# Quantum Key Distribution Based-on Refraction and Polarization Entanglement

**Gunasekaran M, Gopalakrishnan B, Amitabh Wahi**

***Abstract:** Cryptography is the specialty of encoding and decoding messages and exists as extended as the individuals have doubted from one another and need secure correspondence. The traditional techniques for encryption naturally depend on any among public key or secret key approaches. In general, the public key encryption depends on two keys, for example, public key and private key. Since encryption and decryption keys are different, it isn't important to safely distribute a key. In this approach, the difficult of the numerical issues is assumed, not demonstrated. All the security will be easily compromised if proficient factoring algorithms are found. In secret key encryption two clients at first create secret key, which is a long string of arbitrarily selected bits and safely shares between them. At that point the clients can utilize the secret key along with the algorithms to encryption and decryption information. The procedures are complicated and also planned such a way that every bit of output is based on every bit of input. There are two fundamental issues with secret key encryption; first one is that by breaking down the openly known encoding algorithms, it gets simpler to decrypt the message. The subsequent one is that it experiences key-conveyance issue. As a result of the ongoing improvements in quantum processing and quantum data hypothesis, the quantum computers presents genuine difficulties to generally utilized current cryptographic strategy. The improvement of quantum cryptography beat the deficiencies of old style cryptography and achieves these huge accomplishments by using the properties of infinitesimal articles, for example, photon with its polarization and entangled state. In this paper, Polarization by refraction based quantum key distribution (PR-QKD) is proposed for quantum key generation and distribution. The proposed work considers three basis of polarization such as rectilinear (horizontal and vertical), circular (left-circular and right-circular), ellipse (left-ellipse and right-ellipse) and refraction factor. This quantum key can be used for secure communication between two users who are spatially separated and also offer intrusion detection ability to detect attackers. The theoretical approach and conceptual results are discussed in this paper.*

***Keywords:** Quantum key distribution, polarization, refraction, photon, secure communication.*

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

**Gunasekaran M***, Associate Professor, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, E-mail: sangraghav@gmail.com.

**Gopalakrishnan B**, Associate Professor, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, E-mail: bgopal1977@gmail.com

**Amitabh Wahi**, Professor, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, E-mail: awahi.bit@gmail.com.

## I. INTRODUCTION

Cryptography is an art of encrypting and decrypting messages and exists as long as the people have disbelieved among themselves and want to have secure data transfer among them. The classical cryptography [1],[2] methods can be classified as either public-key or secret-key and are currently used cryptography technique for transmission of messages between two users in a network.

The general public key encryption [3] depends on two keys, for example, Public key and Private key. Utilizing this technique, anybody can communicate something specific since people in public key is utilized to encode messages, yet just somebody with the private key can unscramble the messages. Since the encoding and unscrambling keys are extraordinary, it isn't important to safely appropriate a key. There is an issue with this strategy is that the trouble of the scientific issues is expected, not demonstrated. All the security will be disappeared if productive calculations are found. Therefore quantum key generation and distribution come closer to the real world.

In Secret key encryption [4] two clients at first create a secret key, by which extensive string of arbitrarily picked bits and safely shares among them. At that point, the clients can utilize the secrete key. The calculations are exceptionally intricate and can be planned so that all of the yields depend on all of the information. There are two fundamental issues with secret key encryption; the first is that by investigating the openly known scrambling calculations, it once in a while gets simpler to unscramble the message. The subsequent one is that it experiences the key-distribution issue. So, when someone gets their hands on a symmetric key, they can decrypt everything encrypted with that key.

Quantum theory [5][6] is undoubtedly one of the best logical accomplishments of the twentieth century. It gives a uniform system to the development of different present day physical hypotheses. After over 50 years from its initiation, quantum hypothesis wedded with software engineering, another incredible scholarly triumph of the twentieth century and the new subject of quantum calculation was conceived.

Quantum PCs were first pictured by Nobel Laureate physicist Feynman [7] in 1982. He envisioned that no old style PC could reenact certain quantum wonders without an exponential stoppage, in this manner comprehended that quantum mechanical effects should offer something genuinely new to figuring. In 1985, Feynman's contemplations were elucidated and formalized by Deutsch in a unique paper [8] where a quantum Turing machine was depicted. In particular, Deutsch displayed the procedure of quantum parallelism reliant on the superposition standard in quantum mechanics by which a quantum Turing machine can encode various commitments on a comparable tape and play out a calculation on all of the information sources at the same time. Also, he suggested that quantum PCs may have the choice to play out specific sorts of computation that old style PCs can simply perform inefficiently.

In view of the ongoing advances in quantum figuring and quantum data hypothesis, the quantum PC presents genuine difficulties to the generally utilized the current cryptographic system. The improvement of quantum cryptography defeats the inadequacies of traditional cryptography and achieves these noteworthy accomplishments by using the properties of minute articles, for example, a photon with its polarization and ensnared state. In this proposition, we have presented the PR-QKD convention for Quantum Key Generation and Distribution. The proposed work considers three premises of polarization, for example, rectilinear (even and vertical), round (left-roundabout and right-round), oval (left-circle and right-oval) and refraction factor. This quantum key can be utilized for secure correspondence between two clients who are spatially isolated and furthermore offer interruption discovery capacity to identify aggressors.

The objective(s) of the proposed work focuses:

- To generate and distribute quantum keys securely between two users who are spatially separated using quantum states of light and refraction factor.
- To detect the intruders who try to intercept the quantum key during the key generation using fundamental laws of quantum physics and quantum information theory.

The aim of this paper is as follows: Section I to give a brief introduction and a glimpse of the cryptography, quantum theory and quantum computation; Section II is a survey of previous research work based on quantum computation, some potential applications of quantum computation. Section III, describes the proposed approach for quantum key generation and distribution. Section IV discusses the security analysis and a brief conclusion is drawn in Section V.

## II. LITERATURE SURVEY

Quantum cryptography exploits the one of a kind and abnormal conduct of tiny articles to empower clients to safely create mystery keys just as to distinguish listening. In spite of the fact that work on quantum cryptography was started by Stephen J. Wiesner in the late 1960's, the main convention for sending private key utilizing quantum procedures was not distributed until 1984 by Bennet and Brassard.In 1984, Bennett and Brassard [9] initiated the first protocol as BB84 for producing a secret key using quantum spreads. This protocol uses the rectilinear and circular polarization bases for photons.

As of late, analysts at the University of California at Santa Barbara have announced that they figured out how to produce single photons. Single photon emanation would keep Eve from skimming off piece of a photon burst, making it conceivable to deliver a key that is secure from the most developed assaults [10]. The quantum data as captivated photons will be sent via optical fiber or wireless communication, likewise called free-space optics [11]. The troublesome with source quantum data over optical fiber is that polarizations are not held over long separations. Upgrades in optical fiber may help stretch out the separations is to utilize interferometer, seeing contrasts in stage rather than polarization. Using fiber optic cables, photon bits have successfully been transmitted over distances upto 60km, which is about 37 miles [12]. Transmitting through the air eliminates the problems of impurities in optical fiber, but so far, successful transmission has been over shorter distances and the weather conditions must be ideal.

The Quantum Information and Computation (QIC) Group [13] at the Harish-Chandra Research Institute (HRI), Allahabad is associated with look into on a wide range of points in quantum data and calculation. This incorporates quantum calculations, quantum correspondence, quantum cryptography, and hypothesis of entrapment. The QIC bunch additionally effectively works in the as of late creating field at the interface of quantum many-body material science and quantum data. Different interests remember feasible quantum PCs for ultra-cold gases and in quantum optical frameworks. We likewise chip away at establishments of quantum mechanics, geometric stages, quantum data preparing within the sight of shut time like bends and related issues.

Cryptology and Security Research Unit is a piece of the Computer and Communication Sciences Division (CCSD) [14] of the Indian Statistical Institute, Kolkata. It is a fundamental segment of R C Bose Center for Cryptology and Security, a national center for cryptographic necessities, front line investigates exercises and indigenous limit working in every single important field of study. The Unit goes for the advancement of interdisciplinary research in Mathematics, Computer Science and Statistics towards the encouragement of instructing, look into just as preparing and improvement in Quantum Computation Cryptology and Cyber Security.

QuNu Labs [15] is the first quantum key distribution company in India. QuNu Labs has also partnered with Indian Institute of Technology (IIT), Madras with the aim of developing a working QKD product that would be instrumental in securing sensitive data across various public platforms. The system will provide for an unconditionally secure network over an optical link in excess of 40km, suitable for use in metro cities. These products will be utilized by government bodies, open/private undertakings, banks, military and organizations the nation over that require secure information.

In the symmetric key crypto-frameworks, both the correspondence parties have an indistinguishable mystery key for encryption and decoding calculations.

In old-style frameworks, the procedure for key trade isn't genuinely verified, QKD, then again, depends on the quantum mechanical inconceivability of copying data (non-cloning) without alarming the transmitter and collector. Likewise, the procedure of duplication modifies the first information unavoidably. These two variables consolidate to give supreme security of QKD conventions.

There are not many gatherings working in India in the region of quantum figuring [16] when contrasted with different nations. During the most recent decade, there are under 100 worldwide diary productions from India on quantum registering. This is under 2% of research commitment from India to the world's exploration yield. Inside India,

we have to distinguish bunches working in the zone of PC calculations,physical science, gadgets and materials designing with interests in quantum registering. It is an exceptionally interdisciplinary region. PC researchers and mathematicians need to take a shot at calculations, building issues for adaptable framework, information stockpiling and information transmission while others will concentrate on the physical acknowledgment of the fundamental components of the quantum PCs.

## III. PROPOSED PR-QKD APPROACH

Cryptography, the encryption of messages and data, has always been a fundamental topic in the field of communication. A wide variety of different methods were developed over the centuries in order to prevent decryption by third parties. However, all encryption methods have weaknesses; no method is considered entirely secure. Quantum cryptography takes benefit of the unique and unfamiliar behavior of microscopic objects to ensure users to securely create secret keys as well as to identify eavesdropping. The message sent using quantum cryptography would be in an unknown quantum state so they could not be copied and sent on. The effect produced by measuring a quantum property is irreversible, which means an Eve dropper put back a quantum message to its original state. In this paper, a PR-QKD protocol is introduced for Quantum Key Generation and Distribution based on the properties of Refraction and Polarization Entanglement.

### A. System Description

The system model of the PR-QKD protocol is presented in Fig. 1 which consists of pulsed light source, transparent crystal, light sensor, wavelength sensor and polarizer. The pulsed light source is used to produce single or periodically repeated bursts of light lasting from fractions of microsecond to several tens of milliseconds. A polarizer is an optical channel that lets light influxes of a particular polarization go through while blocking light floods of different polarization. It can channel a light discharge of blurry or unified divergence into a light emission characterized polarization that is enraptured light. Transparent crystals display an optical property known as birefringence. At the point when a light beam goes through a birefringent gem, it is bowed, or refracted, at an edge contingent upon the heading of the light and furthermore its polarization, with the goal that the single beam is separated into two captivated beams. The light sensor is a dormant devices that change light energy regardless of whether perceptible or in the infra-red pieces of the variety into an electrical patterns yield. Light sensors are all the more generally known as "Photoelectric Devices" or "Photograph Sensors" in light of the fact that the believer light vitality (photons) into power (electrons). Wavelength sensor can decide the wavelength of monochromatic light, discharged from gadgets, for example, lasers and LEDs, and decide the ghostly pinnacle of light containing numerous wavelengths. The top layer intersection assimilates the shorter wavelengths and passes the more extended ones.

In this work, it emits the light beam which falls on the transparent crystal and gets refracted as ordinary ray and extraordinary ray. The ordinary ray has been polarized randomly based on rectilinear, circular, elliptical base and accordingly qubits are generated. The extraordinary will be sensed by light sensor and wavelength sensor to measure the intensity, wavelength of incident light and angle refraction respectively and generate binary string that will be appended with the qubits to increase the key strength. The same process will be done by the receiver side vice versa. Finally the sender and receiver agree a common quantum secret key for encryption and decryption.

### B. PR-QKD Protocol Description

The Fig. 2 shows overview of the proposed Polarization by Refraction based Quantum Key Distribution (PR-QKD) protocol. The light source generates the light beam with varying intensity which falls on the transparent crystal and gets refracted as ordinary and extraordinary rays. The refracted extraordinary rays have been sensed by sensors (light and wavelength sensor) to measure the intensity, angle of incidence and wavelength of the incident ray. Based on the measurements the 3-bit string (R-Bits) are determined as:

(i) Determination of First bit (intensity):

Step-1:Measure the intensity of each refracted extraordinary ray and find the average.

Step-2: If the average intensity of refracted extraordinary ray is greater than the intensity of the each ray then set to ‘1’ otherwise ‘0’. Perform the XOR operation on these binary strings and the resultant bit is considered as first bit.

(ii) Second bit (wavelength):

Step-1: Find the difference between each incident wave lengths with its refracted wavelength respectively. If the difference is positive then set to ‘1’ otherwise ‘0’ for each pair of wavelengths.

Step-2: Perform XOR operations on these binary strings and the resultant bit is considered as second bit.

(iii) Third bit (angle of incident):Step-1: If the angle of the refracted extraordinary ray is greater than 90 degree then set to ‘1’ otherwise ‘0’.

Step-2: The resultant bit is considered as third bit

The photon of refracted ordinary ray pass through the Transparent Crystal placed before the polarizer. The polarizer measures the state of the photon based on rectilinear (Horizontal – H or Vertical – V), Circular (Left Circular – Lc or Right Circular – Rc) and Elliptical (Left Elliptical – Le or Right Elliptical – Re) basis.

Horizontal = 0, Vertical = 1
Left-Circular = 0, Right-Circular = 1
Left-Ellipse = 0, Right-Ellipse=1

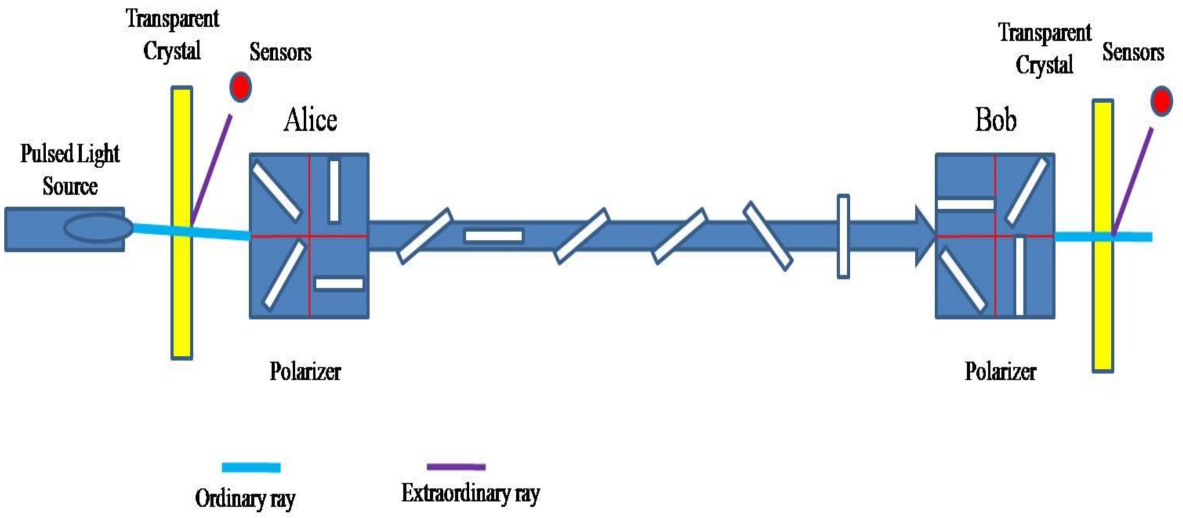


**Fig. 1: Block Diagram for Quantum Key Generation**

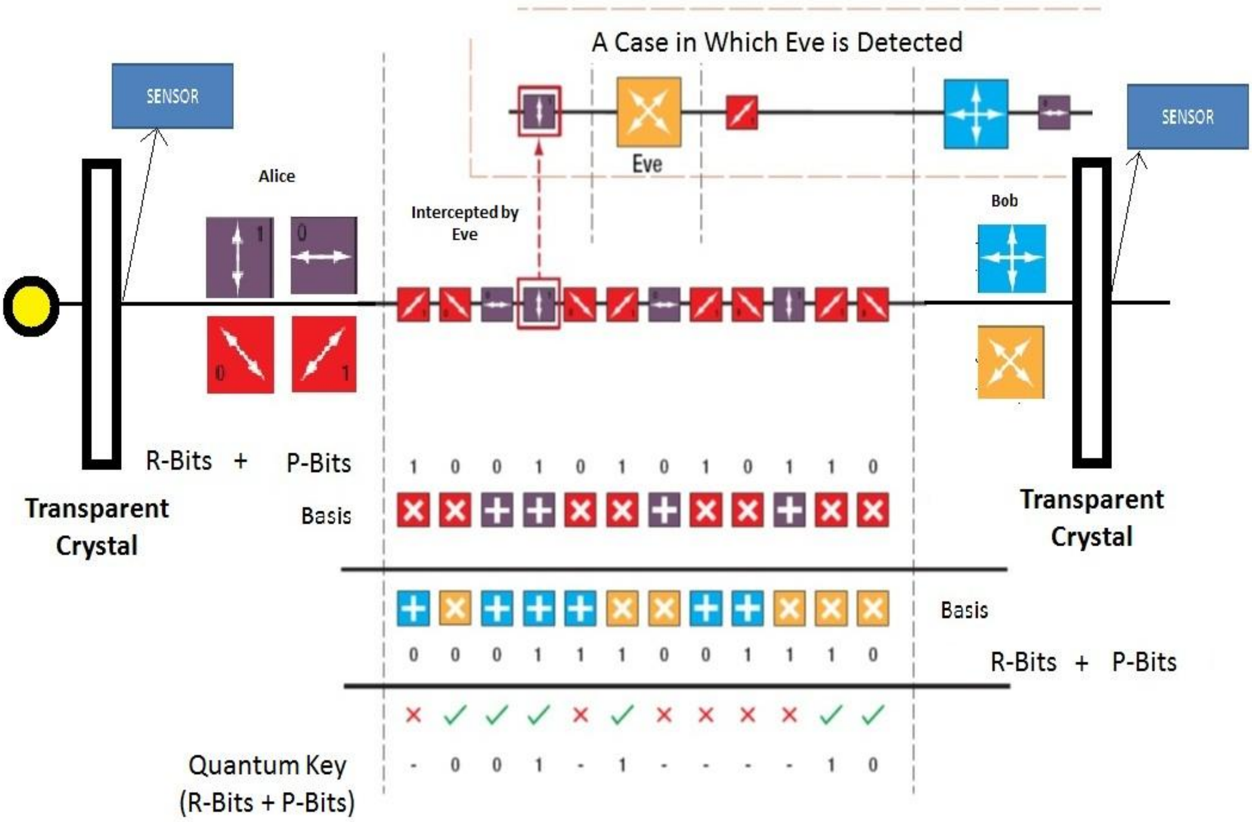


**Fig. 2: PR-QKD Protocol**

The PR-PKD protocol is explained below using the following considerations such as Alice sends the information, Bob receives information sent by Alice and Eve is the Eavesdropper.

Step1: Alice collects photons arbitrarily after refraction using ordinary ray with respect to rectilinear or circular or elliptical polarizations. In addition it also collects the intensity, wavelength and angle of refraction of the extraordinary ray.

Step 2 : Alice records the Bit string (R-Bits) based on the intensity, wavelength, angle of refraction of the extraordinary Ray.

Then the Polarization of the ordinary ray (P-Bits) is calculated. Further the R-Bits are appended with the front of the P-Bits).

Step 3: Bob accepts Photon and haphazardly measure its polarization according to rectilinear, circular or elliptical basis. He also measures the type and the resulting polarization measured (P-Bits). Then intensity of the polarized extraordinary is recorded (R-Bits). Further the R-Bits are appended with the front of the P-Bits).

Step 4: Bob openly communicates Alice that the measurement of (R-Bits + P-Bits) , But not with the results of Measurement.

Step 5: Alice openly conveys Bob by measuring the correctness of the P-Bits. A correct Measurement is correct type of Bob's P-Bits used the same basis for measurement as Alice did for preparation.

Step 6: Alice and Bob both discards the data in which measurement were not in correct type and convert the residual data to a string of bits using following process.

Horizontal (H) = 0, Vertical (V)= 1
Left-Circular (Lc) = 0, Right-Circular (Rc) = 1
Left-Ellipse (Le) = 0, Right-Ellipse (Re) =1

Step 7: Finally Alice and Bob's R-Bits are XORed and appended with the front side of generated key of P-Bits. The resultant key is agreed by both parties as quantum key for encryption and decryption.

Fig. 3 shows the flow diagram of PR-QKD protocol. The first bit is set to 1 when the average intensity of the extraordinary ray is greater than the intensity of the each ray, second bit is set to 1 when wave length difference is greater than 0 and the third bit is set to 1 when the angle of refracted extraordinary ray is greater than 90, otherwise, for all the three cases it is set to 0.

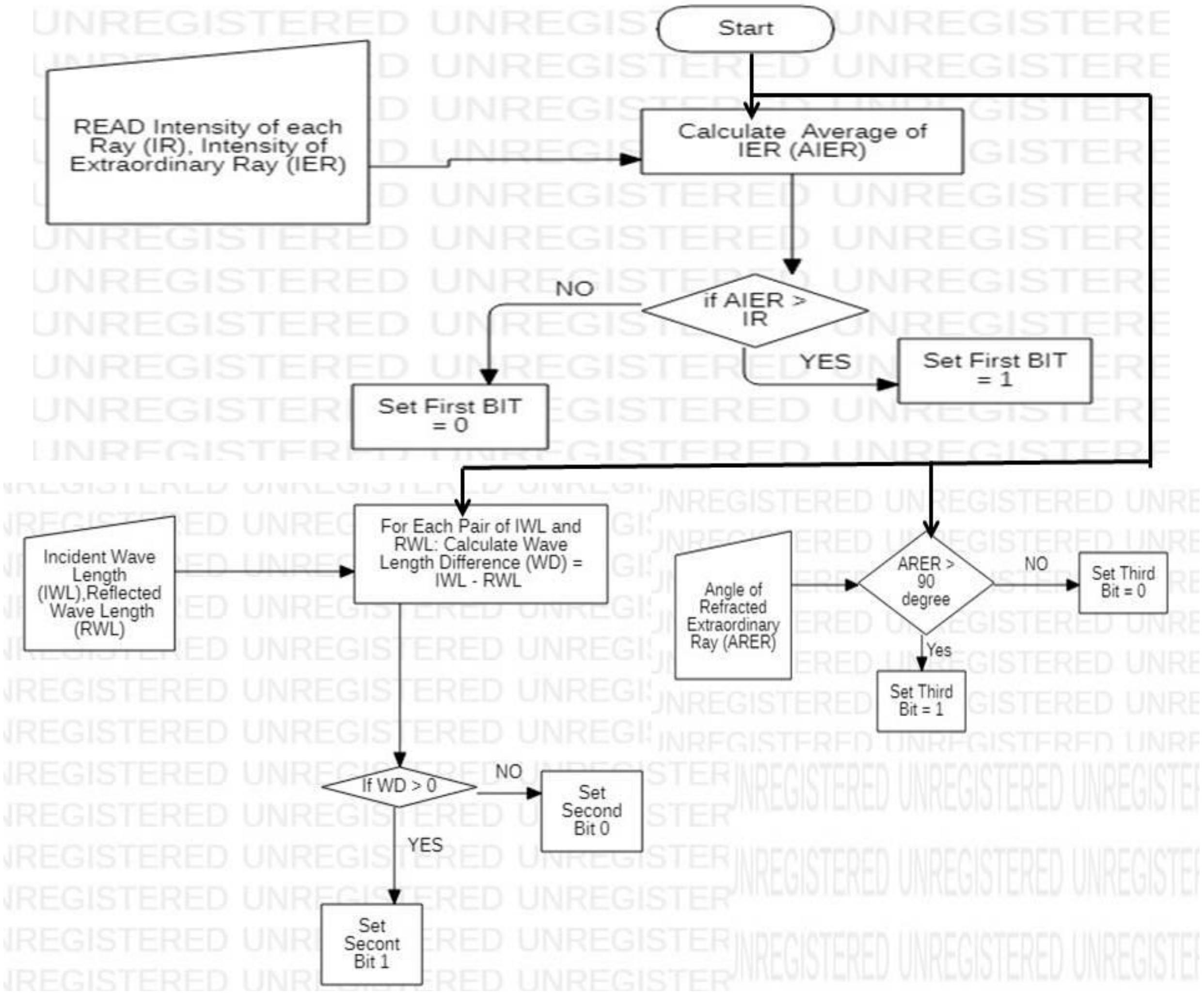
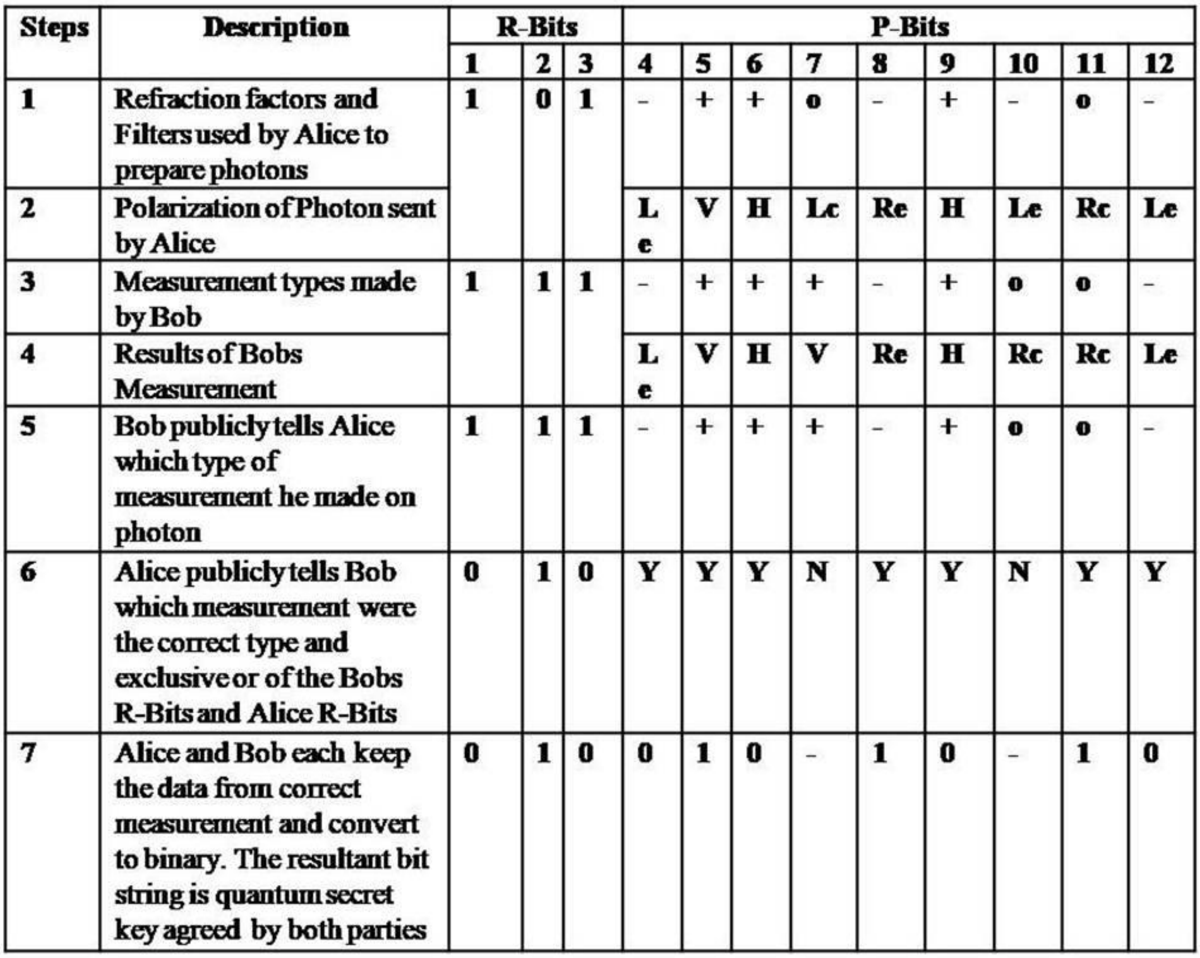

Start
READ Intensity of each Ray (IR), Intensity of Extraordinary Ray (IER)
Calculate Average of IER (AIER)
NO
if AIER > IR
YES
Set First BIT = 1
Set First BIT = 0
Incident Wave Length (IWL),Reflected Wave Length (RWL)
For Each Pair of IWL and RWL: Calculate Wave Length Difference (WD) = IWL - RWL
Angle of Refracted Extraordinary Ray (ARER)
ARER > 90 degree
NO
Set Third Bit = 0
Yes
Set Third Bit = 1
If WD > 0
NO
Set Second Bit 0
YES
Set Secont Bit 1

**Fig. 3 Flow Diagram of PR-QKD Protocol**

## IV SECURITY ANALYSIS

**Table I shows the Quantum Key Generation without Eavesdropper.**

Table I: Quantum Key Generation without Eavesdropper



| Steps | Description | R-Bits | | | P-Bits | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | Refraction factors and Filters used by Alice to prepare photons | 1 | 0 | 1 | - | + | + | o | - | + | - | o | - |
| 2 | Polarization of Photon sent by Alice | | | | Le | V | H | Lc | Re | H | Le | Rc | Le |
| 3 | Measurement types made by Bob | 1 | 1 | 1 | - | + | + | + | - | + | o | o | - |
| 4 | Results of Bobs Measurement | | | | Le | V | H | V | Re | H | Rc | Rc | Le |
| 5 | Bob publicly tells Alice which type of measurement he made on photon | 1 | 1 | 1 | - | + | + | + | - | + | o | o | - |
| 6 | Alice publicly tells Bob which measurement were the correct type and exclusive or of the Bobs R-Bits and Alice R-Bits | 0 | 1 | 0 | Y | Y | Y | N | Y | Y | N | Y | Y |
| 7 | Alice and Bob each keep the data from correct measurement and convert to binary. The resultant bit string is quantum secret key agreed by both parties | 0 | 1 | 0 | 0 | 1 | 0 | - | 1 | 0 | - | 1 | 0 |

Quantum Secret Key = 0100101010

**Quantum Key Generation with Eavesdropper**

Eve is positioned such a way that the light transmitted from Alice is measured and then it tries to transmit the indistinguishable information to Bob. Table II shows the quantum key generation with Eavesdropper.

The following two possibilities are considered for eyedropper detection:

**Eve picks the same basis as Alice**

In this case, Eve processes the signal that Alice drives correctly. Therefore, Eve will be retransmit the correct result to Bob in the same basis that was initially sent by Alice. Now Bob arbitrarily select the basis, and again it leads to two possibilities:

**Bob elects the identical basis as Alice:** Eve has transmitted the signal with respect to the same basis. Thus Bob obtains exactly the polarization state sent by Alice without detecting the presence of Eve.

**Bob chooses the other basis:** By considering different basis received and transmitted by Therefore, one among the detectors will respond at casual. However, when Alice and Bob now compare their basis (same result as in the preceding subsection), this measurement will be discarded by Alice and Bob since both have different basis.

**Eve selects the wrong basis**: In this scenario, Eve pick out a different basis used by Alice and among the Eve's detectors will react at random. Hence, Eve is not able to arbiter the correct basis. Once Eve transfers the signal to Bob, alice will send the bits in the actual basis it has been received from Bob.

Since Bob is also arbitrarily selecting his basis, there are two possibilities:

**Bob picks up a different basis than Alice:** This measurement is rejected by both Alice and Bob while matching the basis.

**Bob selects the same basis as Alice**: This case produces the error which allows Alice and Bob to detect Eve eavesdropping. Keep in mind that Alice and Bob have confirmed that they sent and received the signal using the same basis, so the measurement is not discarded. However, Eve was eavesdropping in a different basis. This means two random detections took place: Eve in intercepting Alice's signal (because her basis did not match Alice's) and Bob's in receiving the intercepted signal (Because his basis did not match Eve's).

In half of the cases the correct detector responds for Bob, so that he receives the same bit which Alice sent. But in the other half of the cases, the other detector will detect the photon. Therefore Bob obtains a different bit than the one sent by Alice.

Table II: Quantum Key Generation with Eavesdropper

| Steps | Description | R-Bits | | | P-Bits | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | Refraction factors and Filters used by Alice to prepare photons | 1 | 0 | 1 | - | + | + | o | - | + | - | o | - |
| 2 | Polarization of Photon sent by Alice | | | | Le | V | H | Lc | Re | H | Le | Rc | Le |
| | Eavesdropper | 0 | 0 | 1 | H | | | | Lc | | | | H |
| 3 | Measurement types made by Bob | 1 | 1 | 1 | + | + | + | + | - | + | o | o | + |
| 4 | Results of Bobs Measurement | | | | H | V | H | V | Lc | H | Rc | Rc | H |
| 5 | Bob publicly tells Alice which type of measurement he made on photon | 1 | 1 | 1 | + | + | + | + | - | + | o | o | + |
| 6 | Alice publicly tells Bob which measurement were the correct type and exclusive or of the Bobs R-Bits and Alice R-Bits | Y | N | Y | N | Y | Y | N | N | Y | N | Y | N |
| 7 | Alice and Bob each keep the data from correct measurement and convert to binary. The resultant bit string is quantum secret key agreed by both parties | 1 | 1 | 0 | - | 1 | 0 | - | - | 0 | - | 1 | - |

Eavesdropper Quantum Secret Key = 1101001

## V. RESULT ANALYSIS

### A. Eve Dropping Level with respect to the Raw Key Length

The Eve dropping is a process of identifying the source to destination with respect to the exchange of light signal between Alice and Bob. The percentage of Eve dropping is calculated on the difference in the threshold value of the particular transitions. If the difference beyond the threshold value makes the data to be resent from the source. The Fig. 4 graph depicts the ratio of change in Eve drop percentage with respect to key size initiated at the source.

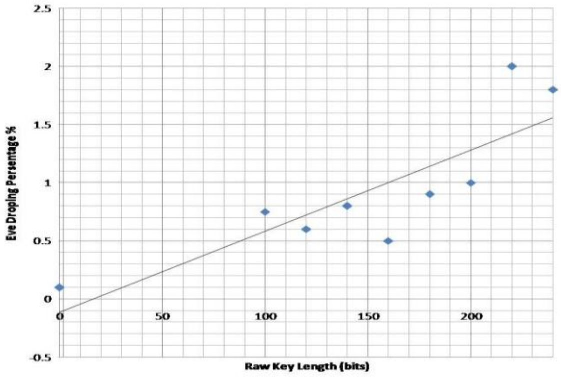


Fig. 4 Key Size Versus Eve Drop %

### B. Optimal Bias Ratio with respect to the raw key length

The bias ratio affects the key generation. The ideal bias ratio prompts the largest key length. It is increasingly effective for Alice and Bob have one basis with the high likelihood for key generation so as to maintain a strategic distance from inefficient basis disparity. The ideal bias ratio drops upto 0.5 where the key length is negligible for positive key generation. The Fig. 5 shows the optimal bias ratio for the minimum key length.

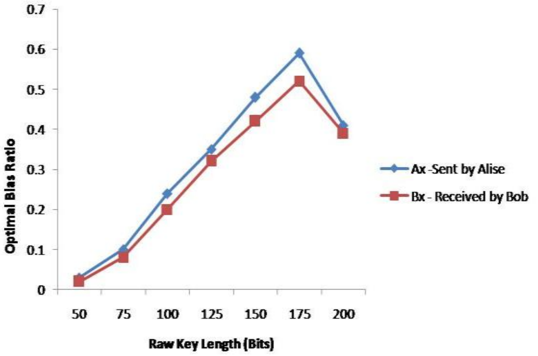


Fig. 5 Key Size Versus Optimal Bias Ratio

## VI. CONCLUSIONS

Cryptography is the specialty of encoding and unscrambling messages and exists as long as the individuals have doubted from one another and need secure correspondence.

Retrieval Number: F8222038620/2020©BEIESP
DOI:10.35940/ijrte.F8222.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The traditional techniques for encryption naturally depend on either public key or secret key approach and have its own flaws in quantum computers. The improvement of quantum cryptography beat the deficiencies of old style cryptography and achieves these huge accomplishments by using the properties of infinitesimal articles, for example, photon with its polarization and entangled state. The Polarization by refraction based quantum key distribution (PR-QKD) approach for quantum key generation and distribution perform better when the quantum computers ar in the picture. The PR-QKD considers three basis of polarization such as rectilinear (horizontal and vertical), circular (left-circular and right-circular), ellipse (left-ellipse and right-ellipse) and refraction factor. This quantum key can be used for secure communication between two users who are spatially separated and also offer intrusion detection ability to detect attackers. The theoretical approach and conceptual results ensures that the proposed PR-QKD perform better in quantum computers.

## REFERENCES

1. L. Von Ahn, M. Blum, N. J. Hopper and J.Langford, Captcha: Using hard ai problems for security. International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2003, pp. 294–311.
2. W. Stallings, Cryptography and Network Security: Principles and practice, 2nd edition, prentice hall, 1998.
3. B. Batt, Encryption: Strengths and Weaknesses of Public-key Cryptography, 2017.
4. D. S. A. Elliminaam, H. M. Abdual-Kader and M. M. Hadhoud, Evaluating the performance of symmetric encryption algorithms, International Journal of Network Security, vol. 10, pp. 216-222, 2010.
5. C. A. Fuchs, Quantum Foundations in the Light of Quantum Information, in Decoherence and its implications in quantum computation and information transfer, Proceedings of the NATO Advanced Research Workshop, Mykonos Greece, June 25–30, 2000, edited by A. Gonis and P. E. A. Turchi (IOS Press, Amsterdam, 2001), pp. 38–82.
6. J. T. Cushing, A. Fine, and S. Goldstein, Bohmian Mechanics and Quantum Theory: An Appraisal, (Kluwer, Dordrecht, 1996).
7. R.P. Feynman, Simulating physics with computers, International Journal of Theoretical Physics 21 (1982) 467–488.
8. D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, Proceedings of The Royal Society of London A 400 (1985) 97–117.
9. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, pp. 175 – 179, D1984.
10. G. Collins, Quantum cryptography defies eavesdropping. Physics Today, November 1992, pp. 21-23.
11. J. Savani, Eavesdroppers beware: Single photon emission prepares way for quantum cryptography. UCSB college of engineering press release.
12. http://www.engineering.ucsb.edu/announcequantum_cryptography.
13. http://searchhp.techtarget.com/Definition /0, sid6_ gci284012,00.
14. http://www.hri.res.in/~qic/contact.html
15. http://www.hri.res.in/~qic/contact.html
16. www.qunulabs.in/
17. M. Jagadesh Kumar, “Quantum Computing in India: An Opportunity that Should Not Be Missed,” IETE Technical Review, vol.31 (3), pp.187-189, May-June 2014.

## AUTHORS PROFILE

**Dr M Gunasekaran** defended Ph. D in Information and Communication Engineering from Anna University Chennai in the year 2014 and completed M. E. Degree in Computer Science and Engineering from Anna University Chennai in the year 2009. He has published more the 40 papers in national / international journals and conferences. His area of interest is Wireless ad hoc networks and internet of things. Currently he is working as Associate Professor in the Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, and Tamilnadu, India.

**Dr B Gopalakrishnan** has completed Ph. D degree in Information and Communication Engineering from Anna University Chennai in the year 2014. He has completed his M. E. Degree in Computer Science and Engineering from Anna University Chennai in the year 2006. He has published more the 20 publications in the area of Network Security and IoT Security for Wireless networks. He is working as Associate Professor in the Department of Information Technology, Bannari Amman Institute of Technology Sathyamangalam, Tamilnadu, India.

**Dr. Amitabh Wahi**, Professor, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, TN, India got Ph. D. degree in the area of Neural Network and Fuzzy Logic and Pattern Recognition from Dept. of Electronics Engineering, IIT-Banaras Hindu University, Varanasi in 1999 and also he has graduate and post graduate degrees in Physics. He has more than 19 years of research and teaching experience. His current research interests include computer vision, image analysis, soft computing, pattern recognition, security and in computer science. He has guided 10 Ph. Ds. research scholar many M. Phil./M. Tech. students in these areas and also involved in consultancy projects from the industries. Also, he has successfully completed the research projects funded by AICTE and DRDO, New Delhi as Principal Investigators respectively. He has published 116 technical papers in International / National Journals and in International / National Conferences/Seminars/workshops.