hilbert space H. For our description of BB84, we have selected the circular polarization quantum alphabet A1.

Symbol	Bit
$\vert\curvearrowright\rangle$	1
$\vert\curvearrowleft\rangle$	0

Circular Polarization
Quantum Alphabet $\mathcal{A}_{\odot}$

Here,

$\mathcal{A}_{\odot}$ A1:

$\mathcal{A}_{\boxplus}$ A2:

and the linear quantum alphabet

Symbol	Bit
$\vert\updownarrow\rangle$	1
$\vert\leftrightarrow\rangle$	0

Linear Polarization
Quantum Alphabet $\mathcal{A}_{\boxplus}$

Bennett and Brassard note that, if Alice were to use only one specific orthogonal quantum alphabet for her communication to Bob, then Eve's eavesdropping could go undetected. For Eve could intercept Alice's transmission with 100% accuracy, and then imitate Alice by retransmitting her measurements to Bob. If, for example, Alice used only the orthogonal quantum alphabet A1, then Eve could measure each bit of Alice's transmission with a device based on some circular polarization measurement operator such as

$$|\curvearrowright\rangle\langle\curvearrowright| \quad \text{or} \quad |\curvearrowleft\rangle\langle\curvearrowleft|$$

Or if, Alice used only the orthogonal quantum alphabet A2, then Eve could measure each transmitted bit with a device based on some linear polarization measurement operator such as

$$|\updownarrow\rangle\langle\updownarrow| \qquad \text{or} \qquad |\leftrightarrow\rangle\langle\leftrightarrow|$$

The above strategy used by Eve is called opaque eavesdropping.

V. Stages for Communication over a Protocol

BB84 quantum cryptographic protocol without noise
Stage1

In the first stage, Alice is required, each time she transmits a single bit, to use randomly with equal probability one of the two orthogonal alphabets A1 or A2. Since no measurement operator of A1 is compatible with any measurement operator of A2, it follows from the Heisenberg uncertainty principle that no one, not even Bob or Eve, can receive Alice's transmission with an accuracy greater than 75%.

.

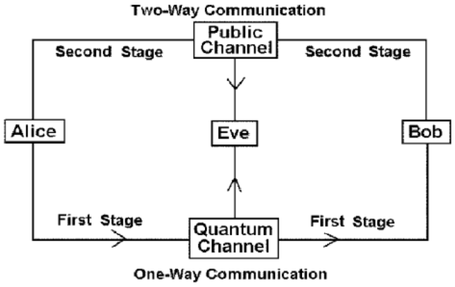


Fig 3 A quantum cryptographic quantum system for security transferring quantum random key.

This can be seen as follows. For each bit transmitted by Alice, one can choose a measurement operator compatible with either A1 or A2 , but not both. Because of incompatibility, there is no simultaneous measurement operator for both A1 and A2 . Since one has no knowledge of Alice's secret choice of quantum alphabet, 50% of the time (that is, with probability ½ one will guess correctly, that is, choose a measurement operator compatible with Alice's choice, and 50% of the time (that is, with probability ½ one will guess incorrectly. If one guesses correctly, then Alice's transmitted bit is received with probability 1. On the other hand, if one guesses incorrectly, then Alice's transmitted bit is received correctly with probability ½ . Thus in general, the probability of correctly receiving Alice's transmitted bit is P=1/2*1+1/2*1/2=3/4

For each bit transmitted by Alice, we assume that Eve performs one of two actions, opaque eavesdropping with probability 1-x1.Thus, if x1=1,Eve is eavesdropping on each transmitted bit, and if x1=0 ,Eve is not eavesdropping at all. Because Bob's and Eve's choice of measurement operators are stochastically independent of each other and of Alice's choice of alphabet, Eve's eavesdropping has an immediate and detectable impact on Bob's received bits. Eve's eavesdropping causes Bob's error rate to jump from ¼ to

¼(1-x1)+3/8*x1=1/4+x1/8

Thus if Eve eavesdrops on every bit ,if x1=1,then Bob's error rate jumps from ¼ to 3/8, a 50% increase.

Stage2

Alice and Bob communicate in two phases over a public channel to check for Eve's presence by analyzing Bob's error rate. This stage is itself divided in two stages.

Phase 1 of Stage 2. Extraction of raw key

It is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Eves eavesdropping. Bob begins by publicly communicating to Alice which measurement operators he used for each of the received bits. Alice then in turn publicly communicates to Bob which of his measurement operator choices were correct. After this two way communication, Alice and Bob delete the bits corresponding to the incompatible measurement choices to produce shorter sequences of bits which we call respectively Alice's raw key and Bob's raw key.If there is no intrusion, then Alice's and Bob's raw keys will be in total agreement. However, if Eve has been at work, then corresponding bits of Alice's and Bob's raw keys will not agree with probability

0*(1-x1)+1/4(x1)=x1/4

Phase 2 of Stage 2. Detection of Eve's intrusion via error detection

Alice and Bob now initiate a two way conversation over the public channel to test for Eve's presence .In the absence of noise, any discrepancy between Alice's and Bob's raw keys is proof of Eve's intrusion. So to detect Eve, Alice and Bob select a publicly agreed upon random subset of m bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed. Should at least one comparison reveal an inconsistency, then Eve's eavesdropping has been detected, in which case Alice and Bob return to stage 1 and start over. On the other hand, if no inconsistencies are uncovered, then the probability that Eve escapes detection is:

P(false)=(1-x1/4)^m

For example if x1=1,m=200

then P(false)=(3/4)^200,==10^ -25

Thus, if Pfalse is sufficiently small, Alice and Bob agree that Eve has not eavesdropped, and accordingly adopt the remnant raw key as their final secret key.

BB84 Quantum Cryptographic protocol with noise

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. It is speculated, but not yet experimentally verified, that the BB84 protocol should be implementable over distances of at least 100 km.

Stage 1. Communication over a quantum channel

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

Stage 2. Communication in four phases over a public channel

In stage 2, Alice and Bob communicate over a public channel in four phases. Phase 1 is dedicated to raw key extraction, phase 2 to error estimation, phase 3 to reconciliation, that is, to reconciled key extraction, and phase 4 to privacy amplification that is extraction of final secret key.

Phase 1 Extraction of raw key

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

Phase 2 of Stage 2. Estimation of error in raw key

Alice and Bob now use the public channel to estimate the error rate in raw key. They publicly select and agree upon a random sample of raw key, publicly compare these bits to obtain an estimate R of the error-rate. These revealed bits are discarded from raw key. If R exceeds a certain threshold RMax, then it will be impossible for Alice and Bob to arrive at a common secret key. If so, Alice and Bob return to stage 1 to start over. On the other hand, If the error estimate R does not exceed RMax, then Alice and Bob move onto phase 3.

Phase 3 of Stage 2. Extraction of reconciled key

Alice and Bob's objective is to remove all errors from what remains of raw key to produce an error free common key, called reconciled key. This phase is of course called reconciliation, and takes place in two steps . In step 1, Alice and Bob publicly agree upon a random permutation, and apply it to what remains of their respective raw keys. Next Alice and Bob partition the remnant raw key into blocks of length l, where the length l is chosen so that blocks of this length are unlikely to contain more than one error. For each of these blocks, Alice and Bob publicly compare overall parity checks, making sure each time to discard the last bit of the compared block. Each time a overall parity check does not agree, Alice and Bob initiate a binary search for the error, that is , bisecting the block into two sub blocks, publicly comparing the parities for each of these sub blocks, discarding the right most bit of each sub block. They continue their bisective search on the sub block for which their parities are not in agreement. This bisective search continues until the erroneous bit is located and deleted. They then continue to the next l block.

Step 1 is repeated, that is, a random permutation is chosen, remnant raw key is partitioned into blocks of length l, parities are compared, etc. This is done until it becomes inefficient to continue in this fashion. Alice and Bob then move to step 2 by using a more refined reconciliation procedure. They publicly select randomly chosen subsets of remnant raw key, publicly compare parities, each time discarding an agreed upon bit from their chosen key sample. If a parity should not agree, they employ the binary search strategy of step 1 to locate and delete the error. Finally, when, for some fixed number N of consecutive repetitions of step 2, no error is found, Alice and Bob assume that to a very high probability, the remnant raw key is without error. Alice and Bob now rename the remnant raw key reconciled key, and move on to the final and last phase of their communication.

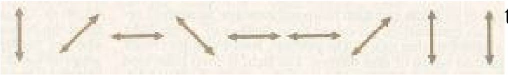
Phase 4 of Stage 2. Privacy amplification, that is, extraction of final secret key Alice and Bob now have a common reconciled key which they know is only partially secret from Eve. They now begin the process of privacy amplification, which is the extraction of a secret key from a partially secret one Based on their error estimate R, Alice and Bob obtain an upper bound k of the number of bits known by Eve of their n bits of reconciled key. Let s be a security parameter that Alice and Bob adjust as desired. They then publicly select n-k-s random subsets of reconciled key, without revealing their contents, and without revealing their parities. The undisclosed parities become the common final secret key. It can be shown that Eve's average information about the final secret key is less than 2^-s= ln 2 bits.

VI. Quantum Key Distribution

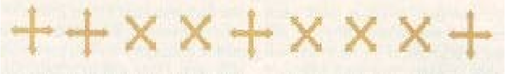
Polarized photons

Quantum cryptographic system will allow two people, say, Alice and Bob, to exchange a secret key. The system includes a transmitter A and a receiver. Alice uses the transmitter to send photons in one of four polarizations: 0, 45, 90 or 135 degrees. Bobs uses the receiver to measure the polarization. According to the laws of quantum mechanics, the receiver can distinguish between rectilinear polarizations (O and 90), or it can quickly be reconfigured to discriminate between diagonal polarizations (45 and 135); it can never, however, distinguish both types. The key distribution requires several steps. Alice sends photons with one of four polarizations, which she has chosen at random.

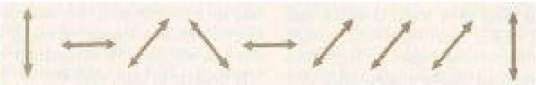
For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (x)



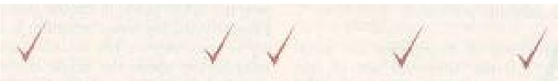
Bob records the result of his measurement but keeps it a secret.

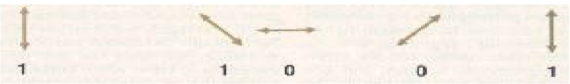


Bob publicly announces the type of measurements he made, and Alice tells him which measurements were of the correct type.



Alice and Bob keep all cases in which Bob measured the correct type. These cases are then translated into bits (I's and O's) and there by become the key.





If Bob and Alice find a small number of errors, they must devise a way to correct them and proceed. On the other hand,

if they find a large number, indicating significant eavesdropping, they must reject their data and start over.

A variety of techniques are available for Alice and Bob to correct a small number of errors through public discussion, such as the use of error-correcting codes. But these techniques potentially leak information to Eve, who may be listening to the public discussion. Therefore, after the quantum transmission and the error correcting discussion, Alice and Bob find themselves with what might be thought of as an impure key, a shared body of data that is partly secret. Information on that key may have leaked to Eve at several stages. She may have gained information by splitting some flashes, by directly measuring others (she cannot do this too often, as it causes errors in Bob's data) and by listening to the public discussion between Alice and Bob. Fortunately, Alice and Bob, because they know the intensity of the light flashes and the number of errors found and corrected, can estimate how much information might have leaked to Eve through all these routes. in itself, such an impure key is almost worthless. Using this technique, Alice and Bob, through public discussion, can take such a partly secret key and distill from it a smaller amount of highly secret key, of which the eavesdropper is very unlikely to know even one bit. The essential idea of privacy amplification is for Alice and Bob, after the eavesdropping has taken place, to choose publicly a length-reducing transformation to apply to their impure key so that partial information about the input conveys almost no knowledge of the output. For example, if the input consists of 1,000 bits about which Eve knows at most 200 bits, Alice and Bob can distill nearly 800 highly secret bits as output. Fairly simple techniques can be shown to suffice, and Alice and Bob do not even need to know which partial information the eavesdropper might have about the input in order to choose a function about whose output Eve has almost no information. In particular, it suffices for Alice and Bob to define each bit of the output as the parity of an independent, publicly agreed-on random subset of the input bits, very much as they had done to gain high confidence that their raw quantum data were identical (except that now they keep the parity secret instead of publicly comparing it).

VII. Attacks

In Quantum Cryptography, traditional man-in-the-middle attacks are impossible due to Heisenberg's uncertainty principle. If anybody attempts to intercept the stream of photons, he will inevitably alter them if he uses an incorrect detector. He cannot re-emit the photons to Bob correctly, which will introduce unacceptable levels of error into the communication. If Alice and Bob are using an entangled photon system, then it is virtually impossible to hijack these, because creating three entangled photons would decrease the strength of each photon to such a degree that it would be easily detected. Anybody cannot use a man-in-the-middle attack, since he would have to measure an entangled photon and disrupt the other photon, then he would have to re-emit both photons. This is impossible to do, by the laws of quantum physics. Other attacks are possible. Because a dedicated fiber optic line is required between the two points linked by quantum cryptography, a denial of service attack can be mounted by simply cutting the line or, perhaps more surreptitiously, by attempting to tap it. If the equipment used in quantum cryptography can be tampered with, it could be made to generate keys that were not secure using a random number generator attack.

VIII. Practical Implementation

The first computer network in which communication is secured with quantum cryptography is up and running in Cambridge, Massachusetts. Chip Elliott, leader of the quantum engineering team at BBN Technologies in Cambridge, sent the first packets of data across the Quantum Net (Qnet) on Thursday 18:43 04 June 2004. The project is funded by the Pentagon's Defense Advanced Research Projects Agency. Currently the network only consists of six servers, but they can be integrated with regular servers and clients on the Internet. Qnet's creators say the implementation of more nodes in banks and credit card companies could make exchanging sensitive data over the Internet more secure than it is with current cryptography systems. The data in Qnet flows through ordinary fiber optic cables and stretches the 10 kilometers from BBN to Harvard University. It is encrypted using keys determined by the exchange of a series of single, polarized photons. The first money transfer encrypted by quantum keys was performed between two Austrian financial institutions in April 2004. But Qnet is the first network consisting of more than two nodes to use quantum cryptography - a more complex challenge."Imagine making a phone call. If you just have one possible receiver, you wouldn't even need buttons," explains Elliott. "But with a network you need a system that will connect anyone on the network to anyone else." In Qnet, software-controlled optical switches made of lithium niobate crystals steer photons down the correct optical fiber.

Intruder detection

Quantum cryptography guarantees secure communications by harnessing the quantum quirks of photons sent between users. Any attempt to intercept the photons will disturb their quantum state and raise the alarm. But Elliott points out that even quantum cryptography "does not give you 100 per cent security". Although quantum keys are theoretically impossible to intercept without detection, implementing them in the real world presents hackers with several potential ways to listen in unobserved. One example is if a laser inadvertently produces more than one photon, which happens occasionally. An eavesdropper could potentially siphon off the extra photons and decrypt the key, although no one has actually done this. "However Qnet is more secure than current Internet cryptography," says Elliott, which relies on "one way functions". These are mathematical operations that are very simple to compute in one direction, but require huge computing power to perform in reverse. The problem is, according to Elliott, that no one has actually proved that they cannot be solved in reverse. "So who's to say that someone won't wake up tomorrow and think of a way to do it?"

_*Large and expensive*

At the moment computers capable of quantum cryptography are large and expensive, because they are custom-made. Elliott imagines a Qnet-like system may first appear in banks, for whom these factors might be less of a problem. Another limitation is that, for distances over 50 kilometers, the photon signal is degraded by noise, and it is unclear as yet how this problem will be overcome.

However, quantum keys can potentially be exchanged over much larger distances through the air. Tiny, aligned telescopes can send and detect single photons sent through the air. The distance record for this form of transmission is currently about 20 kilometers. But calculations suggest that photons transmitted through the air could be detected by a satellite, which would enable data to be sent between continents.

IX. Conclusion

It is not easy to emphasize how dramatic an impact the application of quantum mechanics has had and will have on cryptographic communication systems. From the perspective of defensive cryptography, it is now within the realm of possibility to build practical cryptographic systems which check for, detect, and prevent unauthorized intrusion. Quantum mechanics provides an intrusion detection mechanism never thought possible within the world of classical cryptography. Most importantly, the feasibility of these methods has been experimentally verified in a laboratory setting. Moreover, from the perspective of offensive cryptography, the application of quantum mechanics to computation also holds forth the promise of a dramatic increase of computational parallelism for cryptanalytic attacks. Much remains to be done before quantum cryptography is a truly practical and useful tool for cryptographic communication. We list below some of the areas in need of development:

- Quantum protocols need to be extended to a computer network setting.
- More sophisticated error correction and detection techniques need to be implemented in quantum protocols.
- There is a need for greater understanding of intrusion detection in the presence of noise.
- There is a need for better intrusion detection algorithms. As far as the author has been able to determine, all quantum intrusion detection algorithms in the open literature depend on some assumption as to which eavesdropping strategy is chosen by Eve. It is important that eavesdropping algorithms be developed that detect Eve's intrusion no matter which eavesdropping strategy she uses.

Acknowledgment

I wish to acknowledge my peers who helped me develop this module and used it in projects for better development

REFERENCES

[1] WWW.GOOGLE.COM
[2] WWW.ALTAVISTA.COM
[3] WWW.LINUXQUESTIONS.ORG
[4] http://news.bbc.co.uk/1/hi/technology/2963138.stm
[5] http://www.ecst.csuchico.edu/~atman/Crypto/quantum / quantum-probs-inf.html

Anuradha Singhal MS(Software Systems) Bits Pilani , Assistant Professor , Deen Dayal Upadhyaya College , Delhi University ,Worked as IT Analyst in IBM India .

Tarun Chander B.E Kurukshetra University