IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 5 (May. 2018), ||VI|| PP 15-23

The Quantum Key Distribution Devices and Horizon Calculation Over Ocean Surface for Application in Various Naval Vessels

[1]Sureshkumar P H, [2]Dr. R. Rajesh
[1]SureshkumarP H, Research scholar, Bharathiar University, Coimbatore, India (Mobile:+919020439429;
[2]Dr.R Rajesh , Professor ,SreeNarayanaGurukulam College of Engineering, Kolencherry, Kerala, India
Corresponding Author: sureshkumar P H

Abstract: The quantum encryption is a method of key transfer in cryptography by using quantum entanglement of photons. The real power of quantum entanglement is instantaneous communication that is non-interceptable. The advantage of quantum encryption method is, it can be incorporated with conventional encryption methods safely. The quantum cryptography can replace conventional key exchange mechanism with the polarized photons using channels like optic fiber cables. Quantum cryptographic can also provide far and secure data communication. The present day experiments clearly proved that the quantum cryptography can be implemented through medium like optic fiber cable or air. But the distance of transmission through the air is limited by rule of line of sight propagation. The quantum key distribution will have uses in different types of communication between distant parts of earth. So this paper discussing how the visual horizon affect the quantum key distribution in naval applications over the ocean surface.

Keywords: Quantum cryptography, Communication network, Free-space optical communication

---

Date of Submission: 23-04-2018 Date of acceptance: 11-05-2018

I. INTRODUCTION

The research on quantum cryptography is critical for future fully secured communication needs. The quantum encryption can create codes that are unbreakable with non-interceptable quantum key distribution schemes. Because of this feature quantum encryption systems is considered as more secure and safer. The computing power of quantum computers increasing as compared with conventional computing systems and so can be used for breaking currently existing key distribution scenarios [1]. The different malicious activities and crimes are increasing over the communication networks . The attacks over the critical computer networks causes huge losses and it also challenging the security of nations. The implementation of quantum key encryption can significantly improve the security of communication networks. So this work can help to improve the security in communication systems. Since the quantum cryptography mainly relied on polarized photons the transmission is limited to the line of sight and hence here we discuss the various aspect of this propagation over the surface of earth.

II. QUANTUM CRYPTOGRAPHY AND THE EVOLUTION

In early 1980s, Bennet C, Benioff P, Feynman R proposed that a new powerful way of information processing was possible with quantum states . Richard Feynman was proposed this idea in 1981 that quantum systems could be performed powerful than classical computing [3] , and thus the concept of quantum computing was originated. David Deutsch was further studied it and published a paper in 1985 [4].However the origin of quantum cryptography was considering to be started since 1983 from the work of Weisner[5] ,when he proposed single quantum states had to be used for information transmission. In 1989, Deutch published another paper "Quantum computational networks"[6]and proposed a new quantum idea that quantum gates can combine for quantum computation so that boolean gates could be achieved computation and so similarly quantum circuits also. The major advancement in theoretical quantum cryptography was considered to be happened in 1991 when Ekert suggested that Einstein-Podolsky-Rosen [7] two-particle state of entanglement could be used to establish quantum cryptography state

III. QUANTUM KEY DISTRIBUTION BASED COMMUNICATION LINK

The quantum key distribution based communication link(QKD Link) between the Alice and Bob can berepresented as the figure-1 below. The quantum channel is used for establishing a secure quantum cryptography based key transfer. The classical channel is used for the conventional data transfer between the devices by any medium like optic fiber cables or air. The quantum channel is used for sending the key between source and destination[8] by using the polarization of photons and corresponding bit values zero or one as the figure-2 represents.

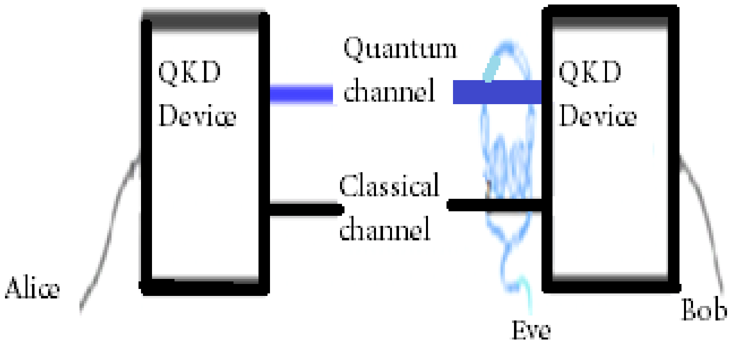

Figure -1 Quantum key distribution based communication

3.1 Quantum key distribution based data transfer

Alice and bob performs the quantum key distribution as per the below steps[8]

(i) Alice communicates with Bob through the quantum channel by sending the polarized photons.

(ii) Then both of them discuss results using a public channel

(iii) Then after receiving encryption key Bob can encrypt the messages and communicate through any public channel. If any attempt at eavesdropping will not only be unsuccessful but also an incorrect reading would destroy information and also Bob and Alice no longer would have the same key because of information already loss and eventually eavesdropper's presence could be known to both parties .

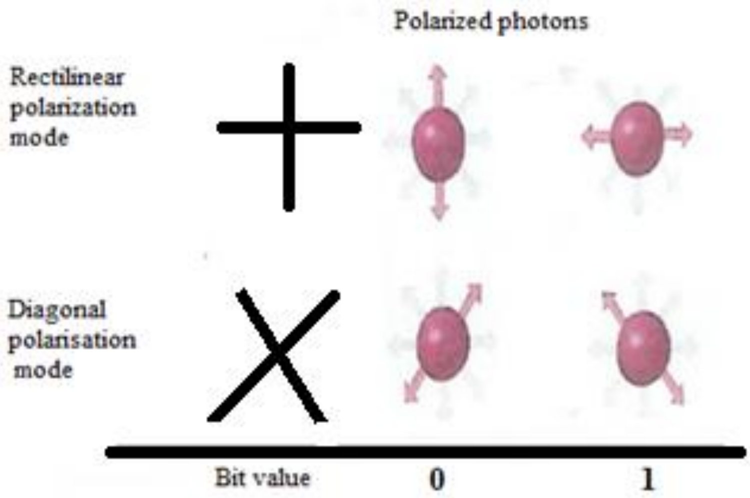

Figure-2 Polarized photons and corresponding bit values

IV. QUANTUM CRYPTOGRAPHY AND POSSIBILITIES OF COMMUNICATION OVER THE OCEAN SURFACE

(i)The QKD(Quantum Key Distribution) can be used for secure communication between ships to command center via satellite

(ii) The QKD can be used for communication between the command center to the aircraft from a remote location

(iii)The QKD between the ship to ship or aircraft is limited within the visible horizon due to QKD uses polarized photons for communication.

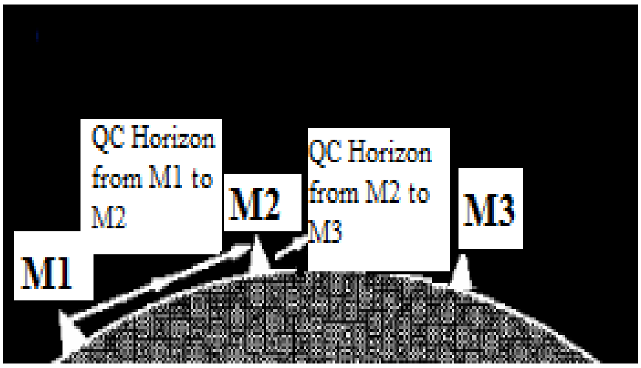

Figure-3 Quantum cryptography (QC) horizon from different points over earth surface M1 to M2 and M2 to M3

V. THE QUANTUM CRYPTOGRAPHY LINK HORIZON CALCULATION

The horizon or skyline is the apparent line that separates earth from sky, the line that divides all visible directions into two categories: those that intersect the earth's surface, and those that do not. At many locations, the true horizon is concealed by trees, tall buildings, mountains, etc. but it is clearly visible in ocean and the resulting intersection of earth and sky is termed as the visible horizon. Historically, the distance to the visible horizon has long been critical for the successful navigation at sea, because it determined an observer's maximum range of visibility[9] and similarly for Line of sight propagation of Quantum Key Distribution. This importance had been became less significant due to the development of the radio communication systems but today and future, the horizon calculation can become again significant due to the technology like Quantum

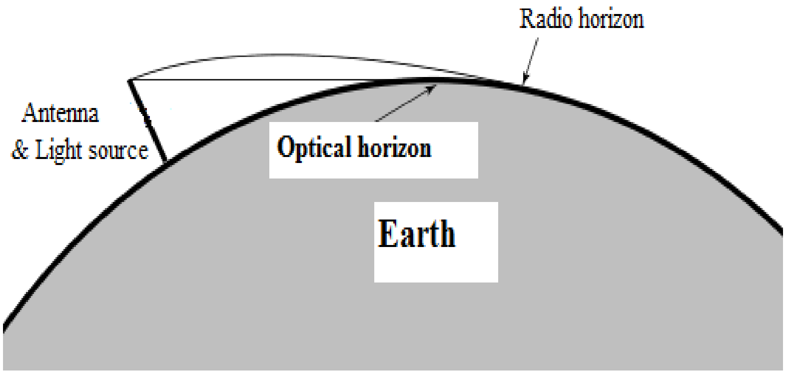

Figure -5 Optical and Radio horizon

Cryptography based communication.

The radio horizon is the locus of points at which direct rays from an antenna are tangential to the surface of the Earth. If the Earth was a perfect sphere and there was no atmosphere, the radio horizon would be a circle. The radio horizon of the transmitting and receiving antennas can be added together to increase the effective communication range. In astronomy the horizon is the horizontal plane of the observer. It is the fundamental plane of the horizontal coordinate system, the locus of points that have an altitude of zero degrees. While similar in ways to the geometrical horizon, in this context a horizon may be considered to be a plane in space .

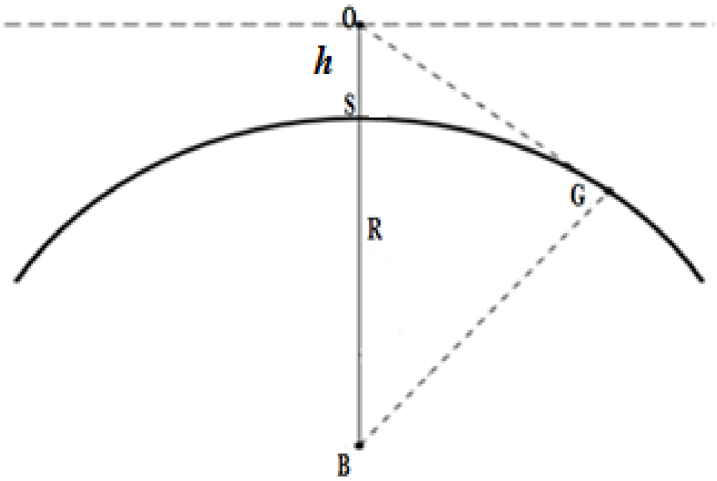

Figure-4 Geometrical horizon calculation

The horizon for QKD transmission can be calculated at a point 'O' to the point G by the Pythagorastheorem[10]

$(R + h)^2 = R^2 + BG^2$, Where BG=OG

So $(R + h)^2 = R^2 + OG^2$

So $OG^2 = (R + h)^2 - R^2$ expand term $(R + h)^2$ we get $R^2 + 2 R h + h^2$,

$OG^2 = (R^2 + 2 R h + h^2) - R^2$ so that

$OG^2 = 2 R h + h^2$ and we get

$OG = \sqrt[2]{(2Rh + h2}$.

when calculating earth horizon $h < R$, so that can neglect the second term h^2 .

So we get finally get the OG as $OG = \sqrt[2]{2Rh}$, using kilometers for d and R, and meters for h, and taking the radius of the Earth as 6371 km, the distance to the horizon is $\sqrt{(2 * 6371 * h)/1000}$ is approximately equal to $3.570\sqrt{h}$ is the equation

Examples, assuming no refraction:

i. For an observer on the ground with his eye level at h = 1.70 m, the horizon can be calculated by substituting in above equation and the answer is 4.655 km.

ii. For any observer standing on a hill top or a tower of 50 m in height, the horizon would be at a distance of 25.24 km

iii. For an observer standing over a mountain with 5000 m in height, the horizon will be at a distance of 252 km approximately.

iii. For a pilot, who flying in a plane at 10000 m, the horizon will be at a distance of 357 km with neglecting the effect of refraction of the light that passing through the air. Distance to horizon calculations gives an idea how far away an object that visible for the line of sight propagation. The refractive error on Earth's curved surface causes an error in geometric calculation. When any ground, water or surface is colder than the air above which cause a dense layer of air forms close to the surface and so light bends downward while traveling. The reverse phenomena happens when the ground is hotter than air above it, usually happening at desert environment.

VI. APPROXIMATE COMPENSATION FOR REFRACTIONIN QUATUM KEY DISTRIBUTION

The atmosphere bends light while travelling through the atmosphere due to the refraction of light but the rate of bending is unpredictable and never be a constant value. This is because of the variation of temperature and pressure in the atmosphere. So when measuring longer distances over the horizon in an ocean surface, increase R by the 15-20% from the calculated horizon value and ensure line of sight is at least 5 feet from the surface, for reducing random errors created by refraction.

To compute the maximum distance at which an observer can see the top of an object floating in ocean surface ,then add this height h for the calculation as $d = \sqrt{2Rh + h2}$

Where R is the radius of the Earth, where R and h must be in the same units. Consider an example, when a satellite revolving presently at a height of 1500 km, then distance to the horizon will be at 4372 kilometers .So the r random errors created by refraction can be calculated by increasing R by 20% of the value as follows

20% increase of 6371 km is 7645

$$\sqrt[2]{(2Rh + h2}$$.

$$\sqrt{((2 * 7645 * 1500) + 1500 * 1500)}$$

=5018.47km

VII. QUANTUM CRYPTOGRAPHY LINK HORIZON CALCULATION FOR A SATELLITE BASED QUANTUM KEY DISTRIBUTION DEVICES

The quantum cryptographic link between any naval vessels is limited by the line of sight propagation of photons. However it can be resolve by using the satellite nod between communication entities, but possibility is that each node must have to completely process polarized photons and have to establish a fresh quantum key distribution link between each nodeto node as per the law of quantum mechanics that polarization state of particles can measure only once without changing itsstate.

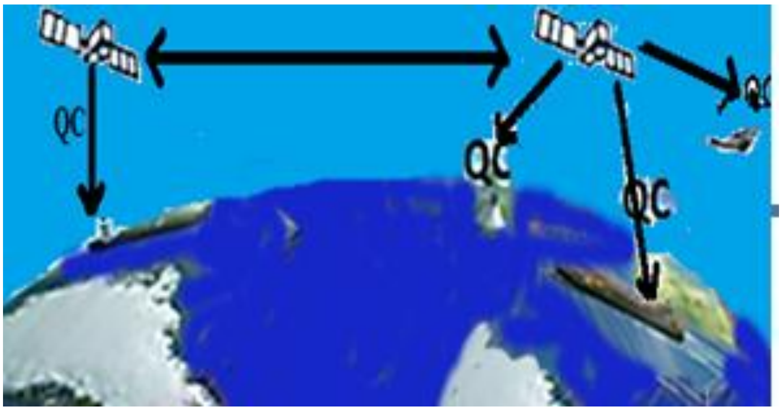

Figure-7 A method for beyond horizon Quantum key distribution, where QC is Quantum key distribution (QKD) links from satellite to ship, Satellite to aircraft, Command station to satellite. CC is commanding center

When height h is significant with respect to R for the case of most satellites, then the approximation of calculation for simplicity made previously will be no longer valid and so the exact formula is required,

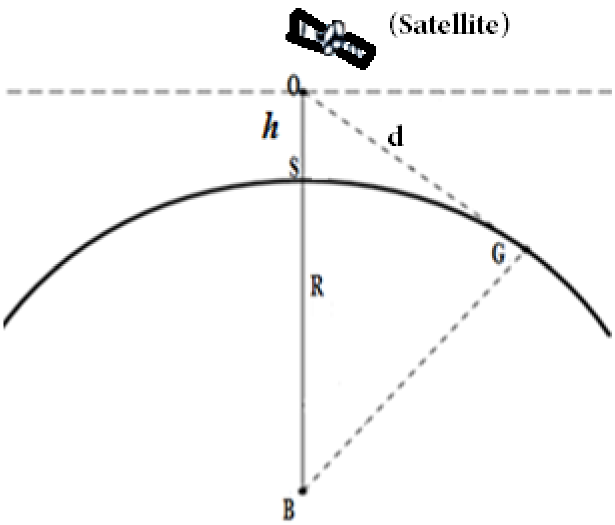

Figure-8

So that $d = \sqrt[2]{(2Rh + h2}$

where R is the radius of the Earth ,where R and h must be in the same units. Consider an example, when asatellite revolving presently at a height of 1000 km, then distance to the horizon will be at 4372 kilometers

.So the r random errors created by refraction can be compensated by increasing 20% R of the value, So horizon can be calculated as follows

20% increase (because of 'h' is large as 1500km) to the 6371 km is 7645km. So Horizon OG = $\sqrt[2]{(2Rh + h2}$

= $\sqrt{((2 * 7645 * 1000) + 1500 * 1500)}$

= 4188km

So 4188km is the horizon for a quantum key distribution link of a satellite revolving 1000km

VIII. THE QUANTUM CRYPTOGRAPHY (QC) LINK HORIZON CALCULATION FOR HAND HELD QUANTUM KEY DISTRIBUTION (QKD) DEVICES WHEN USING OVER NAVAL VESSELS

The initial success of achievement of reducing the size of components as well as higher key generation rates could be achieved while making the pocket size Quantum key distribution . That module will be an attractive add-on to conventional wireless methods. Such an integrated photonics platforms could enable secure communication with handheld devices such as smartphones. The work of Gwenaelle Vest, Markus Rau, Lukas Fuchs[11] presented a new design for a system where Alice(One user) owns a mobile Quantum key distribution unit, which allows her to perform secure free-space communication with any type of Quantum key distribution receiver (Bob). A secure key could be generated on demand and could be directly used for transactions or stored for future online authentication.

The height for finding horizon of handheld mobile devices (h) = The height of the person holding mobile QKD device(X) + Height of the platform person standing from sea level (H)

The equation (1) derived earlier can be transformed for the scenario as below

$3.570\sqrt{h}$,Where h is the height from sea level

Horizon OG =$3.570\sqrt{h}$, Where h = H + X . So that horizon when a person holding hand held Quantum key distribution device is

$3.570\sqrt{H + X}$

IX. THE OPERATIONAL RANGE OF QUANTUM CRYPTOGRAPHIC DEVICES WHEN USING ON THE DIFFERENT TYPE OF NAVAL VESSEL

9.1 Aircraft Carrier

Largest naval vessel type existing now is aircraft carrier. The height and width of aircraft carrier varies according to its class , but this type of ship can be as tall as 200 feet and 120 to 250 feet width[12]. The ships need to be wide to enable aircraft to take off and land, and they include space for storing and maintaining planes as well as housing a large crew. The maximumpossible height of any quantum cryptographic devices can be calculated by the feature of largest naval vessel existing now.

Figure 6- USS Theodore Roosevelt

Largest naval vessel type: Aircraft carrier [13]
Name: USS Theodore Roosevelt
Length :332.8MeterWidth : 76.8Meter, Which includes flight deck. TheUSS Theodore Roosevelt (CVN-71) was entered the service on 1986. It is the fourth in US Navy's Nimitz class of nuclear powered aircraft carriers and has a maximum speed of more than 34 miles per hour and can remain at sea for up to 25 years. It cost around $4.5billion.The horizon of quantum cryptographic link possible of this largest naval vessel(aircraft carrier) is equal to $3.570\sqrt{h}$,Where h is the height of the aircraft carrier from sea-level and Aircraft carrier usually as tall as 200 feet with the width of 120 to 250 feet .We know that 200ft approximately equals 60.96 Meters, so the answer is

$3.570\sqrt{60.96}$= 27.88 Kilometer (KM)
Area of a Circle $= \pi r^2$
So the operational circular area of a Quantum Key Distribution devices around aircraft carrier can be calculated as

=3.14*$(27.88)^2$
=2440.70 Km^2

9.2 Small Category Naval Vessels
Consider that, usually this type of vessels can be categorized as tall as up to 50feet,we can calculate that 50 Feet approximately equals615.24 Meters, so the Line of Sight is

$3.570\sqrt{\mathbf{15.24}}$

= 14 Kilometer(KM)

Figure -7 Small Naval Ship

So the operational circular area of a Quantum Key Distribution devices around a small naval vessel up to 50 Feet height can be calculated as
Area of a Circle $= \pi r^2$
= 3.14*$(14)^2$
= 615 Km^2
9.3 Experimental Verification of Line of Sight of a vertically polarized Light while using in a small Ocean vessel
We have experimentally tested Line of sight of a vertically polarized beam using a LASER light and a vertical polarser using an Ocean vessel with height of 10 Feet approximately equals 3 .048 Meters, as

$3.570\sqrt{\mathbf{3.048}}$ **= 6.23** Kilometer(KM)
Area of a Circle $= \pi r^2$
So the operational circular area of a Quantum Key Distribution devices around a small naval vessel up to 20 Feet height can be calculated by equation

=3.14*$(6.23)^2$
$^=$121Km^2
The variation of Line of Sight of both Measurementon table below can be attributed to the height variation due to tidal waves and Refraction of Light
(Table 1-Calculation of Line of Sight by Equation and by LASER experiment)

Theoretically calculated Line of Sight of a Vertically Polarized Laser Light in a 10 Feet Height Small Naval Vessel using equation	Experimentally Obtained Line of Sight of Vertically Polarized Laser Light in a 10 Feet Height Small Naval Vessel (Average of 5 times Measurement)
6.23 Kilometer	**6.54 Kilometers**

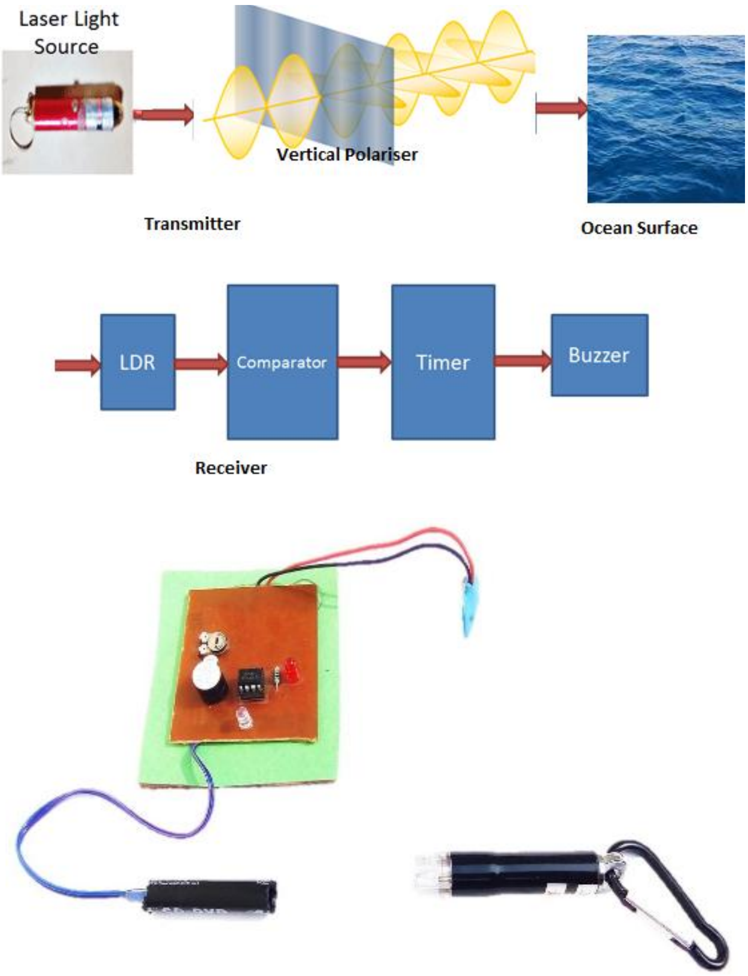

Figure 8 -LDR Based Vertical PolarizedLaser Beam Detection System over Ocean surface

REFERENCE

[1]. Marie A. wreight "The Impact of Quantum Computing on Cryptography" Network Security Volume 2000,Issue 9,p 13-15,2000

[2]. Diffie W and Hellman L,"New Directions in Cryptography", IEEE Transac on Information Theory, No. 6 ,1976.

[3]. Richard P Feynman, "Simulating physics with computers" , International journal of theoretical physics ,Volume 21 , Nos 6/7 , pp.467-488,1982

[4]. David Deutsch "Quantum theory, the Church-Turing principle and the universal quantum computer", Proceedings of the Royal Society of London A 400, pp 97-117 , 1985.

[5]. S J Weisner:1983, "Conjugate coding",SIGACT News 15:1 , pp.78-88 , 1983

[6]. D. Deutsch, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, Vol. 425, No. 1868 , pp. 73-90, Sep. 8, 1989

[7]. Ekert A.K., ''Quantum cryptography based on Bell's theorem'' , Phys. Rev. Lett. 67, 661–663, 1991.

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

[9]. David.K..Lynch, "Visually discerning the curvature of the Earth", December 2008, Vol.47, No.34 ,pp.42

[10]. A. P. French, "How far away is the horizon?" American. J. Phys. Vol. 50, pp.795–799 ,1982.

[11]. GwenaelleVest, Markus Rau, Lukas Fuchs, "Design and Evaluation of a Handheld Quantum Key Distribution Sender module", IEEE journal of selected topics in quantum electronics, VOL. 21, No.3, May/June 2015.
[12]. American fighting ships of the 20th century, New York : Mallard Press, 1991
[13]. List of longest ships. Available:https://en.wikipedia.org/wiki/List_of_longest_ships

Sureshkumar P H: Presently working as Assistant professor of Computer Science in the Department of Computer science, Saint Philomena's college (Autonomous), Mysore, Karnataka, India. He was doing his doctoral program in Quantum cryptography at Bharathiar University, Coimbatore. His educational qualification includes Bachelor in Electronics, Master of Science degree in Computer Application,Master of Technology degree in Advanced Information Technology and interested in research of areas in Quantum Information Science, Cryptography, Wireless communication, Embedded Systems . He has published 06 papers in various Journals and Conferences.

. 

Dr Rajesh R: Presently working as Professor of Computer Science in the Department of Computer Applications, SreeNarayanaGurukulam College of Engineering, Kadayiruppu post, Kerala, India. He was also worked in Ministry of Education, Government of Ethiopia around two and a half years. His educational qualification includes Master degree in Computer Applications, Master degree in Personnel Management and Ph.D. in Computer Science. Currently seven research scholars are pursuing Ph.D. under his guidance. Dr.Rajesh R research interests are in the areas of Data Structures and Analysis of Algorithms. He has organized many national and international conferences jointly with Government bodies and universities. He has published 24 papers in various Journals and Conferences. Dr. Rajesh R is also serving as Managing Editor, Lead Guest Editor, Associate Editor, Editorial board member and Technical Committee member of various National and International Conferences and Journals. He has received RashtriyaGaurav Award, Best Citizen award and Veenus International Foundation's Outstanding Faculty award to his credit.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

sureshkumar P H "The Quantum Key Distribution Devices and Horizon Calculation Over Ocean Surface for Application in Various Naval Vessels." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 5, 2018, pp. 15-23.