PARTICLE MAGIC: NEED FOR QUANTUM CRYPTOGRAPHY RESEARCH IN THE SOUTH ASIAN REGION

Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

ABSTRACT

Securing sensitive and important information from intruders is a tedious task in the 21st century. In order to protect information different ciphering techniques has been used. Quantum Cryptography has taken a new path in the field of crypto systems where all the presently used crypto systems are classified as classical cryptography systems. Classical cryptography systems use mathematical formulas where quantum cryptography uses the principles of photon polarization and heisenberg uncertainty principle. As the south asian region is developing rapidly in almost all the sectorsthe need of securing information has become a difficult task. Therefore, the need of starting extensive research on quantum cryptography for the south asian region to safeguard information from intruders has been the purpose of this study. Comparative study of the growth of the telecommunication sector in the south asian region and how quantum cryptography could assist in securing information has been discussedas results.In the end, details of the need to research on quantum cryptography in the south asian region to overcome future predicted cyber threats are also discussed.

KEYWORDS

Quantum Cryptography, Classical Cryptography, South Asia

1. INTRODUCTION

From as far as the written history is concerned mankind has been involved in sending different messages across families, states, as well as countries for different purposes. The messages could be classified into different categories. Exchange of family information and warfare information were the main two types involved. The transport medium was with the assistance of birds or through human message's. Mostly these messages were written in plain text. Before long these messages were intercepted by rivalry which was a major disadvantage when coming to warfare. From the above mentioned history to the present, interception can be seen. However, the medium of receive/ transmission and method of intercepting has been changed from time to time. As a solution to the above mentioned issue different cryptography methods were introduced. Figure 01, illustrates how a plain text from a sender is intended to be sent to the receiver. ATBASH, Scytale, Polybius Square, Caesar, Changing keys, Wheel, Playfair were some of the ancient ciphering methods used [1] [2]. A leap from ancient cryptology happened after the World War I when Germany developed a ciphering machine named as "Enigma" [2]. However, Enigma and other similar cipher systems such as "Stepping Switch" systems were exploited during World War II and new ciphering techniques were on research till 1976 where Data Encryption Standard (DES) was introduced [1] [3].

DOI : 10.5121/ijaia.2015.6507

DES uses two different keys in communication. Those are public and private keys. The algorithm distinct different means of communication. As figure 02, explains the public key exploitation does not reveal the encrypted message till the private key is not known to the attacker [1] [3]. DES is commonly categorized as a symmetric encryption technique where the sender and the receiver share a key for encryption as well as decryption [4]. It contained a 56-bit key length where by 1999 was too small to be cracked within 23 hours in a distributed net project using an exhaustive key search method [5]. As it was exploited DES was removed as the ciphering method for National Security Systems. However, DES is still used presently as a component for the Triple Data Encryption Algorithm (3DES/TDEA) which came as a replacement for DES.

The system has been illustrated through figure 03. 3DES is also a symmetric encryption technique where a number of three DES keys are used instead of one DES key. A combination of three 56-bit key lengths gave a total of 168-bit key which was more secure than DES. However, as 3DES is a symmetric system where the same key is shared between the source and the destination as well as the weightage of the key made the cipher system more vulnerable as well as too slow in performance [4]. As a solution Advanced Encryption Standard (AES) was introduced.

AES is also a symmetric cipher technology with key values of 128, 192, and 256 bits. Functionality of AES system has been illustrated through figure 04. The main disadvantage of AES is the common issue faced by symmetric encryption where the same key is used for encryption as well as decryption. However, with the use of four main processing methods used in AES, which are 1) SubByte; 2) ShiftRows; 3) MixColumns; and 4) AddRoundkey secures the key which is better than other symmetric techniques [6]. A better solution than symmetric systems were researched where asymmetric encryption systems were built. Asymmetric encryption systems such as Rivest-Shamir-Adleman (RSA) eliminates the shared key exchange issue by using different encryption and decryption keys [7].

RSA is a cryptosystem where the source of the data uses the receiver's public key to encrypt the data where it is only possible for the specific receiver to decrypt using the private key where RSA uses block cipher encryption. It uses two large prime numbers being multiplied as and converts to 0s and 1s which are usable keys that cannot be factored in reasonable time [8] [9]. This is the widely used cryptosystem in web browsers, email programmes, mobile phones, virtual private networks, and secure shell [9]. However, with the introduction of the cryptanalysis which reveals, or to attempt to reveal cipher text into the original message. It assesses the vulnerability of cryptosystems such as RSA. The revealing of the original message is to factor the large prime number to get the private decryption key and the public encryption key. The cryptanalysis to crack the above mentioned keys combines a mathematical, brute-force, and implementation attack [8]. However, due to the factor of implementation of faster computers, supercomputers, and quantum computers enable to factor cipher text into associated prime numbers of the original message which has been discussed in [10]. Furthermore, there is a possibility for an eavesdropper to keep a copy/clone the captured packet for future decryption of the cipher text as well as there would be no trace or warning that indicates the mentioned anomaly. In the early 1970s, a new cryptography named Quantum Cryptography (QC) was recommended and in the year 1984 the first QC protocol named "BB84" was introduced [10].

QC is based on quantum physics where the encryption and decryption happens through quantum state of light which is the closes mankind has reached in the law of nature. As a fundamental theory is concerned QC is based on two elements which are the Heisenberg Uncertainty principle and the principle of photon polarization [10]. Presently, this technology is researched widely around the world as QC is a non-clonable technology first presented by WoottersAndzurek in 1982 [11]. Furthermore, through figure 06 Quantum Key distribution (QKD) has been illustrated which explains that QC is different than conventional/classical cryptography. QC was first

implemented for fibre optics where in 2004 two Austrian banks with the distance of 500m in road system, but 1.5 km of fibrelaid in a sewage system has been linked was the first transaction of money transfer without interruption [10]. In the same paper, it discusses the QC operation in free space in Vienna in the year 2003.

Through this paper the author has concentrated on why QC is important to South Asian Countries. Prior to the above mentioned purpose the author would highlight the importance of the growth of telecommunication services in the South Asian Region. The growth has been determined by comparing the growth of broadband subscription services in the years of 2012 and 2013 with the assistance of censor statistics of three South Asian Countries. The subscription has grown as shown; Sri-Lanka 47.3%; India 40.2%; Pakistan 26.5% [12] [13] [14]. It has been illustrated through figure 07, 08, and 09.

The analyzed statistic indicated above states an increase of a number of individuals connected to the World Wide Web. The number comprises governmental, private as well as individual connections. Online connectivity has enabled reachability to different services offered by large to mid/small size institutes which comprises financial, educational, telecommunication, airlines and more. Critical information would be transferred using different service providers in the South Asian region in the above mentioned services. It explains that more the accessibility to the outside through serviceproviders, carries more risk of exploitation. Exploitation of information can result a downfall of not only an institute, but as well as a country. Therefore, almost all the organizations in the region should be using a crypto system to encrypt and decrypt sensitive information. Mostly Symmetric and Asymmetric cryptography systems would be widely used. Through the mentioned explanation classifies the issues with symmetric and asymmetric systems which were described earlier in this paper. The author considers sharing keys or mathematical algorithms would not be secure systems as the processing power of the ordinary computers would be growing each year which results an increase of exploitation year by year. Therefore, the author suggests Quantum Cryptography a better replacement to the conventional crypto systems. At the same time the author explains the need of research for QC for the South Asian Region which would be discussed extensively in the upcoming sections.

2. QUANTUM CRYPTOGRAPHY IMPLEMENTATION

The need for Information and Communication Technology (ICT) has rapidly developed from early 1970s' to present where the concept Anything, Anytime, Anywhere has taken a toll on day to day lives of a human being. Any information can be accessed at any time of the day across the globe with just an internet connection. Organizations require employees to be productive by giving access to critical information at the work place, on the go through mobile applications or at home. At the same time organizations invest in keeping the information secure as possible from intruders through the assistance of different vendor products, following different standards and giving permission to different users inside the organization as well as for outside users. The most popular method of securing information is through a system named as cryptography. It is where information is encrypted when transmitting and decrypted when receiving. Widely used crypto systems uses an algorithm that comprises mathematical formulation. However, latest development, such as cryptanalysis has indicated the vulnerability of widely used crypto systems by cracking encryption and decryption. This vulnerability has been addressed by researchers where in early 1980s' Quantum Cryptography was introduced which is based on natural laws of photons.

2.1 Conventional Cryptography and its limitations

Conventional Cryptography comprises two different key algorithms. Those are Symmetric and Asymmetric key algorithms. Symmetric key algorithms such as Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DES/TDEA), and Advance Encryption Standard (AES) uses the same key to encrypt as well to decrypt information where RSA (Ron **R**ivest, Adi**S**hamir and Leonard **A**dleman) uses different keys to encrypt as well as to decrypt information. This key generation is a product of prime factorization. Longer the key generation better secured. However, longer the key, slower the system operates in data communication as the processing unit of the device needs to utilize the processing power immensely for the encryption and decryption process. The development of faster machines and quantum computation has enabled the keys to be cracked faster than legacy computers. Specifically, man in the middle attacks could be dangerous in transmitting critical information. A person located center of the communication pathway between the source and the destination can obtain original information and can keep a copy for later use and send the original to the destination. The difficulty faced by most of the network administrators is that there are no information received whether the data was intercepted in the middle or not.

In 1984 Quantum Cryptography was introduced with BB84 which was beyond classical encryption and decryption methods. It used the source of light to operate in a linear and circular polarization where a middle person tries to intercept the light particle will be destroyed where a notification of particles not reaching the destination has been sent. At the point of interception data will stop transporting where the middle person would not receive any further information.

2.2 Theoretical overview of Quantum Cryptography

Quantum cryptography is based on quantum mechanism. When QC was first introduced it was researched on optical fibre where discrete particles named as photons were used for the crypto system. In QC encryption Heisenberg uncertainty principle is a measurement which states that a photon in transmission cannot be measured. If tried the photon would be destroyed. Photon polarization is also a principle used in QC. It explains the direction of electromagnetic field associated with its wave. There are four different polarization states. 0-bit can be represented through a horizontal state which states -45^0 and 1-bit through vertical state of $+45^0$. It has been illustrated through figure 10. A single photon is called Quantum Bits or QBITS.

However, QC would also distribute keys from the source to the destination. The difference between the distribution in classical cryptography and QC is that QC uses a separate channel to distribute quantum keys which are called Quantum Key Distribution (QKD). Using the quantum channel a large number of photons are sent across from the source to the destination which are recorded based on the orientation pattern the destination was able to record. Afterwards, the filtered orientation will be sent across in the classical channel which is through the normal data distribution channel without disclosing the actual results. Emitter located in the source compares the sent orientation from the destination with the actual sent. Then the emitter sends the mismatching orientation to the destination where the mismatch is discarded from both source and the destination. This phase is called shifting of the key.

2.3 The importance of Quantum Cryptography in the real world

As mentioned in the section 2.2, before transmitting information QKD is exchanged to verify the agreed key combination. The advantage of QC over classical cryptography is that QC firstly a different medium of key distribution which is involved with photons, secondly by using a separate channel named as Quantum channel to distribute a large number of photons, and thirdly

the mismatching orientation would be discarded without the actual results not been shared by the receiver.

Through the above mentioned processors an eavesdropper would have a difficulty in identifying the real key distribution. If any case an eavesdropper is present in the middle firstly source and the destination which shared the orientation would not be the real one that the eavesdropper has, secondly due to the reason of mismatch orientation been discarded the real key distribution or the discarded orientation would not be accurate to the eavesdropper where statistically it is a 50-50 chance of getting it correct and thirdly if the eavesdropper does any change to figure out the correct key orientation photons would be destroyed where alerts would raise of destroyed photons.

The advantages mentioned above displays an error free communication along with more security and monitoring capabilities been involved which cannot be seen in classical cryptography.

2.4Varieties of services offered and latest implementation of Quantum Cryptography

As mentioned in section 1.0, two Austrian banks were involved in transferring the first money transaction while the same paper discusses open air transmission in Vienna. In Switzerland turnkey services in quantum cryptography has been commercialized [16]. Furthermore, quantum cryptography implementation in wireless networks has been discussed through a protocol named as SARG04 [17]. In SARG04 a different 4-way handshake has discussed over 4-way handshake which is standardized by IEEE through 802.11. In the year 2004 Cambridge, Massachusetts became the first quantum cryptography network that is up and running while Chip Elliott of BBN Technologies in Cambridge sent the first data across the Quantum Net [10].
There are some modifications such as detecting errors, anomalies using cryptanalysis which is theoretically researched which needs to be experimentally researched. However, it is the latest generation of cryptography with wireless and optical fibre experiments and deployments happening throughout the world. Mobile QC is yet to be researched.

2.5 Need of Quantum Cryptography to the South Asian region

The South Asian region has a number of developing countries where a lot of financial activities along with a number of cyber threats increasing which is a major threat to the development of the region. According to the Federal Bureau of Investigation: Internet Crime Complaint Centre's 2014 report, India is placed 04th while Pakistan is placed 17th in complaint statistics by country [15]. Furthermore, Colombo, Sri Lanka has been ranked first as the fastest growing cities in the world [18].

The stated statistics indicated above as well as in section 1.0 which states the growth of telecommunication services in the region makes the region more depended on Information Technology with the concept of Internet of Things. Along with it brings more exploitation on sensitive information which effects from the stock markets of the countries, defense systems of the countries to day to day activities with the association of Internet. Different anomalies such as scanning, enumeration, phishing, escalating privileges, Denial of service attacks (DOS), unauthorized access to the local super user (U2SU), and Unauthorized access from a remote machine (R2L) would be increasing significantly. Furthermore, terrorist activities are not as field war any longer. It is a cyber-war. As described South Asian is rising in collaborating cybercrimes by terrorist and extremist for the international movement of money, smuggling arms, and illegal drugs [19].

Therefore, with the analysis stated above the author would recommend in starting quantum cryptography research sooner than later in South Asian region. Furthermore, the author considers latest cryptography needs to be improved to mitigate and overcome cyber threats and anomalies.

3. CONCLUSION

Cryptography has become more advanced and more secure with Quantum Cryptography without being depended on mathematical formulas and to protect the algorithms created being cracked by intruders. South Asia is a vastly developing region with vast telecommunication subscription base along with a large transaction base accumulating in day to day basis in almost all the sectors. With it comes disruption of compromising sensitive information. In this paper the author has discussed not only the technical details of Quantum Cryptography, but also a widespread implementations that have been executed in the real world except mobile communication. Along with it the author has stated combined Quantum Cryptography and South Asian Region through the need of starting research on Quantum Cryptography in South Asian Regions to overcome future predicted cyber threats.

ACKNOWLEDGEMENT

My sincere thanks goes to the staff members of Sri Lanka Institute of Information Technology Computing (Pvt) Ltd as well as all the authors whom I have referred in this research paper. Without their contribution to the field would have not been possible to be successful in this research.

REFERENCES

[1] Saini, N., Mandal, S., “Review Paper on Cryptography”, International Journal of Research, May 2015, pp. 45-49.

[2] Cohen, F.B., “Introductory Information Protection” Fred Cohen and Associates, 1995 <Available - http://all.net/books/IP/Chap2-1.html > [Access 06th June 2015].

[3] Diffie, W., Hellman, M., “New Direction in cryptography”, IEEE Transaction on Information Technology, November 1976, pp. 644-654.

[4] Karthil, S., Muruganandam, A., “Data Encryption and Decryption by using Triple DES and performance analysis of crypto system”, International Journal of Scientific Engineering and Research, November 2014, pp. 24-31.

[5] Kenekayoro, P.T, “The data encryption standard thirty four years later: An overview” African Journal of Mathematics and Computer Science Research, October 2010, pp. 267-269.

[6] Fadul, I.M.A., Ahmed T.M.H., “Enhanced Security of Rijndael Algorithm using Two Secret Keys”, International Journal of Security and its applications, July 2013, pp. 127-134.

[7] Pahal, R., Kumar, V., “Efficient Implementation of AES”, International Journal of Advanced Research in Computer Science and Software Enginnering, July 2013, pp. 290-295.

[8] Abubakar, A., Jabaka, S., Tijjani, B.I., Zeki, H.C., Usman, M.J., Raji, S., Mahmud, M., “Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA] cryptosystem: Issues and Challenges”, Journal of Theoretical and Applied Information Technology, March 2014, pp. 37-43.

[9] Kota, C.M., Aissi, C., “Implementation of RSA algorithm and its cryptanalysis”, Proceedings of ASEE Gulf-Southwest Annual Conference, March 2002.

[10] Kilor, P.P, Som, P.D., “Quantum Cryptography: Realizing next generation information security”, International Journal of Application or Innovation in Engineering and Management, February 2014, pp. 286-289.

[11] Sharma, R.D., “Quantum Cryptography: A New Approach to Information Security”, International Journal of Power System Operation and Energy Management, 2011, pp. 11-13.

[12] Central Bank of Sri Lanka, “Economic and Social Statistics of Sri Lanka 2014”, Central Bank of Sri Lanka Statistics Department, April 2014, pp. 160.

[13] Baruah, P., Baruah, R., “Telecom Sector in India: Past, Present and Future”, International Journal of Humanities and Social Science Studies, November 2014, pp. 147-156.

[14] Pakistan Telecommunication Authority, “Annual Report 2014”, 2014 pp. 51.

[15] Federal Bureau of Investigation: Internet Crime Complaint Centre, "2014 Internet Crime Report", Federal Bureau of Investigation, May 2014, pp. 22.
[16] Reddy, M.I.S., Reddy, K.S., Reddy, M.P., Bhat, P.J., Rajeev, "Key Distillation Process on Quantum Cryptography Protocols in Network Security", International Journal of Advanced Research in Computer Science and Software Engineering, June 2012, pp. 12-24.
[17] Ahmed, J., Garg, A.K., Singh, M., Bansal, S., Amir, M., "Quantum Cryptography Implementation in Wireless Network", International Journal of Science and Research, April 2014, pp. 129-133.
[18] Hedrick-Wong, Y., Choong, D., "Master Card: 2015 Global Destination Cities Index", MasterCard Worldwide Insights, 2015, pp. 02.
[19] Rollins, J., Wilson, C., "Terrorist Capabilities for Cyberattack: Overview and Policy Issues", CRS Report for Congress, January 2007.

Author

I am a Lecturer / Network Engineer with over 08 years of hands on experience who worked for Millennium Information Technologies, a subsidiary of the London Stock Exchange as well as a lecturer in SLIIT Computing (Pvt) Ltd which is a leading private university in Sri Lanka. I have been involved in many critical projects primarily in Sri Lanka, United Kingdom, and the Maldives. I have also acquired a bachelors and a masters degree with a number of professional examinations as well as being a Toastmaster with Competent Communication Status.

APPENDIX

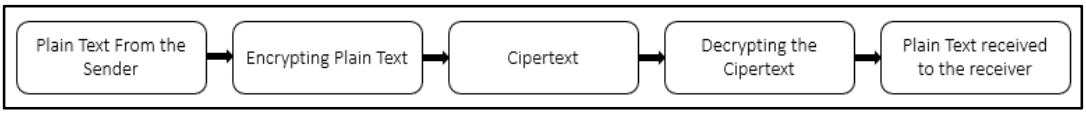

Figure 01: Process involved in encryption and decryption

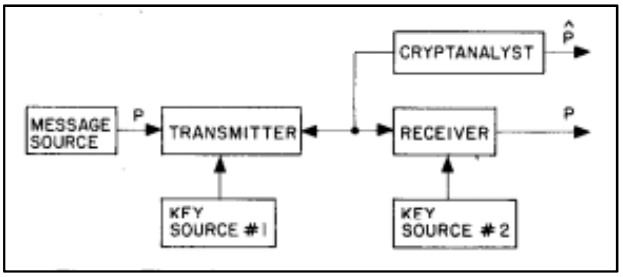

Figure 02: Public key involvement in DES
(Source: http://www-ee.stanford.edu/~hellman/publications/24.pdf)

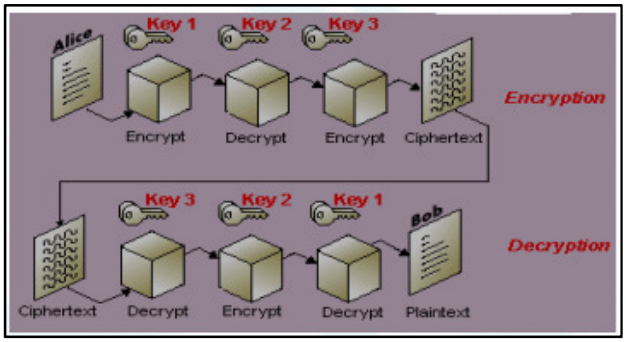

Figure 03: 3DES System

(Source: http://www.ijser.in/archives/v2i11/SjIwMTM0MDM=.pdf)

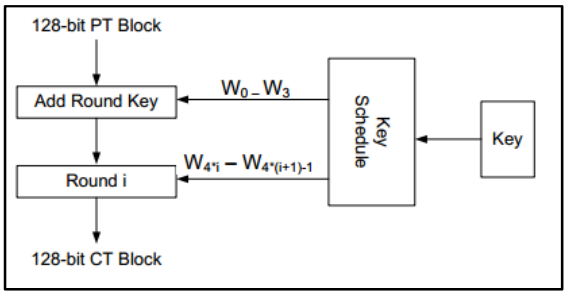

Figure 04: AES System
(Source: http://arxiv.org/ftp/arxiv/papers/1307/1307.3057.pdf)

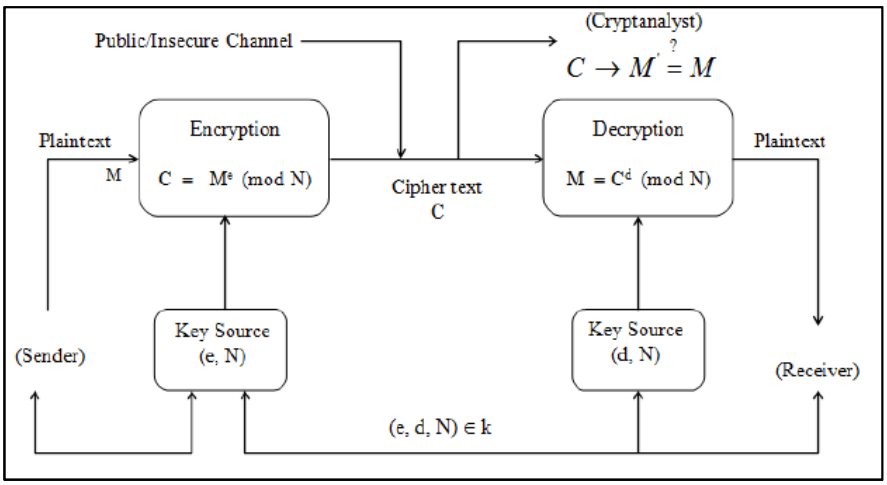

Figure 05: RSA Cryptosystem
(Source: http://www.jatit.org/volumes/Vol61No1/5Vol61No1.pdf)

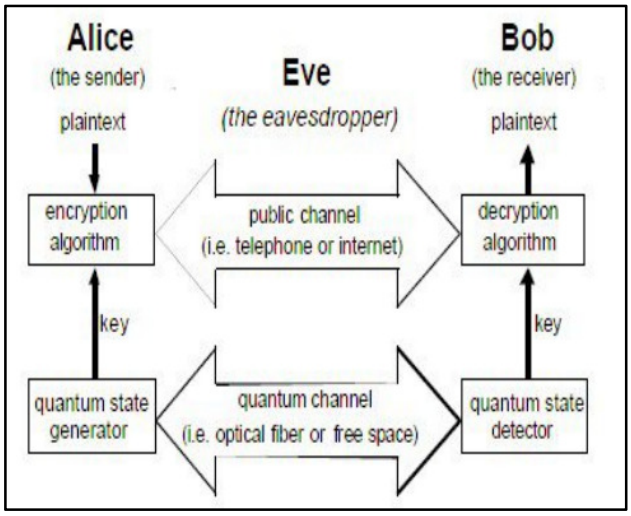

Figure 06: Quantum Cryptography Operation
(Source: http://www.interscience.in/IJPSOEM_Vol1Iss1/paper3.pdf)

SOCIO-ECONOMIC SERVICES **Table 13.27**

Telecommunication Services 2004 – 2013

Item	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013(a)
Fixed Access Services										
Subcriber Base ('000)	991	1,244	1,884	2,742	3,446	3,436	3,535	3,608	3,449	2,707
Wireline Services ('000)	860	919	910	932	934	872	897	942	999	1,062
Wireless Access Services ('000)	131	325	974	1,810	2,513	2,564	2,638	2,667	2,450(b)	1,645(c)
Growth Rate of the Subscribers	6.1	25.5	51.4	45.5	25.7	-0.3	2.9	2.1	-4.4	-21.5
Telephone Density (d)										
(Telephones per 100 persons)	5.1	6.3	9.5	13.7	17.1	16.8	17.1	17.3	17.0	13.2
Turnover (d) (Rs. Mn.)	31.9	49.3	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Other Services										
Cellular Phones ('000)	2,211	3,362	5,412	7,983	11,083	14,264	17,267	18,319	20,324	20,315(c)
Turnover of Cellular Operators (Rs. Mn.)	53	26	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Cellular Mobiles per 100 Persons	15	17	27	40	55	70	84	88	100	99
Public Pay Phone Booths	6,095	6,285	7,561	8,526	7,417	7,378	6,958	6,458	6,983	6,788
Radio Paging Subscribers	828	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Internet Connections (e)	93,300	115,000	130,000	202,348	234,000	240,000	502,000	844,749	1,365,655	2,011,600

(a) Provisional
(b) Wireless Local Loop telephones declined in 2012 due the rectification of statistical reportings subsequent to the merger of two companies.
(c) Wireless Local Loop telephones and Cellular phones declined in 2013 due to a revision in the classification of active subscribers in January 2013.
(d) Include Wireline Services and Wireless Services only
(e) Includes mobile internet connections from 2010 onwards
n.a. – Not available

Sources : Telecommunications Regulatory Commission of Sri Lanka
Central Bank of Sri Lanka

Figure 07: Sri Lankan Telecommunication Services of Years 2004 – 2013
(Source: http://www.cbsl.gov.lk/pics_n_docs/10_pub/_docs/statistics/other/econ_&_ss_2014_e.pdf)

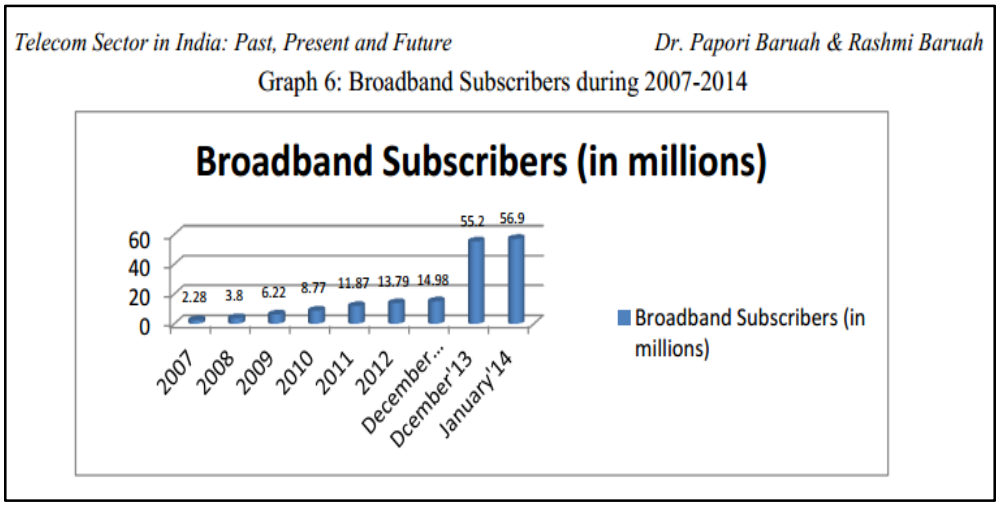

Figure 08: Indian Telecommunication Services 2007 – 2014
(Source: http://www.ijhsss.com/files/RASHMI-BARUAH.pdf)

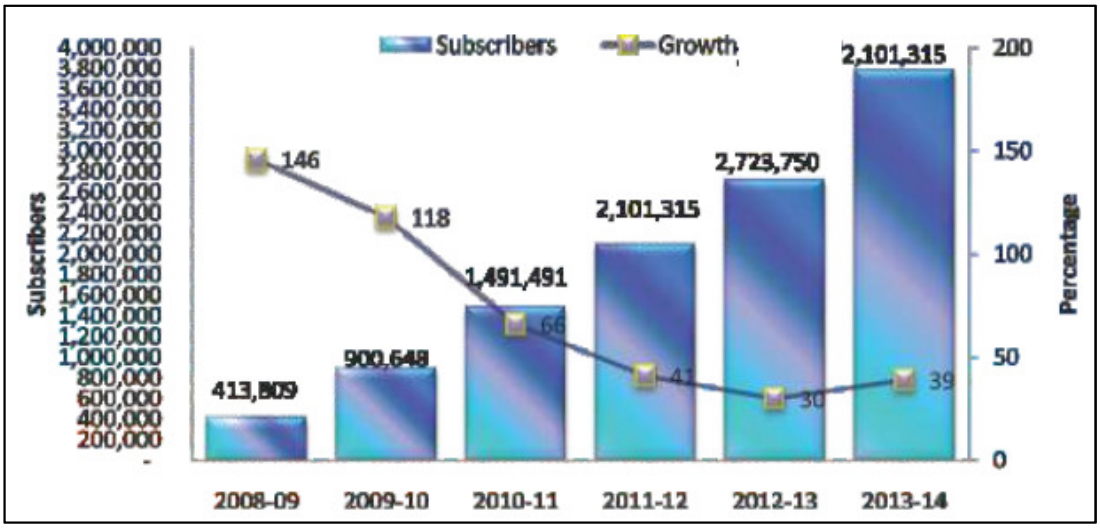

Figure 09: Pakistan Telecommunication Services 2008 – 2013
(Source: http://www.pta.gov.pk/annual-reports/ptaannrep2013-14.pdf)

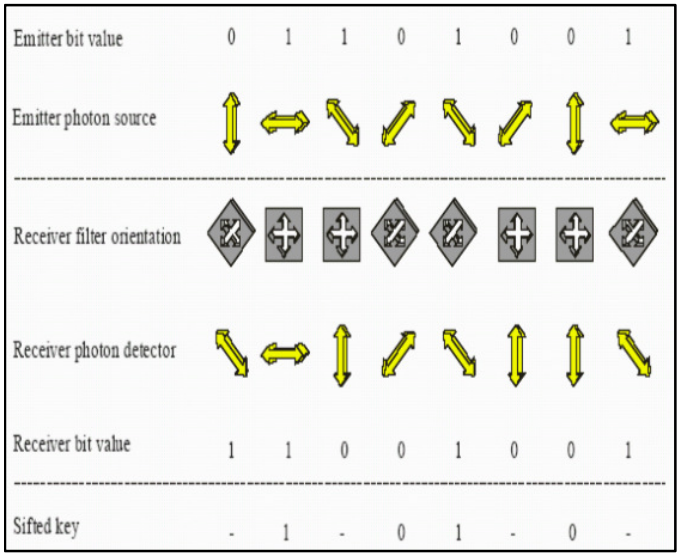

Figure 10: Photon Polarization states
(Source: http://www.ijarcsse.com/docs/papers/June2012/Volume_2_issue_6/V2I600121.pdf)