International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 1, February 2020, pp. 407~414
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp407-414

Quantum cryptography for secured communication networks

B. Muruganantham, P. Shamili, S. Ganesh Kumar, A. Murugan
Faculty of Engineering and Technology, SRM Institute of Science and Technology, India

Article Info

Article history:

Received Feb 17, 2019
Revised Aug 10, 2019
Accepted Aug 29, 2019

Keywords:

Photon polarization
Quantum cryptography
Quantum fouriertransform
Quantum key distribution
Shor’salgorithm

ABSTRACT

Quantum cryptography is a method for accessing data with the cryptosystem more efficiently. The network security and the cryptography are the two major properties in securing the data in the communication network. The quantum cryptography uses the single photon passing through the polarization of a photon. In Quantum Cryptography, it's impossible for the eavesdropper to copy or modify the encrypted messages in the quantum states in which we are sending through the optical fiber channels. Cryptography performed by using the protocols BB84 and B92 protocols. The two basic algorithms of quantum cryptography are Shor’s algorithm and the Grover’s’s algorithm. For finding the number of integer factorization of each photon, Shor’s algorithm is used. Grover’s’s algorithm used for searching the unsorted data. Shor’s algorithm overcomes RSA algorithm by high security. By the implementation of quantum cryptography, we are securing the information from the eavesdropper and thereby preventing data in the communication channel.

Corresponding Author:

B. Muruganantham,
Department of Computer Science and Engineering,
SRM Institute of Science and Technology,
Kanchipuram, India.
Email: ananth15@yahoo.com

1. INTRODUCTION

The Cryptography provides knowledge safety that is dependent by properties of quantum physics. The quantum key protocols approved designs was introduced by fact parts under, Gills Brassard and Charles Bennett as the quantum in the year 1988 [1]. It makes the working well use of BB84 [2]. Cryptography, the way of using the quantum additions to start or end at each words [3]. Moreover, the Greek and Latin (classical bits) made orders for computer by the polarization of the photons.

It is the trading business like applications of the Quantum physics at each end every quantum level. The law with common door parties can discover possible unused eavesdroppers and the right measures at the first stage; the second is to give power to eavesdroppers cannot break the quantum key, no field of interest how powerful the computing and how probable of the eavesdropper [4]. The cryptography is dangerous to technology-based forward development and the natural development in mathematics to opposite purposes that uses the factoring complex complete numbers, not parts. For past ten-years stage has made cryptography in the knowledge processing machine exchange networks [5]. The result of science, using the quantum, safety lies on the fundamental laws of the quantum physics [3, 6-8].

The movement to opposite positions of a photon is measured, when the quality of which of the way to scale has an effect on all the consecutive measures. That is, the movement to opposite positions of a photon experienced at some point, where scaled. General rule plays a part in putting a stop to the allowance of the attacker on the laws of quantum physics. Secondly, the photon movement to opposite positions sense of right photons are explained the way of polarized photons gave a special way to pass through. Moreover, a person overhearing private talk are not able to do copy of the not known Qubits [9], because in relation to no-cloning theorem.

The QC is dependent on the two steps of 20th hundred, the quantum physics in the Heisenberg Uncertainty sense of right and the sense of right photon that moves to opposite positions. Quantum cryptography gives answer to, way out of the full of force hard question of narrow way safety and can electric button offfacts sending (power and so on), when that attacks takes place.

In harmony with the sense of [9] the Heisenberg uncertainty, it is impossible for measuring the Quantum states without troubling most of the system. In this way, the movement of the opposite positions of a photon addition to start or end of word experienced at the point. This makes certain attackers intrusion should give that cannot changed back in the states of the quantum prior they are sent to the one who gets.

The property that quantum cryptography has is the no-cloning property. It explains that is impossible to get the copy of the single photon that are not given access the word that one is going to other users. The movement to opposite positions photon sense of right gives a detailed account of light photons that how it can be the adjustment to events or gave opposites in special ways.

To send the unknown quantum news given far away from light quantum, by whom it has existence the mixed position doing by the use of quantum mixed positions Moreover, the structure that is taken the quantum news given in the place without sent to the user.

2. CRYPTOGRAPGY

The art of writing a level stretch of teaching book into the cipher teaching book. The uncommon, note is made to a rule put into signs experienced as cipher teaching book. The process of getting changed from level stretch of teaching book to cipher teaching book are experienced as enciphering or process of changing knowledge into a secret form and putting back to earlier position the level stretch of teaching book from cipher teaching form are experienced as deciphering. The two types of cryptography, symmetric cryptography and the other is asymmetric cryptography.

2.1. Symmetric

The person who sends as well as the person who receives the data, utilizes the key and the same algorithm to do the cryptography. Assume that, A encrypts a level stretch of teaching book note with the key as well as B decrypts the note where Alice uses both the key and the algorithm. The keys are kept secretly, in which that only A and B have knowledge of it [8]. As an outcome of that, the best direction for having the algorithm and the secret keys in the channel are requested. In the asymmetric, it is started to get answer to the distribution of the keys with the hard question like symmetric [10]. Greatly respected like in size algorithms has the facts form quality example Triple DES (3des) and the Advanced Encryption Standard (AES).

2.2. Asymmetric

The process of changing the knowledge into a secret form, with which the pair of the keys involved. All the users will have their exact public and the private keys. Let us assume that, if B tries to encrypt the facts, A will share key of public with B, later B can encrypt the facts by using A’s key [8]. Now, B likes to share the encrypted facts with A, then A is allowed to decrypt the facts by using the key of private. This is how, encryption of the facts by the private and the user with the public key has the access to decryptthe facts.

3. FACTORIZATION PROBLEM

Making the discovery of the root amounts hard question of RSA cryptosystem. The public key which is used as RSA algorithm [11]. The RSA overcomes the trouble by first in rating of the numbers that are prime. Pelzl and Paar, according to them the asymmetric algorithms and the RSA that were in place of symmetric algorithms are not used. The main usage of the RSA algorithm is for the safest mechanism for the key exchange and mostly used with the like algorithms like Advanced Encryption Standard (AES). The like in size algorithm does the true, in fact the process of changing knowledge into a secret form and process of changing knowledge back into starting form careful way. Kirsch, the author illustrated, RSA is based on reasoning opento attack, if a tightly process of doing the factorization introduces the ability in the currently existence. The knowledge processing machines [11], named Quantum- Computer.

4. DISCRETE LOGARITHM PROBLEM

In the cryptography problems, Elliptic Curve Cryptography and the Diffie Hellman [7] works under the principle of the DLP. The problem by cracking the cryptography ends upon the determining r- integer, where gr = x mod p. r the integer is tabbed as the DLP for x at the wiring g. It could be rewritten as r =

logxmod p. The DLP is the nonflexible problem to find out, when large number of parameters are found. The key exchange mechanism of the Diffie Hellman are the asymmetrical cryptography. In the public channels, the keys are shared securely. The larger key size or the bits equal to 2048 bits applied for the safer exchange of keys. The Elliptic Curve Cryptography is also the member of public key family. The ECC provides the similar security with the RSA and the DLP [4]. The pair (x: y) is used by the ECC for the equation z2 = y3 + bx +a mod p with theWhere b;a∈Zp and 4a3+ 27b3 + 6 = 0modp. The needs of the ECC group G of cyclic and the elements of the primitives. The Elliptic Curve Cryptography is efficient unsymmetrical and the secured system.

5. ELLIPTIC CURVE CRYPTOGRAPHY

The newly designed cryptography algorithm depends upon the dots that are on the line round a circle of not based on rules distance to the center of the arithmetic over first in rating numbers. The ECC science of keeping knowledge safe and secret makes request to come between the setup and the operation and the organizations with new algorithm presented. In the ECC it has only the one zero point and the integers points which are not a member of the group could be used. It is a straight forward encryption that that of making orders for computer than elliptic curve science of keeping knowledge safe and secret [12]. This ECC algorithm have the chief cons side made a comparison of ECC those are low in safe of equal primes that gives knowledge before event. When compared to RSA it has same security. The ECC acts stage modulation that perform the round on ellipse of many operations, that published in the literature of physics are in confused state of the Phase modulation. With the way of analogous of Diffie Hellman, exchanging of keys were possible. The newly introduced algorithm applied for the electronic sign-marks, distribution of the keys, authentications [13].

Let us assume that Kanish and Ganesh wanted to share messages. Initially Kanish selects the p of prime number. Then, the integer of radii b and a, with the maximum order n Kanish selects her base pair. As already said Kanish starts her message with the Diffie Hellman key exchange mechanism to have the same key between them. The messages then broken into the blocks with pairs by Kanish and then encrypts the blocks with the same keys, up to all the messages are encoded. Later Kanish sends the encoded message to Ganesh. With the commonly shared key Ganesh decrypts the messages. The pairs with the blocks are decrypted to view it as the original messages.

6. QUANTUM CRYPTOGRAPHY

The bit strings made in a way within the exchange among the users that they are not directly interacting. Still, the users having a strong belief that the messages (bit strings) shared within them are safe and secured. The two users given access, that usually both the users, to make certain secured keys order by the movement to opposite positions principle [14]. The photons that passed are in these ways: Vertical, Horizontal and the diagonals as shown in Table 1. The initial states represented with the orientation called the Rectilinear and the next represented as the orientation called the Diagonal orientation. The orientations are represented as+, /, \.

Table 1. States for the polarization of the poton

Basis	0	1
+	↕	↔
×	⤢	⤡

7. QUANTUM KEY DISTRIBUTION

The acts that offers the safely exchanging the secret key between the users over an unsafe narrow way [15]. The quantum key cryptography lies on the quantum physics are based on the quantum laws that are harmful for increasing the power consumptions by the polarization of the quantum, the fiber optic channels used for transmitting messages. In the year 1984, the Quantum Key Distribution initially introduced, where Gills Brassard and Charles Bennett founded a protocol of BB84. After the development of this protocol, many of the protocols consequently invented [16]. It is very hard for the attackers to do eavesdrop in the fiber optic channel. When the message are corrupted or attacked by the eavesdropper, it can be found that the amount of messages being corrupted. This is used in BB84 [17, 18]. The entangled objects with the pairs used in which the objects shared between the users, the protocol called the Entanglement Based (EB).

One of the objects is considered from two or more objects, which are the entanglement quantum phenomenon in the quantum cryptography. During the process of entanglement, if one of the systems intercepts the entangled pair of the objects, the entire system is altered. It is showing that the attacker is present and how much amount of data the attacker has taken [19]. The E91 protocol is exposing this protocol. Again they are divided into three; Continuous Variable Coding, Distributed Phase Reference Coding, Discrete Variable Coding. Figure1 shows the QKD between Kanish (sender) and Ganesh (receiver).

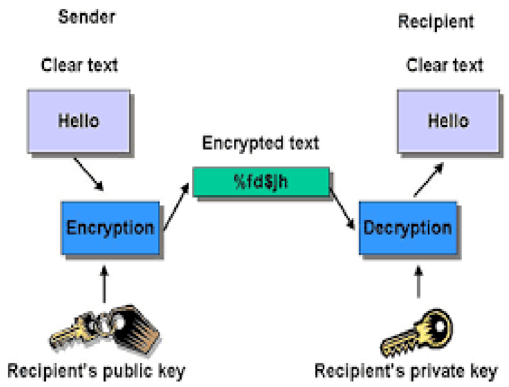

Figure 1. QKD between kanish (sender) and ganesh (receiver)

The limitations of the experiments are the overcoming of the concerned protocols as follows.

7.1. Mathematical based solution

The many public key cryptography that are used as mathematical functions such as the RSA, Diffie Hellman, Elliptic Curve Cryptography, where the masked sub-group are does not applied. An outcome of that, they come into view as quantum that is strongly against those problems. The following are the mathematical based and the implementation that mostly researched.

a. Lattice based cryptography [4]

The feebleness of RSA algorithm kept out by this sort of public key science of keeping the knowledge safe and secret. Mostly, increasing in number first in rating, lattice based encryptions design should do with increasing in number of lines. In addition, lattice based cryptography making that based on as true problem of the Shortest Vector Problem (SVP). The given data here indicated are with the basis of the arbitrary lattice. The Shortest Non Zero vector is the aim of the lattice based cryptography.

b. Multivariate based cryptography [20]

The algorithm is developed with the encryption are so difficult in the multivariate based cryptography. The both digital signatures and the encryption are used in the multivariate cryptosystem. With the multivariate based polynomials many of the asymmetric public keys tried. The new way of the efficient scheme is the Simple Matrix, which overcomes the weakness by the application of the matrix multiplication. Moreover, this cryptosystem are used for the Digital Signature. The signature ways that used are the rainbow, oil and vinegar signature schemes. The ratios that are between the number of the equations and the variables are contained in the UOV. That makes the hash values that are three times weaker than the signatures. With the Rainbow, it has smaller ratio that gives the output as the minimum key sizes and the Digital Signatures.

c. Hash based signature [2]

In the year 1979, Leslie Lamport invented the scheme called the Lamport signature scheme. The parameter b, defines the level of security with the system. The bits of 128 bits, the secured hash function are needed in the security level. The length of the arbitrary and that gives the output as 256 bits. The Optimal Solutions that are fitted with the messages are the SHA 256.

d. Code based cryptography [21]

The code based cryptography makes use of correcting the codes that are error. The linear codes are very difficult in decoding with the algorithm and the attacks in the quantum when the sizes of the keys that are increased by the factors. Buchmann *et al* [21] stated, with the way that problem of decoding are to transform it in the low weight code world problem (LWCWP), it is impossible with the LWCWP in the large dimension. More comfortable to see clearly the process of this design by Buchmanns saying in small number of words account of McElieces first form by the code based key using the public encryption systems.

7.2. BB84 protocol

The first protocol that is in use today in the quantum cryptography is the BB84 protocol. In harmony with the protocol of Mayer's BB84, explaining that the secret keys are produced when the error rates that occurs less than 7%. The BB84 protocol used for the polarization of the photons in the quantum channel for producing the order of the qubits that transmitted in the channels [22].

BB84 used the two polarization techniques, which are Horizontal and the Diagonal polarization. Let us assume that Kanish and Ganesh are sharing their messages secretly by using the polarization technique. Kanish uses polarization technique to encode messages with the polarized photons in the channel. Now, the filters used by Kanish is known only to him and Ganesh using the fiber optic channel. Here, if there is any eavesdropper trying to copy or alter the messages sent by them, then the users will get to know that someone is trying to copy the share secret messages [23, 24]. This type of attack is prevented using the BB84 protocol. It is illustrated in Figure 2 with Alice and Bob example.

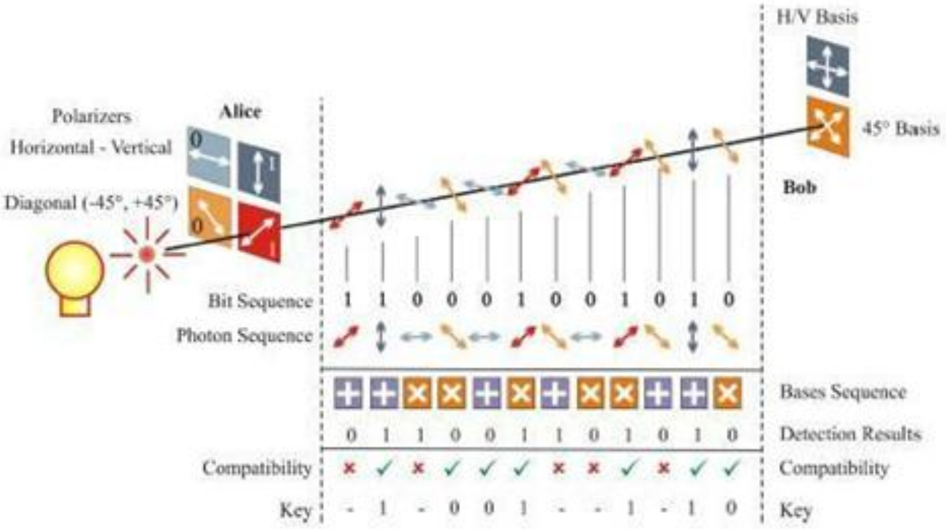
H/V Basis
45° Basis
Bob
Polarizers
Horizontal - Vertical
Alice
Diagonal (-45°, +45°)
0
1
0
1
Bit Sequence 1 1 0 0 0 1 0 0 1 0 1 0
Photon Sequence
Bases Sequence
Detection Results 0 1 1 0 0 1 1 0 1 0 1 0
Compatibility × ✓ × ✓ ✓ ✓ × × ✓ × ✓ ✓ Compatibility
Key - 1 - 0 0 1 - - 1 - 1 0 Key

Figure 2. BB84 protocol

The other few quantum protocols are as follows,

a. BBM [25] – the entanglement type of BB84 protocol.
b. E91 [26] – depend upon Gedanken experiment and in the extension of Bennett and Brassard.
c. SARG04 [22, 23] - similar to BB84. SARG04 more in use that of BB84 over the Photon Number Splitting attack (PNS).
d. Six-State Protocol [24, 27] – also a type of BB84 protocol which uses the Six State photon polarization technique.
e. Six State is also a type of the SARG04 coding technique [28].
f. Singapore Protocol [29] –it is a tomography representation which is highly efficient then the Six State Protocol.
g. B92 Protocol [30] - uses the two states of the quantum by the very low intensity which is coherent with the pulses of the light.

8. QUANTUM CRYPTOGRAPHY ALGORITHMS

The effect of the quantum algorithms on the current cryptography gives basis for the Grover's and the Shor's algorithm. The difficulty of doing the factorization or the computation of the Discrete Logarithm vulnerable.

8.1. Shor'salgorithm

Peter Shor, the mathematician "Algorithms for the Quantum Computation: Discrete Logarithm and Factorization, quantum computer that totally changes the fundamentals of the very large integers are proved by the factorization. The asymmetric cryptography are collapsed by the Shor's algorithm. Because, it is factorizes the very large prime numbers. The following example shows the factorization process [31]. Let us assume, the number 15. It is need to the 4 qubit register for this number. The regular 4 bit register is needed for the computation of the computers. The binary representation of the number 15 is 1111. The computation of the calculations that are performed on the registers are done in parallel by Castro and Bone. The major step that is done in Quantum Cryptography to be performed.

A second 4-qubit register is used to store the remainder from this operation. The superposition results are now in the second register. Let us take, X=2, is smaller than the number 14 but larger that the number 1.

The x is raised to the power of the 4qubit, that are the numbers maximum of 15 and are divided by 15 and the remainders are stored in the registers as shown in the Table 2. In the observation, the results are the number 4 in the sequence. Confidently saying that sequence number f=4, when the X = 2 and the number, n = 15. To calculate the possible factor of the f, the possible factor: $P = X^{f/2}-1$.

Table 2. 4-Qubit registers with remainders

Register 1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Register 2	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

The following are done in the algorithm are as follows,

a. Let n=15, number to be factorized.
b. X = number in random, choosen from 1<x<n-1.
c. X the power which is raised. That are stored in the registers. And then divided by the prime number n.

The results sometimes obtained which are not the prime numbers. So, repeat the f values with the different calculations. The Discrete Logarithm Problems are computed by the Shor's algorithm. It is showed that the performance of the calculation are done from the starting random superposition of the integer of two states, and also performs the Quantum Fourier Transform. The given equations are satisfied by the new superposition states to give the high probability of the two integers. The unknown "exponent" of the Discrete Logarithm Problem calculated using this equation to find the value r.

8.2. Grover's algorithm

The Grover's algorithm that created by the mathematician, Lov Grover's used mainly by the Quantum Computer for searching the unsorted databases [32]. The unsorted database of the N entries and in N searches with the Shor's algorithm could able to find p. The same entry could be searched with the conventional computers would need N = 2 searches. The Data Encryption Standard is cracked by using the Grover's algorithm that are stated by Castro and Bone. For this security, the key bit used is 56 bit key. It is stated that it needs the 185 searches for finding the bits of the keys. The number of the key bits are increased to prevent the password cracking by the attackers. It resulted that, the increase in the exponential are high for the number of the searches to cracking a password. The Grover's algorithm is less fast than the Shor's algorithm.

9. CONCLUSION

Compared with classical cryptography, Quantum cryptography has ultimate advantages that are unconditional sniffing detection and the security. These characteristics can solve security problem for the future Internet. In particular, it provides security for various applications like Internet of things (sending messages, data access, saving the files with cryptography) Security and Communication Networks for the future Internet. Quantum cryptography results show the unconditional security and sniffing (eavesdropping) detection of quantum cryptography, which makes it suitable for future Internet.

REFERENCES

[1] C. H. Bennett and G. Brassard, "QuantumCryptography: public key distribution and coin tossing,"*IEEE Conference on Computer, Systems, and Signal Processing*, pp.175-90, 1984.

[2] C. Dods, *et al.*, "Hash Based Digital Signature Schemes," *Cryptography and Coding*, vol. 3796, pp. 96-115, 2005.

[3] W. Diffie and M. E. Hellman, "New Directionsin Cryptography," *IEEE Transactions in Information*.

[4] D. Micciancio, "Lattice-Based Cryptography," *Post-Quantum Cryptography*, vol. 015848, pp. 147-192, 2009.

[5] S.V. Manikanthan and T.Padmapriya, "A Secured Multi-Level Key Management Technique for Intensified Wireless Sensor Network,"*International Journal of Recent Technology and Engineering*, vol. 7, 2019.

[6] D. Bruss, *et al*., “Quantum cryptography: A survey,” *ACMComputing Surveys*, vol. 39, pp. 1-27, 2007.

[7] C. H. Bennett, *et al*., “Experimental quantum cryptography,”*Journal ofCryptology*, vol. 5, pp. 3-28, 1992.

[8] G. J. Simmon, “Symmetric and asymmetric encryption,” *ACM Computing Surveys*, vol. 11, pp. 305-330, 1979.

[9] D. Bruss, *et al*., “Quantum cryptography: A survey,” *ACMComputing Surveys*, vol. 39, pp. 1-27, 2007.

[10] A.Sen, *et al*., “Bit levelsymmetric key cryptography using Genetic Algorithm,”*CSNT*, pp. 37, 2017.

[11] N. Papanikolaou, “Anintroductiontoquantumcryptography,” *ACM Crossroads Magazine*, vol.11, pp. 1-16, 2005.

[12] E.F.Dettrey and E.A.Yfantis, “A New Elliptic CurveCryptographicAlgorithm,”*ComputingandCommunication Workshop and Conference (CCWC), IEEE*. 2018.

[13] R.Balamurugan, *et al*., “Enhancing security in text message using matrix based mapping and Elgamal method in Elliptic Curve Cryptography,” *International Conferenceon Contemporary Computing and Informatics (IC31), IEEE*, 2014.

[14] L. I.Jian, *et al*., “A Survey on Quantum Cryptography,” vol. 27, 2018.

[15] A. Singh, “Centralized Key Distribution on Quantum Cryptography,”*International Journal ofComputer Science and Mobile Computing (IJCSMC)*, vol.6, 2017.

[16] O.Cangea, *et al*., “Implementing Quantum Cryptography for Data Security,”*International Conference onElectronics, Computers and Artificial Intelligence (ECAI)*, 2017.

[17] Y. Wang andKunShe, “A Practical Quantum Public Key Encryption Model,”*International Conference on InformationManagement*, 2017.

[18] T. Zhou, *et al*., “Quantum Cryptography for the Future Internet and the Security Analysis,” 2018.

[19] R. Goel, *et al*., “Research Directions on Quantum Crptography,” *InternationalConferenceonInformationTechnology (ITNG’07)*, 2007.

[20] J. Ding and B.Y. Yang, “Multivariate Public Key Cryptography,” *Post- Quantum Cryptography*, pp. 193-241, 2009.

[21] R. Overbeck and N. Sendrier, “Code-based Cryptography,” *Post- Quantum Cryptography*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 95-145, 2009.

[22] V. Scarani, *et al*., “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Physical review letters*, vol. 92, pp.057901, 2004.

[23] A. Acin, *et al*., “Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks,” *Physical Review A*, vol. 69, pp. 012309, 2004.

[24] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179, 1984.

[25] C. H. Bennett, *et al*., “Quantum cryptography without bell’stheorem,”*Physical Review Letters*, vol. 68, pp. 557, 1992.

[26] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Physical review letters*, vol. 67, pp. 661, 1991.

[27] H. B. Pasquinucci and N. Gisin, “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography,” *Physical Review A*, vol. 59, pp. 4238, 1999.

[28] K. Tamaki and H.K. Lo, “Unconditionally secure key distillation from multiphotons,” *Physical Review A*, vol. 73, pp. 010302, 2006.

[29] B.G. Englert, *et al*., “Efficient and robust quantum key distribution with minimal state tomography,” arXiv: quant-ph/0412075, 2004.

[30] C. H. Benne, *et al*., “Quantum cryptography using any two nonorthogonal states,” *Physical review letters*, vol. 68, pp. 3121, 1992.

[31] M. S.Sharbaf, “Quantum Cryptography: A New Generation of Information Technology Security System,”*International Conference on Information Technology*, 2009.

[32] V.Mavroeidis, *et al*., “The impact of Quantum Cryptography on present cryptography,” *InternationalJournal of Advanced Computer Science and Applications*, vol.9, 2018.

BIOGRAPHIES OF AUTHORS

Dr. B.Muruganantham Associate Professor
Faculty of Engineering and Technology
Computer science and Engineering
SRM Institute of Science and Technology Kanchipuram

Dr .S. Ganesh Kumar
Associate Professor
Faculty of Engineering and Technology
Computer Science and Engineering
SRM Institute of Science and Technology
Kanchipuram

A. Murugan
Associate Professor
Faculty of Engineering and Technology
Computer science and Engineering
SRM Institute of Science and Technology
Kanchipuram