An Effective Technique for Data Security in Modern Cryptosystem

Dilbag Singh[1] and **Alit Singh**[2]

Abstract - Present paper provides a conceptual framework on the proposed C-QUBITS Key exchange technique, which is used as a base for the data security through quantum computing in the modern cryptosystem. In the first phase a detailed description of the BB84 Cryptographic protocol is given, which is used as a standard protocol for quantum key distribution in quantum cryptography and the emphasis is also given on the loopholes present in this protocol which makes it less effective than it pretends to be. In the next phase the focus is made on the C-QUBITS technique, which can be used for the exchange of key between the sender and the receiver. Thereafter the key is used for the encryption of the data to be transferred between the two entities. This technique makes use of the concepts of quantum physics like polarization and more importantly C-NOT gate which is mainly used in case of qubits (quantum bits) and it is more effective and secure than the BB84 protocol. In the last phase the focus is made on the information reconciliation and privacy amplification, which is used for error correction carried out between Alice and Bob's keys and for reducing a third party's partial information about the shared secret key between two parties, Alice and Bob respectively. Further the security level in the C-QUBITS technique can be increase by performing the privacy amplification that convert the realized secret key into a smaller length key through some hashing function chosen at random from a known set of hashing functions.

Index Terms - C-qubits algorithm, BB84 protocol, qubits, quantum key distribution, privacy amplification, information reconciliation and hashing function.

1. INTRODUCTION

Modern cryptosystem are specifically designed for use on computers and no longer concern with the written alphabet. The focus is on the use of binary bits. One of the main part of the modern cryptosystem is quantum cryptography. It was born in the early seventies when Stephen Wiesner wrote "Conjugate Coding", which unfortunately took more than ten years to see the light of print[1]. In the mean time, Charles H. Bennett and Gilles Brassard picked up the subject and brought it to fruition in a series of papers that culminated with the demonstration of an experimental prototype that established the technological feasibility of the concept[2]. Quantum cryptographic systems take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement [3]. Eavesdropping on a quantum communication channel therefore causes an unavoidable disturbance, alerting the legitimate users. This yields a cryptographic system for the distribution of a secret random cryptographic key between two parties initially sharing no secret information that is secure against an eavesdropper having at her disposal unlimited computing power. Once this secret key is established, it can be used together with classical cryptographic techniques such as the one-time-pad to allow the parties to communicate meaningful information in absolute secrecy. Advantage of quantum cryptography over traditional key exchange methods is that the exchange of information can be shown to be secure in a very strong sense, without making assumptions about the intractability of certain mathematical problems. Even when assuming hypothetical eavesdroppers with unlimited computing power, the laws of physics guarantee (probabilistically) that the secret key exchange will be secure, given a few other assumptions [4].

[1]*Department of Computer Science & Engineering, Choudhary Devi Lal University, Sirsa,Haryana (India)*
[2]*Department of Computer Science & Engineering, BPS Mahila Vishwavidyalaya, Khanpur Kalan, Sonepat, Haryana (India)*
E-Mail: [1]*dbs_beniwal@rediffmail.com and*
[2]*ghanghas_ajit@rediffmail.com*

2. QUANTUM APPROACH

Main problem of secret-key cryptosystems is secure distribution of keys. It is here that quantum mechanics offers a solution. While the security of public key cryptographic methods can be undermined by advances in technology and mathematical algorithms, the quantum approach will provide unconditional security [12,13]**.** Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be acquired without changing the state of the object. All classical signals can be monitored passively. In classical information, one bit of information is encoded in billions of photons, electrons, atoms, or other carriers. You can always deviate part of the signal and perform a measurement on it, whereas in quantum mechanics, any projective measurement will induce disturbances [5].

3. QUANTUM KEY DISTRIBUTION

Key distributed using quantum cryptography would be almost impossible to steal because Quantum key distribution (QKD)[5,6,7] systems continually and randomly generate new private keys that both parties share automatically

A compromised key in a QKD system can only decrypt a small amount of encoded information because the private key may be changed every second or even continuously. To build up a secret key from a stream of single photons, each photon is encoded with a bit value of 0 or 1, typically by a photon in some superposition state, such as polarization. These photons are emitted by a conventional laser as pulses of light so dim that most pulses do not emit a photon. This approach ensures

that few pulses contain more than one photon. Additional losses occur as photons travel through the fiber-optic line. In the end, only a small fraction of the received pulses actually contain a photon [10]. However, this low yield is not problematic for QKD because only photons that reach the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon.

4. CRYPTOGRAPHIC PROTOCOL BB84

The most common standard protocol for quantum key distribution is called BB84, it was invented by Charles H. Bennet and Gilles Brassard in 1984. It allows two users to establish an identical and purely random sequence of bits at two different locations while allowing revealing of any eavesdropping. BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used.

Basis	0	1
+	↑	→
×	↗	↘

The first step in BB84 is quantum transmission. Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the table to the left. So for example a 0 is encoded in the rectilinear basis (+) as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 135° state. Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent [8].

In the lab experiment [9], the BB84 protocol encodes single photon polarizations using two bases of the same 2–dimensional Hilbert space:

- rectilinear basis $\{0°: |\rightarrow\rangle, 90°: |\uparrow\rangle\}$
- diagonal basis $\{45°: |\nearrow\rangle, 135°: |\nwarrow\rangle\}$

Only requirement on the involved quantum states is actually that they belong to mutually non-orthogonal bases of their Hilbert space, where each vector of one basis has equal-length projections onto all vectors of the other basis. If a measurement on a system is performed in a basis different from the one the system is prepared in, its outcome is completely random and the system looses all the memory of its previous state.

Any measurement in the diagonal basis on photons prepared in the rectilinear basis will yield random outcomes with equal probabilities and vice versa. On the other hand, measurements performed in the basis identical to the basis of preparation of states will produce deterministic results. The protocol relies on Heisenberg's uncertainty principle, which forbids the measurement of more than one polarization component of one photon.To exchange a secret key in the BB84 protocol[8], Alice and Bob must do as follow:

Alice creates a binary random number and sends it to Bob using randomly the two different bases + (rectilinear) and X (diagonal):

- $|\rightarrow\rangle$ and $|\nearrow\rangle$ both represent 1
- $|\uparrow\rangle$ and $|\nwarrow\rangle$ both represent 0

Therefore, Alice transmits photons randomly in the four polarization states

$$|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, \text{and } |\nwarrow\rangle.$$

1. Bob simultaneously measures the polarization of the incoming photons using randomly the two different bases. He does not know which of his measurements are deterministic, i.e. measured in the same basis as the one used by Alice.
2. Later, Alice and Bob communicate to each other the list of the bases they used. This communication carries no information about the value of the measurement, but allows Alice and Bob to know which values were measured by Bob correctly.
3. Bob and Alice keep only those bits that were measured deterministically and will disregard those sent and measured in different bases. Statistically, their bases coincide in 50 % of all cases, and Bob's measurements agree with Alice's bits perfectly.
4. Together, they can reconstitute the random bit string created previously by Alice.

4.1 Loophole in BB84 Protocol

Now as we have given a complete description of BB84 protocol. If Eve intercepts the transferred photons two cases are possible.

CASE 1: First one is that the base used by the Alice, Bob and Eve will be same.

CASE 2: Second one is that the base used by the Alice and Bob is same but that used by the Eve is different.

As the base used by all three of them is same in **Case 1** so Eve will be able to correctly guess the value corresponding to the polarized photon. As the base used by Eve and Alice is same so after the interception of the photon, the polarization of the photon won't change so it would be impossible for the Bob to guess that interception took place.

And if suppose 40 photons are send by Alice then on an average in 20 photons (using probability) out of that, the base used by Alice and Bob will be same (Which will form the key) and out of that also in 10 photons base used by Alice, Eve and Bob will be same. So we can conclude that out of 20 photons that will form the key 10 will be known to Eve i.e. **½** of the total key.

NOTE: Here we have not considered the case where the base used by the Alice and Bob will be different as in that case photons won't be considered for being the part of the key (No matter what is the base used by the Eve).

5. PROPOSED C-QUBITS TECHNIQUE

In this the photons will be send in pairs. First photons will be passed through the C-NOT gate (as shown in Fig. -1) and

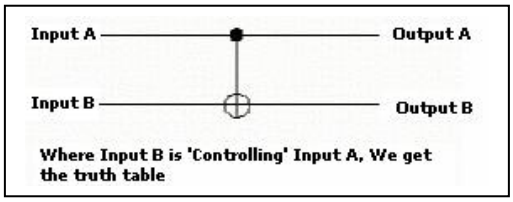

Figure 1 C-NOT gate.

then will be passed through the polarized. Before going any further we would like to explain the working of C-NOT gate.

Input		Output		Type
A (Control)	B (XOR)	A	B	
0	0	0	0	Identity
0	1	0	1	Identity
1	0	1	1	Swap
1	1	1	0	Swap

Table 1: Truth table of the C-NOT gate

The gate will take two inputs and correspondingly give two outputs. Table 1 summaries all input-output possibilities for a C-NOT gate. Output value of B depends on the value of A. If value of A is 0 then Value of B will remain as it is, and if value of A is 1 then value of B will change[12]

The diagram given in Fig. 2 shows how pair of bits is passed through the C-NOT gate and then how polarization takes place[12]. The polarization [9] takes place in the same way as in case of original BB84 algorithm.

5.1 Steps in C-QUBITS Technique

C-QUBITS technique includes the following steps and the actual data to code conversion is given in Table 2[12].

i. Alice creates a binary random number and divides them into pairs and then each pair is passed through **C-NOT gate**. Then it to Bob using randomly the two different bases + (rectilinear) and X (diagonal):

- $|\rightarrow\rangle$ and $|\nearrow\rangle$ both represent 1
- $|\uparrow\rangle$ and $|\nwarrow\rangle$ both represent 0

Therefore, Alice transmits photons randomly in the four polarization states

$$|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, \text{and } |\nwarrow\rangle.$$

ii. The bases of the pair of photons can be **+X**, **++**, **X+** or **XX**.

iii. Bob simultaneously measures the polarization of the incoming pair of photons using randomly the four possible combinations i.e. **+X**, **++**, **X+** or **XX**. He does not know which of his measurements are deterministic, i.e. measured in the same pair of basis as the one used by Alice.

iv. Later, Alice and Bob communicate to each other the list of the bases they used for each pair of photons.

v. Bob and Alice keep only those pair of bits that were measured deterministically and will disregard those sent and measured in different bases. Statistically, the pair bases coincide in 25 % of all cases, and Bob's measurements agree with Alice's bits perfectly. In those cases only the output B of C-NOT gate is considered for being part of the key.

vi. Together, they can reconstitute the random bit string created previously by Alice.

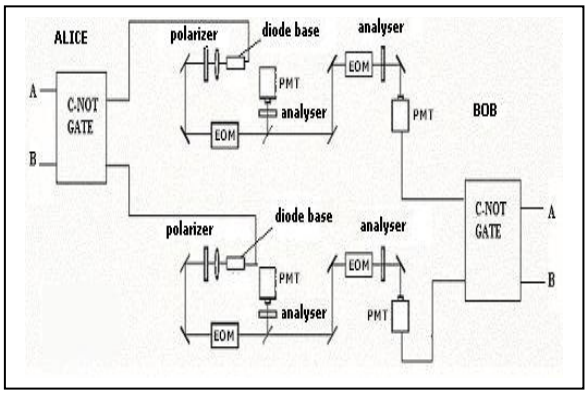

Figure 2: Diagrammatic view of the C-QUBITS technique

Alice	1	0	1	1	1	1	0	1	0	1	0	0
C-NOT gate	1	1	1	0	1	0	0	1	0	1	0	0
Random bases	X	+	X	X	+	X	+	+	+	X	X	+
Alice Polarization	↗	→	↗	↖	→	↖	↑	→	↑	↗	↖	↑
Bob's random Bases	X	+	X	+	+	X	X	+	+	+	X	+
Bob's measurement	↗	→	↗	→	→	↖	↗	→	↑	↑	↖	↑
C-NOT gate	1	0			1	1					0	0
Values Kept		√				√						√

Table 2: Shows the actual data to code conversion.

Note: The table-2 given at the end of the paper shows C-QUBITS in tabular form. The same color cells are used to indicate pairs. Here 3 bits have been deduced which will become part of the final key. This process continues until we get desired number of bits to form the complete key.

5.2 What if Eve intercepts?

Eavesdropper (usually called Eve) intercepts in between to listen to the quantum channel, she can intercept the pair of photons sent by Alice, perform measurements on them and resend them to Bob. However, as Alice alternates her encoding bases at random, Eve does not know the basis to use for her measurement; she must choose her measurement bases at random, as well. Now as there are 4 possible pairs i.e. ++, +X,

XX, X+ Eve will guess the pair correctly one out of every four times. In that case she will be able to send the pair of photons correctly to Bob. But in other 75 % of the cases, though, she measures in the wrong basis and produces errors.
Example, lets assume Alice sends a pair of 1and 0.Now when they are passed through C-NOT gate, value of 1 will remain as it is but value of 0 will change to 1 (refer the C-NOT truth table). Now suppose '**1'** is send in the rectilinear basis i.e. the state → and other 1 in diagonal base i.e. the state (We are only considering the case where Bob will also use are rectilinear base for the first photon and diagonal base for the second base) because for all the other cases the photons wont be considered for being the part of the key. Suppose Eve also measures the first photon in the rectilinear base and the second photon in the diagonal base then she will able to guess the value of that photon perfectly (but this will happen in only 25% of the cases as compared to 50% cases in case of BB84 algorithm). In rest of the 75% cases when Eve will make a mistake in choosing one or both of the random bases, then no matter which polarization Eve detects and re-sends she won't be having any idea of the value of the photons used. **(**Eve won't be able to guess the remaining bits as we are considering only output of B (of the C-NOT gate) for the key, as Eve does not know the value of A on which final value of B depends)[12].

6. COMPARISON OF C-QUBITS TECHNIQUES WITH BB84 PROTOCOL

6.1 BB84 Protocol:

Suppose we have 640 bits (we have taken a large value so that on repeated division we don't get a decimal value). Now if we apply probability then in 320 bits rectilinear base will be applied by Alice and in other 320 bits diagonal base will be applied. Again on an average if Eve intercepts the photons then in ½ of the times the random base used by her, will be same as used by the Alice i.e. again for 320 bits. Now as Bob will also be using the same random bases as by Alice half of the times (on an average) and in 160 of that bits the case will be such that Base used by the Alice, Eve and Bob will be same. So this indicates that out of the 320 bits key that will be generated 160 bits will be known to Eve (although guessing of the remaining 160 bits will be very difficult, which itself explains the power of quantum cryptography).
So the **conclusion** is that:
Total Bits used = 640
No of bits used for the formation of Key =320
No. of bits that Eve could guess =160
i.e. Eve knows half of the key

6.2 C-QUBITS Technique

Suppose we have 640 bits i.e. 320 pair of bits. Here if Eve intercepts the photons then in 1/4 of the times the random base used by her, will be same as used by the Alice because there are 4 possible combinations i.e. ++, +X, XX, X+ i.e. on average in 80 pairs she will guess correctly. Now as Bob will also be using the same random bases for the pair of photons as by Alice 1/4 of the times (on an average) i.e. again 80 pairs and 20 of that pairs the case will be such that the pair of Base used by the Alice, Eve and Bob will be same. So this indicates that only 80 pairs will be considered for the key and of that only the value of B will be considered so out of 640 bits used we will get a key of only 80 bits and out of that only 20 bits will be known to the Eve.
So the **conclusion** is that:
Total Bits used=640 bits or 320 pairs
No of bits used for the formation of Key=80
No of Bits that Eve could guess=20
i.e. Eve will be able to guess only ¼ of the key (Use of C-not gate will make it impossible for Eve to guess the remaining Key)

7. INFORMATION RECONCILIATION

Information reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimize the information sent about each key, as this can be read by Eve. A common protocol used for information reconciliation is the cascade protocol, proposed in 1994. This operates in several rounds, with both keys divided into blocks in each round and the parity of those blocks compared. If a difference in parity is found then a binary search is performed to find and correct the error. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively, which is the source of the cascade name. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. At the end of multiple rounds Alice and Bob will have identical keys with high probability, however Eve will have gained additional information about the key from the parity information exchanged [15].

8. PRIVACY AMPLIFICATION

Further to increase the security, Privacy Amplification is performed. **It** is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possible parity information). Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This can be done using a hash function,(A hash function is a function from a set of possible inputs, *U*, to a set of outputs, which is usually taken to be $\{1, \ldots, N\}$ for some *N*.) chosen at random from a publicly known set of such functions[11], which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated, based on how much information Eve could have gained about the old key (which is

known due to the errors this would introduce), in order to reduce the probability of Eve having any knowledge of the new key to a very low value[14,17].

9. HOW DOES PRIVACY AMPLIFICATION WORK

In Quantum Key Distribution, to arbitrarily limit the amount of partial information that an eavesdropper can know about a quantum distributed key, the sender and receiver can use privacy amplification. This uses a set of universal hash functions chosen at random to compress both the key size and Eve's knowledge accordingly.

The hash algorithm which defines the family of universal hashes is in the clear. Like if

$$h(x)=(a\_1.x\_1+a\_2.x\_2+a\_3.x\_3+a\_4.x\_4)$$

for an N bit key divided into 4 chunks x_i . The values a_i are randomly generated, and it's this which we don't get how it's transmitted between Alice and Bob and hash function can be publicly communicated. For example, let's say Eve (eavesdropper) knows 1/3 of the key. Alice (sender) and Bob (recipient) can publicly agree to break the key into 3 bit chunks and perform a parity operation on those, to make a key one third the length of the original. Since, at this point, Alice and Bob's keys agree completely, the reduced key will also agree completely without any need for communicating the results of the parity operations. Eve can know that they are performing this hash function, but since she only has 1/3 of the key, she can not perform the hash function on her partial key to get the official reduced key. So the hash function can be made completely public. Of course, Eve could know three consecutive bits, which would allow her to perform the hash function on those to get a bit from the reduced key. So the hash function needs to be chosen intelligently, based on the estimated knowledge of Eve. So, instead, if the hash function took 10 bit blocks for parity check, then Eve's expected knowledge goes down even farther.

To estimate Eve's knowledge, Alice and Bob will look at the error rate in the keys (using information reconciliation). Errors can be caused either by Eve's measurements or by noise. Alice and Bob will attribute all errors to Eve, to be safe. This gives them an idea of how much reduction their hash function must do. When we say the hash function is randomly chosen, the term random just means it is not chosen before hand. If Eve knew that the hash function would use three bits in a row, she could optimize her measurement to be more likely to give three bits in a row. But if she doesn't know how the bits will be grouped for the parity check (they need not be in a row), or if something other than parity will be used, she will have no way to optimize her measurement for the eventual hash function that is used. So 'random', in this case, just means 'decided after the key is sent.

Finally, it might wonder if Eve could do a man-in-the-middle attack, where she intercepts the discussion about the hash function and makes Bob think Alice is using a different has function. She can do this, for sure, but it will not result in Eve learning about the message. It will only keep Alice from communicating her message to Bob [16].

10. PROSPECTS

The current commercial systems are aimed mainly at governments and corporations with high security requirements. Key distribution by courier is typically used in such cases, where traditional key distribution schemes are not believed to offer enough guarantee. This has the advantage of not being intrinsically distance limited, and despite long travel times the transfer rate can be high due to the availability of large capacity portable storage devices. The major difference of quantum cryptography is the ability to detect any interception of the key, whereas with courier the key security cannot be proven or tested. QKD (Quantum Key Distribution) systems also have the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network.

Factors preventing wide adoption of quantum cryptography outside high security areas include the cost of equipment, and the lack of a demonstrated threat to existing key exchange protocols. However, with optic fibre networks already present in many countries the infrastructure is in place for a more widespread use [17].

11. CONCLUSION

The C-QUBITS technique can be used as a powerful tool for combating the problems of data security and provide more security that previously used BB84 protocol. Further this technique can be make more effective by using the concept of information reconciliation and privacy amplification.

REFERENCES

[1]. W. Die, M.E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory 22, 644-654, 1979.

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

[3]. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptol. 5, pp3–28, 1992.

[4]. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys.74, pp145–195, 2002.

[5]. G. Brassard and L. Salvail "Secret key reconciliation by public discussion" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23, 1993.

[6]. C. Gobby, Z. L. Yuan and A. J. Shields, "Quantum key distribution over 122 km telecom fiber," Appl. Phys. Lett. 84, pp 3762–3764 2002.

[7]. D. Gottesman, H. K. Lo, N. L¨utkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Inf. Comput. 4,pp 325–360 ,2004.

[8]. Frederick Henle, BB84 online demo. <http://monet.mercersburg.edu/henle/bb84/>. An online

demonstration of the original BB84 algorithm from, Bennett et al. 1991.
[9]. Matthias Scholz, Quantum Key Distribution via BB84 an Advanced Lab Experiment, (Oct. 14th 2004).
[10]. K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova and P. D. Townsend, "Quantum key distribution system clocked at 2 GHz," Opt. Express 13, pp 3015–3020 2005.
[11].J. F. Dynes, Z. L. Yuan, A. W. Sharpe and A. J. Shields, "A high speed, post-processing free, quantum random number generator," Appl. Phys. Lett. 93, 031109 ,2008.
[12].A.Singh, An efficient quantum cryptography's algorithm for data security, Indian Journal of Engineering & Materials Sciences, Vol. 14, pp. 352-357, October 2007.
[13].Z. L. Yuan, A.W. Sharpe and A. J. Shields, "Unconditionally secure quantum key distribution using decoy pulses," Appl. Phys. Lett. 90, 011118, 2007.
[14].C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. SIAM Journal on Computing, 17(2): 210-229, 1988.
[15].G. Brassard and L. Salvail "Secret key reconciliation by public discussion" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23,1993.
[16].M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality, Journal of Computer and System Sciences", 22, pp 265-279, 1981.
[17].http://en.wikipedia.org/wiki/Quantum_cryptography/Accessed on 25th October, 2009.