Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol

Rahul Aggarwal[1], Heeren Sharma[2], Deepak Gupta[2]

[1]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab 144011, India.

ABSTRACT
Quantum Key Distribution (QKD) networks are the best application of quantum cryptography in which we use the principles of quantum mechanics with classical cryptographic techniques to provide the unconditional security. This paper discusses the various attack strategies over BB84 quantum key distribution protocol and the analysis of these attacks.

General Terms
Quantum computing, network security, cryptography, attacks.

Keywords
Quantum cryptography, QKD, BB84, Intercept/Resend.

1. INTRODUCTION
In this fast moving and ever enhancing world, the aspect that comes in mind of every person is that of security. Secure transmission of data and information is the prime requirement of every organization and entity. Cryptography is a method to transfer the data or stream from one party to another. Here, the data is first encrypted using some key by the sender side and then the same encrypted data is later decrypted with the help of same or another key by the receiver side as per the accepted protocol between the two parties. Now, this key is the heart and soul of this whole procedure. The better and efficient is this key, harder will be to crack the whole encrypted by any eavesdropper. With the larger key, comes the problem of secure key transfer. If the desired key gets stolen by the third party during the exchange, then whole foundation of the secure transmission can get shattered.

Quantum cryptography is the method which converge the concept of quantum mechanics with that of classical cryptography. Here, the quanta or photons are used to form the key for the secure communication. The soul of quantum cryptography is the Heisenberg's Uncertainty Principle which states that one can't measure the properties of a photon like spin, polarization etc. without being introducing any errors or deviation of the normal photon transmission which can easily be detected. This makes this whole concept a provider of "unconditional security".

The foundation of this revolutionary concept was laid by Bennett and Brassard in 1984 [1] by proposing the first protocol to implement the quantum cryptography practically. The best application of quantum cryptography is quantum key distribution (QKD) networks. Later the protocols using entangled photons pair [2] was also proposed, the enhanced version of BB84 protocol using only two quantum states [3] was proposed, and realization of QKD networks in practical world was felt more strongly.

Recently, SECOQC- Development of a Global Network for Secure Communication [4-5] based on Quantum Cryptography practically demonstrated the secure transmission of data by implementing the QKD network.

But, as the time progresses, the various loopholes in this concept of quantum cryptography are detected which demands some further research and proper measures. Various efficient attacks over the QKD networks are performed. Hence, there is a lot to be studied in this field and various research groups are coming in support of this technology so as to fulfill the dream of unconditional security.

2. QUANTUM KEY DISTRIBUTION
To blend the principles of quantum mechanics in the classical cryptography scheme, the property of photon that was used by researchers was photon polarization and spin. In the generic terms, the key components of QKD network are quantum channel, classical or public channel, sender and receiver which are equipped by proper detector and devices.

First and the most studied protocol for the implementation of QKD networks was the BB84 protocol [1]. The various other protocols for the same have been proposed like E91 [2], B92 [3] etc. In BB84 protocol, there are two basis sequence are used: rectilinear basis (+) and diagonal basis (×). In the rectilinear basis, the two possible polarizations are 0˚ and 90˚ i.e. horizontal and vertical polarization, which represent the 0 and 1 bit respectively. Similarly, in the diagonal basis, the two polarizations are 45˚ and 135˚ which represent the 0 and 1 bit respectively. This whole bit value representation is shown in Table 1.

Table 1: Bit value representation for BB84 protocol

Polarization Mode	Symbol	Bit value 0	Bit value 1
Rectilinear Basis	+	0˚ , →	90˚ , ↑
Diagonal Basis	×	45˚ , ↗	135˚ , ↖

Suppose the two communicating parties are Alice and Bob. The BB84 protocol is implemented in two phases which are as follows:

1) First Phase (over Quantum Channel)
   a) Alice first forms the raw key string which comprise of a random order.
   b) After this, using the random basis sequence, she transmits the polarized photon sequence to Bob.
   c) Bob will measure the incoming photon sequence using his basis sequences.
   d) As Bob doesn't know the bases sequence of Alice, thus it is not the deterministic basis sequence.

2) Second Phase (over public channel)
   a) Bob and Alice exchange the basis sequence used by each other.
   b) After the basis exchange, the common matched bases points are kept intact while the different bases are discarded.
   c) At this stage, Alice and Bob have the common raw bit sequence after all the acceptance and rejection of bases but this cannot be treated as final secret key has Eve can intercept this photon sequence.
   d) To achieve the final secret key, Error Estimation (estimating the amount of error occurred during the whole transmission procedure), Error Correction (perform the necessary error correction measures), and privacy amplification (detect the presence of Eve and regenerate the key using the same procedure until the surety of the secret key is established) are performed as final step.

3. ATTACKING STRATEGIES

Though the QKD networks seems to provide us the unconditional security, but there are various attacking strategies that have been proposed which requires serious attention. Some of these attacks are possible in ideal environment while other attacks get their roots from the real time implementation. In ideal environment, photon sources are considered to be the single photon generators and the detectors for the same are 100% efficient. In every strategy, the main aim is to gain the large content of the information without getting detected or traced. Greater the information gain, the smarter is the attack.

3.1 Intercept and Resend

This attack strategy is particularly implemented in the ideal environment. In naive intercept/resend (I/R), Eve intercepts the light photons coming from the Alice (sender) end with his own predefined basis. Since, in the ideal environment, detectors are highly efficient, thus Eve can get a hold on each photon. Eve follows a scheme which is shown in the form of the decision tree in Fig. 1. In Fig. 1, the scheme is shown for sending bit value 0. Eve then send the replacement photon to the Bob as per his defined basis. Now, the intensity of the pulse to Bob is such adjusted that Bob will detect this pulse with the same rate. So, in a sense Eve is working like a median person and performing the detection of the photons from the Alice side same as that of Bob.

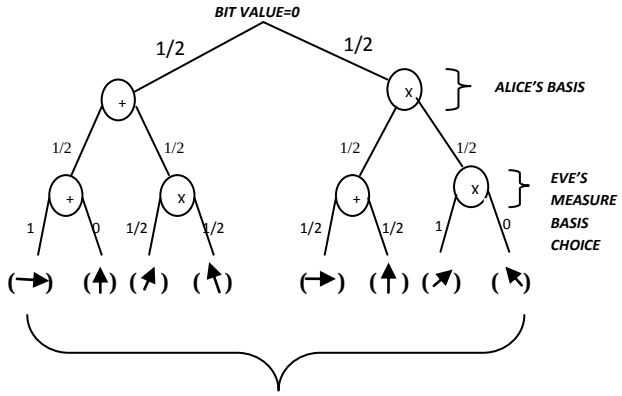

Fig 1: Decision tree for naive I/R attack strategy

Eve's efforts are said to be worth if she succeeds in getting the $1/\sqrt{2}$ of the Alice's information. In the error correction and privacy amplification phase of BB84 protocol, suppose t error bits are detected. Now using this information, Alice and Bob comes at some estimation that lesser than e1 bits are subjected to intercept/resend attack. Furthermore, the amount of information gained by Eve is not more than $e1/(\sqrt{2})$. An example of intercept resend attack is shown in Table 2.

Table 2: Simple intercept/resend attack

Alice random bits	0	1	1	0	1	0	0	1
Alice sending Basis	+	×	+	×	×	+	×	+
Alice polarization	→	↖	↑	↗	↖	→	↗	↑
Eve basis measurement	+	+	×	×	+	×	×	+
Polarization Eve measures and sends	→	→	↗	↗	↑	↗	↗	↑
Bob basis measurement	+	×	×	×	+	×	+	+
Polarization Bob measures	→	↗	↗	↗	↑	↗	→	↑
Shared secret key	0	0	-	0	-	-	-	1
Error generated	√	x		√				√

In the naïve intercept resend attack, the assumption is that Eve is not listening over the public channel i.e. sifting phase of BB84 protocol. This gives the information gain of approximately 0.2 bits out of every bit sent by Alice which is very low.

There are also other advancements of this attack. One is with Breidbart basis [8] which gives the information gain of 0.4 and the other is Full intercept/resend. In the later one, Eve taps on both quantum and public channel to get the larger portion of the information from the legitimate parties' side. This gives the

maximum information gain of 0.5 bits from every bit sent by Alice.

3.2 PNS Attack

In a realistic environment, perfect single photon sources are hard to manufacture. A normal signal pulse contains a large number of photons. Weak coherent pulses (WCP) are used in actual cryptographic devices. Fig. 2 shows a simple outline of such a photon source. A WCP is a photon pulse that has low mean photon number i.e. number of photons in that pulse. PNS attack takes advantage of this limitation of photon sources that emit WCPs.

Photon Number Splitting (PNS) attack was described properly by Brassard [6] and Lǜtkenhaus [7] and is quite a powerful attack. This attack concentrates on realistic photon sources. As highlighted above the limitation of weak coherent pulse generator, sometimes multiple-photon pulses are emitted. The strategy for Eve is to intercept a slight fraction of the multi-photon pulse fetched from Alice and send the remaining fraction to the Bob. Now, all the Eve has to do is to wait for the public announcement of the base sequence used by the two parties. Afterwards Eve can measure the intercepted photon in the correct basis.

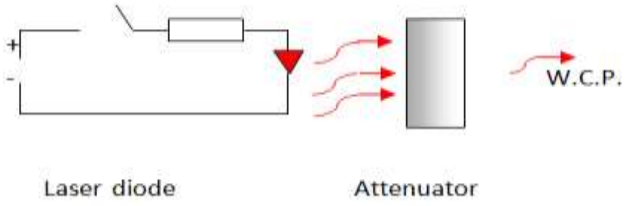

Fig 2: Weak Coherent Pulse generator.

Practically, PNS attack is quite complex to implement. The probability that the multiple-photon beam is emitted is around 5% [9] and the number of dark counts i.e. there is no photons in the pulse, is quite high. Hence, Eve has to check whether the emitted pulse contains the multiple photons or not which demands proper hardware and algorithms. If these things are taken care of, then in that case it will be very hard for the Bob to detect the presence of Eve.

3.3 Trojan Horse Attack

This is comparatively new form of attacking strategy. It has discussed in detail in [10] where they have introduced the experimental setup of for this kind of attack and the possible countermeasures for this kind of attack. Trojan Horse attack is also known as light injection attack.

In this form of attack, Eve pays total attention on the quantum cryptographic devices that is being used by Alice and Bob, unlike the previously defined attack which try to extract the information from the photons that are being transmitted in the channel. This strategy is implemented by sending out the light pulses towards the sender's or receiver's setup, which in return comes as the reflected pulse and enter the detection scheme which is also a possession, of Eve.

Eve can use the information of the reflected signal and can intercept the basis used by Alice for the preparation of the photon. Now, if Eve is able to get this information before that photon reaches the Bob side, then Eve can perform simple Intercept/Resend attack and measure it to get the exact secret string of qubits. Hence, Eve can get sufficient amount of the information without being detected.

3.4 Faked States Attack

A new type of attack was introduced by [11] which primarily focus on to gather the information by utilizing the imperfections in Bob's (receiver) scheme. It is special form of Intercept/Resend attack, where instead of recreating the signal, Eve sends the self derived signal in such a way that it controls the whole communication.

Another major fundamental that comes into this attack is of "full detector efficiency mismatch". In detail, the signal that Eve sends to Bob after intercepting the Alice's signal has such a time shift that if Bob chooses the basis other than that of the Eve for that particular signal then, Bob will not be able to detect that signal or in generic terms his detector will get blinded in this case. And, throughout this process, Eve is still undetected.

In BB84 protocol, the various steps of this protocol can be listed as follows:

1. First of all, Eve performs the simple Intercept/Resend attack over the transmitted signals and make the measurements as per his own basis.
2. Then, she sends a signal pulse to bob such that it has opposite bit value in the opposite state. And, with this she will sets the time shift of the signal such that if Bob measures the signal with the same basis as that of the Eve then he will get the signal, otherwise he will get nothing, i.e. he will not be able to detect that signal.
3. Now, if Eve measures the signal with the basis as that of Alice, then Bob will also get the same result. Otherwise, whatever errors Eve get in estimating the base for the particular signal, Bob will also get the error.
4. Hence, Eve has the taken the full control over the Bob's scheme.

This attack strategy is the advanced form of Intercept/Resend strategy and is quite effective. But, the small problem with this scheme is that it is very much dependent over the synchronization and the efficiency of the detectors of Eve. Overall, this is a different strategy than the rest of the attacks.

4. ATTACKS ANALYSIS

Different attack strategies have the different peculiar properties. Intercept/Resend attack and Beam Splitting (PNS attack) came into picture with the practical concept of quantum key distribution networks while Trojan Horse and Faked State attack are relatively new schemes of attacks. A lot of research work has already done over the Intercept/Resend and PNS or Beam Splitting attack and over their successful countermeasures and the same is proposed by the explorers of Trajan Horse and Faked State attacks.

The attention is always focused on the individual attacks, not on group attacks. This is so because first a technology should be able to be tolerant toward the single person attacks. And, lots of

research is also focused on individual attacks. As PNS and I/R attack are detected ay back earlier, hence these have gone through lots of discussion and thought processes. [12] provide us with some interesting results regarding the two which can easily be deduced from Fig. 3.

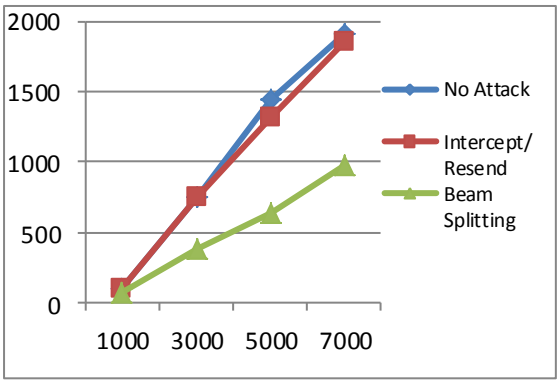

Fig 3: Initial Bits Length vs Final Bits Length [12].

In Fig. 3, initial bits length emitted by Alice is represented by x-axis and final bits length which is the outcome of BB84 protocol is represented by y-axis. Here, the clear strength of PNS (or Beam Splitting) attack can be seen over the Intercept/Resend attack. The length of final bit length is much lower in case of Beam Splitting attack than that of I/R attack while error rate is lower than the maximum allowable error rate. On the other hand, I/R attack seem close to the no attack line. On close examination of results, it can further be inference that Eve has 50% probability to measure the incoming bits from Alice correctly.

Considering Trojan Horse attack and Faked State attacks, these lead to the advent of new and powerful attacking strategies. The beauty of these attacks is that these are out of box attacks. I/R attack and Beam splitting attacks are used as sub strategies in these attacks. These are quite powerful attacks in themselves and their main strength is that if they are implemented perfectly then these are undetectable. The proposed countermeasures for these attacks are also not that much perfect as they themselves decrease the efficiency of BB84 protocol [10].

On close examination, I/R attack is proposed under ideal environment while the others have taken the practical imperfection of the communication system under their key areas of interest and hence are quite realistic ones. But, it does not imply that I/R attack is not effective one as it is used for the extraction of information of emitted photons in the remaining protocols.

5. CONCLUSION

Quantum cryptography is indeed the method to look forward and it can give the network security a whole new direction which is still lot to be discovered. It gives us the vision of the unconditional security by exploiting the fundamental concepts of quantum mechanics in classical cryptography. BB84 protocol was the first protocol to encourage this giant step to put forward in light and due to its simple yet powerful approach, it is the most studied protocol among the all other.

On the other side of the hedge, it is hard to take this whole theme of unconditional security by QKD networks because it is vulnerable to various types of attacks. The harsh reality of these attacks is that the origin of these attacks comes from the various imperfections or unfinished touches in the implementation of the QKD networks. These loopholes in the technology should be treated with utmost attention if this whole provision of unconditional security is required to establish in commercial environment. Though in the recent times, various new attacking strategy and countermeasures for previous strategies are treated properly by various research groups, which make quantum cryptography, a very much promising concept and the method to implement in the near future.

6. REFERENCES

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

[2] Ekert, Artur K. 1991. Quantum cryptography based on Bell's theorem, Physical Review Letters, Vol. 67, No. 6, 661-663.

[3] Bennett, C. H. 1992. Quantum cryptography using any two non-orthogonal states, Physical Review Letters 68 (21), 3121-3124.

[4] Alleaume, R., et al. 2007. SECOQC White Paper on Quantum Key Distribution and Cryptography. Arxiv preprint quant-ph/0701168.

[5] Poppe, A., M. Peev, and Maurhart O. 2008. Outline of the SECOQC quantum-key-distribution network in Vienna. International Journal of Quantum Information, **6**(2), 209-218.

[6] Bennett, Ch. H. et al. 1992. Experimental Quantum Cryptography, J. Cryptology, 3-28.

[7] Lů tkenhaus, N. 1996. Security against eavesdropping attacks in quantum cryptography, Phys. Rev. A 54(1), 97-111.

[8] Kollmitzer C., Pivk M. (Eds.) 2010. Applied Quantum Cryptography, Lect. Notes Phys. 797, Springer, Berlin Heidelberg.

[9] Gisin, N., Ribordy, G., Tittle, W., Zbinden, H. 2002. Quantum cryptography, Rev. Mod. Phys. 74(1), 145.

[10] Vakahitov, A., Makarov, V., Hjelme, D.R. 2001. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt., 48(13), 2023-2038.

[11] Makarov, V., Hjelme, D.R. 2005. Faked states attack on quantum cryptosystems, Journal of Modern Optics, 52(5), 691-705.

[12] Muhammad, N.A., Zukarnain, Z.A. 2009. Implementation of BB84 Quantum Key Distribution Protocol's with Attacks, European Journal of Scientific Research, 32(4), 460-466.