A Study of Various Quantum Cryptographic Architectures and an Efficient Implementation in Present Scenario and Results BB84 Protocol -A Practical Overview

G. Srinivasa Rao
Sr.Faculty of Computer Science
Dept of Computer Science
Key Soft Computer Education,
Mehdipatnam, Hyderabad.

B. Sujatha
Dept. Computer Science
Asst.Prof.Engineering College,
Osmania University,
Hyderabad

S. Nagaprasad
Lecturer in Computers
Dept. Computer Science
S.R.R.Govt.Degree College
Karimnagar

ABSTRACT:
Quantum Cryptography is also a Promising Approach visible of final Quantum Computers existence. it is a singular study Technique that provides us a singular secret Protocol that cannot be glorious by anybody. Quantum Cryptography holds foot on laws of Physics The quantum physics Law, however not as like that we have a tendency to area unit victimization addition, multiplication kind of arithmetic Puzzles used in PGP (Pretty smart Privacy). Quantum Cryptography will stand as a mile stone and cannot be challenged by future advancements throughout this field; if truth be told they'd be suggesting it as a certain communication protocol channel. enable us to careful derive the functions that provides a full account of the operational characteristics of a general QKD system. We wish to analyze specifically created to characterize the Bennett-Brassard Four-State (BB84) QKD protocol plenty of precisely, a group of generalizations that embrace the primary BB84 protocol as a special case, where the sender and so the receiver may take overtime in their alignment.

Keywords
QC (Quantum Cryptography), QKD (Quantum Key Distribution), Quantum Mechanics, PGP (Pretty Good Privacy), Sender, Receiver, Intruder, Alice, Bob, Eve, Photon, BB Protocol (Bennet and armour plate Protocol),Hilbert Space, AER(Average Error Rate),Single Photon, noise rate, Ge(Germanium),InGaAs(Indium-gallium arsenide)

1. INTRODUCTION:
Primarily we consider two people in this scenario 1.Alice (the sender), 2.Bob (the receiver) and 3.Eve (the intruder).

1.1 Alice and Bob Approach Each other:
'Bob' (Who is that the receiver) then receives them and checks the key using the calculations of the polarization. Currently once the Bob (Receiver) sends back the calculated key that sets the polarization values, Alice (The Sender) then sends the premise on each every Photon was polarized in Recipient sends the premise on it every photon's polarization was measured in Alice checks the values of these single photons that every the Alice and Bob used the same basis to form and live the polarization.

1.2 Alice And Bob Approach Every Other:
Currently allow us to imagine 'Alice' (The Sender) sends an encrypted key within the approach of 'polarized photons' that ar entangled. Any Intrusion in these values warns them that there would be a placing intrusion presence by 'Eve' (The Intruder) so the method is left and a replacement process begins. Primarily we have to think about 2 people to consider during this situation one. Alice (the sender), 2.Bob (the receiver) and three. During this case this approach utilizes the 'photons' to send as a key, because the keys ar sent, Communication is enabled in between the Alice and Bob. This polarization of photon will permit America only 1 'Bit' of data that may be sent. The QKD that firmly distribute a randomized scientific discipline key using the quantum physics Principle, there are two protocols. This can be as a result of the involvement of Eve that changes the direction of polarized photons. Eve (the intruder).Here the no-cloning principle it makes the Eve to live the key incorrectly.

2. BB PROTOCOL:
Abbreviated as "Bennet and Brassard Protocol" has the subsequent characteristics.

(1) Polarized Photons are utilized because the data carriers

(2) This algorithmic program uses four totally different Polarized angles like 0^o, 45^o, 90^o, and 135^o one hundred thirty five o for a secured communication.

(3) This Protocol then Polarizes

2.1 Eckert Protocol:
Has the subsequent characteristic.

(1) Principle is employed

(2) This method uses already polarized photons

As since this paper expresses interest in BB Protocol, therefore we have a tendency to proceed.

2.2 Hilbert Space:

In "Hilbert Space"… needed Photon's quantum states to be equally non-orthogonal bases, during this each basis vector can have identical-length projections over the all basis vectors. It mean to mention once we calculate the whole system equipped with our in set basis is executes on different basis also; the result would be utterly discretionary. and therefore the gift system couldn't be remembered or disbursed the sooner states. currently Assume that the polarized Instruction, the premise may be bridged with another like horizontal and vertical. allow us to currently think about |H> may be a horizontal vector and |V> may be a vertical vector. Imagine this as a linear basis. presently consider the second basis as a diagonal basis this might be bridged by the polarized photons. but the condition is that they have to be polarized with angle |A> with 45°, and |D> with 135°.

Using the Equations… Let us prove that…in BB84 Protocol,

$|A\rangle = \sqrt{2}/2(|H\rangle + |V\rangle)$ *and* $|D\rangle = \sqrt{2}/2(|H\rangle + |V\rangle)$

$\langle H|V\rangle = \langle A|D\rangle = 0$

$\langle HH\rangle = \langle V|V\rangle = \langle A|A\rangle = \langle D|D\rangle = 1$

Squaring on Both sides that equals to…

$|\langle H|A\rangle|^2 = |\langle H|D\rangle|^2 = |\langle V|A\rangle|^2 = \langle V|D\rangle^2 = 1$

So if any calculations created on one basis can give the discretionary results with a similar risk. The calculations created on the premise would be same with the premise of ready of states can build resolvable outcomes.

As the Hilbert space provides us 2-dimensional polarization this makes us to have coefficients combinations, using this we may be able to make a 3rd R- & L-polarized photon basis. These Polarized photons shows the identical characters.

0	**1**	**1**	**0**	**0**	**1**	**0**	**1**
×	×	+	+	+	×	+	×
$\|A\rangle$	$\|D\rangle$	$\|V\rangle$	$\|H\rangle$	$\|H\rangle$	$\|D\rangle$	$\|H\rangle$	$\|D\rangle$
×	+	+	×	×	+	+	×
$\|A\rangle$	R	$\|V\rangle$	R	R	R	lost	$\|D\rangle$
×	+	+	×	×	+	−	×
OK	−	OK	−	−	−	−	OK
0	−	**1**	−	−	−	−	**1**

Fig.1 POLARIZED PHOTANS R- & L- BASIS

1 Random bits of Alice
2 Random Polarized basis of Alice
3 Sent photons original Polarization
4 Random bases that are detected by Bob
5 Detected Photons Polarization
6 Using this Bob announces in a public channel his calculating basis
7 Using this Alice answers in a public channel then Bob later realizes by correcting the bas
8 The Original Cryptographic Key

Fig.2 POLARIZED PHOTANS R- & L- BASIS with connected operations.

The above given information on this Quantum Cryptographic BB84 Protocol is given in a general idea where as some more things to be considered for its way to implement. The 1st thing is noise. This has to be corrected. To be precise, error correcting protocol will have calculating an Average Error Rate(AER),later dividing the obtained data into some random parts say 'K', assuming that there could be 1 error in a taken block. The sender and receiver need to estimate every parity of the block. Every Block's parity is now compared, whether both sender and receiver accepts on parity of the Block In a case that they did not accepted , the Block could be divided into two parts. The process continually carried out un- till they accept each other. In this process The Intruder say 'Eve' may guess the 'K'. In view of security, all the time the parity bits are exchanged and, every block last bit is left over Repeating on 'N' Number of times, till the Alice and Bob are accepted with minimum number of errors. Now the sender and receiver can utilize the public communications channel to arbitrarily to select a hash-function. This hash-function is used to the obtained data to execute a key. This means Intruder 'Eve' does not know anything about the communication between Sender-Alice and Receiver-Bob. Generating the 'single photons (Unique Photons)'is a biggest challenge. To resolve this situation a continuous pulses are created. These pulses could be without any difficulty can be guessed by the beam- splitting techniques by Eve. Even there is no need to detect them, but remains unworthy. There may be two types of common attack. (1)The N photons sent between sender and receiver could be calculated as a complete N state system. The public communication channel is checked at the same time. The total outcome is that the eve could guess precisely the exact key. (2). Tiny photon pulses created may be sampled and the photons may be stored in a perfect reflector till the direction of polarization is announced on the public channel. This data then can be utilized to decipher the photon's value when it could be utilized as block of the key. Implementation wise speaking the above two cases can be categorically denied. BB protocol thinks that an 'Eve' can never fraud the public communication channel. In fact it could be done by utilizing an authentication scheme, to check the Alice and Bob. For the authentication scheme … it requires a key to be shared earlier, it means then this authentication scheme will not be a distribution mechanism but then it becomes a key expansion mechanism. Remember a hardcore intruder may be continuously impede and eventually weaken all exchanged keys before any "safe" communication is Initiated. Denial of service attack is a complicated problem with in all quantum cryptographic technology. Leaving this an

intruder could establish his/her identity between the Sender and receiver therefore he/she of intruder never seeks this way. In Present situation we are available with the Latest Technological Equipments such as

a) Multiple Transmitter-Receiver Multiplexing Analysis For sending and receiving the data

b) Data Recording De-multiplexing Constraints For data recording

c) High Speed Opto-electronics Components Interferometers process. Time-multiplexing interferometer that eliminates environmental fluctuations

d) High Pulse-Repetition-Frequency Lasers for Photon calculations

e) Synchronization Constraints for data synchronization

Thus, if a 1.3- m photon is injected into a fiber in a short wave packet (300-ps, say) it will emerge for the far end without being significantly stretched out in time and so, because we know that the photon will be expected within a short time window we need only consider the probability of a noise count in this short time interval it could be approximately 5x10-6 for 50-kHz noise rate.(The loss mechanism is predominantly Rayleigh scattering out of the fiber.) Conversely, optical fibers have much lower attenuation at 1.3 m it could be approximately 0.3 dB/km, and lower again at 1.55 m, but although there are commercially available germanium (Ge) and indium-gallium arsenide (InGaAs) APDs that are sensitive to light at these infrared wavelengths, there is no commercially available single-photon counting modules. Nevertheless, several groups have shown that these devices can detect single photons at 1.3 cm if they are first cooled to reduces the noise, also operates in "Geiger mode" , in that they are partial above stop working . The incoming photon frees the electron-hole pair, which with some probability initiates an avalanche electricity, whose detection signals the arrival of the photon. Once we had established that single 1.3- m photons can be detected with acceptably low-noise background, we had to decide which photon states are most suited for quantum key distribution: polarization and/or phase? For a polarization scheme we would have to propagate two non-orthogonal polarization states down the fiber. For the photons that ar the particles of sunshine within the wavelength vary of 600 - 800 nm these ar commercially accessible single-photon enumeration modules supported atomic number 14 avalanche photodiodes (APDs), that have high efficiencies but ninetieth and fewer sound rate it can be close to fifty cycle and once cooled it can be close to -25^{o}C.An immediate issue is that we want to grasp the link between vertical polarization (say) at the fiber input and therefore the output polarization, as a result of the refraction introduced by bends within the fiber can, in general, convert a linear polarization input state into associate degree elliptically polarized output. So, if we have a tendency to align one among the QKD polarization states with the quick axis (say) then the opposite non-orthogonal state are going to be step by step depolarized throughout propagation once its 2 element polarizations become separated by over the coherence length of the sunshine supply. Several parameters ar vital in characterizing the detector Performance: single-photon detection efficiency; intrinsic noise rate (dark counts); and time resolution. We have made the calculations completely detection efficiencies of ten - four-hundredth, (for InGaAs APDs), however noise rates that ar it can be close to one,000 times beyond for Si-APD gauge boson enumeration modules at 800 nm.However, our detectors even have superb time resolutions it can be close to few one hundred postscript, which may be utilized to atone for the upper intrinsic noise rate as a result of the low dispersion of optical fibers at one.3 nm.However, the attenuation of (single-mode) optical fibers is sort of high during this wavelength vary it can be close to three dB/km), which can adversely have an effect on the information rate and therefore the noise rate if we elect to work during this region. The distinction in propagation speeds45 (polarization mode dispersion or PMD) generally amounts to a couple of -phase distinction over (a beat length of) ten cm to one m of fiber. Furthermore, this refraction implies that a given length of fiber can, at any instant, have stable “fast” and “slow” propagation modes which can be orthogonally polarized. For our project we have a tendency to set that the propagation distance benefits of the one.3- m wavelength we have a tendency tore such we characterized the performance of many APDs (both Ge and InGaAs) for single-photon detection at this wavelength. Thus, PMD can create a polarization QKD theme tough for long propagation distances bigger than many kilometre. Nevertheless 2 teams have incontestable polarization-based QKD over it can be close to one kilometer of fiber.

Relative Number of Counts(RNC)	alignment Time
0	0
5.1	5.4
10.11	10.20
17.4	15.83
20.09	20.67
15.67	15.38
10.11	10.99
5.0	5.38
0.01	0.94
0.08	0.91
0.11	0.35
0.17	0.38
0.19	0.48
5.7	5.56
10.13	10.57
15.24	15.58
20.25	20.54
15.34	15.45
10.03	10.45
5.16	5.47
0.0	0.45
0.34	0.47
0.23	0.00
0.28	0.45
0.7	0.49
5.1	5.35
10.23	10.45
15.23	15.35
20.34	20.34
25.57	25.56
30.78	30.45

15.34	15.46
10.36	10.34
5.71	5.34
0.00	0.03
0.45	0.35
0.83	0.45
0.37	0.46
0.99	0.34
5.3	5.57
10.67	10.45
15.75	15.68
20.48	20.93
25.12	25.45
30.23	30.68
35.34	35.78
15.94	15.56
10.88	10.45
5.67	5.35
0.00	0.45
0.53	0.56
0.67	0.56
0.45	0.56
0.99	0.57
5.23	5.67
10.11	10.45
15.13	15.58
20.34	20.68
15.99	15.68
10.45	10.79
5.83	5.34
0.45	0.58
0.34	0.00
0.99	0.48
0.07	0.32
0.08	0.57
5.45	5.94
10.46	10.69
15.41	15.46
20.49	20.56
15.46	15.67
10.47	10.67
5.35	5.8

TABLE. 1 RNC AND ALIGNMENT TIME TABLE

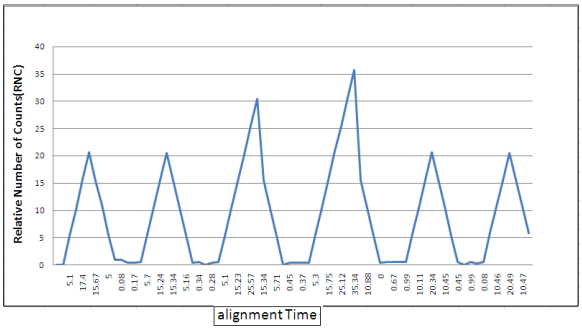

Fig.3 POLARIZED PHOTANS R- & L- BASIS

3. CONCLUSION

Quantum Cryptography is more practical than it is philosophical; it is the 1st of its kind to implement the Quantum Mechanics applied to Computer Science Field. It provides an un-conditional secrecy to the user. How long distances need to expanded, repeater stations are absolutely in need. QKD just creates a key rest of all we can have the existing system. Its flexibility of combining with our existing 56-bit DES keys provides us to consider the Quantum Cryptography in our wide spread Web based applications. However our theoretical evaluations on Practical values suggests that" sender and the receiver may take overtime in alignment".

4. REFERENCES

[1] **AppliedQuantumCryptography**
Volume 797 of Lecture Notes in Physics, ISSN 0075-8450

[2] Quantum Cryptography and Secret-Key Distillation
By Gilles Van Assche

[3] Ryszard Horodecki, Sergei Ya Kilin, J. Kowalik
IOS Press, 01-Jan-2010 - Political Science

[4] Dirk Bouwmeester, Artur K. Ekert, Anton Zeilinger
Springer, 2000 – Computers

[5] Giuliano Benenti, Giulio Casati, Giuliano Strini
World Scientific Pub., 2007 – Computers

[6] Noson S. Yanofsky, Mirco A. Mannucci
Cambridge University Press, 11-Aug-2008 – Computers

[7] Julian Brown
Simon and Schuster, 05-Apr-2002 – Computers

[8] Sir Roger Penrose
Oxford University Press, 04-Mar-1999 – Computers