Distributed Protocol Using Quantum Cryptography for Secure Communication in Ad Hoc Networks

[1]Rajaram Jatothu,[2]Dr. R P Singh

[1]Research Scholar, 2 Research Guide
[1]SSSUTMS, Sehore, India, [2]SSSUTMS, Sehore, India

***Abstract*— In this work discussed about how quantum network can be combined with modern cryptographic technologies in fiber network and with emerging mobile terminals in wireless network, creating new solutions for the future cryptographic and communication systems. Cryptography can provide authentication and Validation of data. Cryptography is expected to play an important role in assuring the integrity of transactions in a society where the rights and obligations of persons are handled by information and communications systems.**

***IndexTerms*— Cryptographic, Quantum security, Quantum key dissemination, Distributed Protocol**

I. INTRODUCTION

More interestingly, the quantum channel achieves one of the main advantages of public-key cryptography by permitting secure distribution of random key information between two parties who share no secret information initially, provided both parties have access, beside the quantum channel, to an ordinary channel susceptible to passive eavesdropping, but not to active tampering. Even in the presence of active tampering, the two parties can still distribute a key securely if they share some much shorter secret information initially, provided the tampering is not so frequent as to suppress communications completely. These key distribution and key expansion schemes remain secure even if the enemy has unlimited computing power. Recall that it is a theorem that this is impossible to achieve for mathematically based schemes. The purpose of quantum cryptography is to propose a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics. Quantum cryptography can achieve the benefits of public-key cryptography, with the additional advantage of being provably secure, even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws. It can be roundly asserted that any successful attack on some of our schemes would have more far reaching consequences on contemporary physics than an efficient factoring algorithm, or even a proof that P=NP (sic), would have on mathematics and computer science. Cryptography remains a fascinating topic of discussion. Cryptography is expected to play an important role in assuring the integrity of transactions in a society where the rights and obligations of persons are handled by information and communications systems.

Quantum keys must be stored safely or they are not effective. No means for ensuring total security have yet been found. In theory, quantum entanglement has been proposed as a solution. This is a method that could use pairs of photons generated at the same time, where one photon is not read until the key is needed, thus ensuring that the other photon, which was used to generate the key, had not been tampered with. Unfortunately, no method of storing photons has been found where quantum states can be preserved for more than a fraction of a second. In summary, quantum techniques should meet the encryption needs of users, perhaps indefinitely. It is uncertain if or when someone will discover a fast way to factor large numbers. It is equally important to look at the human weaknesses inherent in any system and try to eliminate them as much as possible.

The ultimate goals in a few decades is to realise quantum safe infrastructure in fibre and wireless networks, in which post-quantum cryptography, QKD and physical layer cryptography will be integrated. In the age of rapid growth of digital data storage and communication, cryptography plays an integral role in our society. It is a challenge to respect the serious concerns of information and data security in the internet and electronic communication. In this article security issues involving data and information has been highlighted and what cryptography is, how it work and some of its application have also been shown in terms of securing information.

Furthermore, the book cannot be put back to the way it was. Now the book is of no use to the recipient, but it can be seen that someone broke into the package. This is why quantum cryptography is so useful in distributing the keys used to encrypt messages. A lucky eavesdropper could intercept a quantum encrypted message, and if he made the correct measurement for each bit of the message he would have the key, although the likelihood of making the correct measurements is extremely low for longer messages. But keys are random strings of characters, so even a successful eavesdropper could not tell if he had successfully intercepted a key. For all of his work, the eavesdropper is still unsuccessful – he has altered the key by reading it, and the recipient can see that it has been tampered with, and new keys are sent until one is received that has not been tampered with.

II. CURRENT QUANTUM ENCRYPTION DISTANCES AND SPEEDS

The state of quantum encryption has reached the point where it is useful in real situations, as opposed to just in laboratories. Recently, teams of British and German researchers sent a key between two mountains in Germany for a distance of

14.5 miles (Reuters, Keys). The Los Alamos National Laboratory is thought to hold the distance record for optical fiber at 30 miles (DeJesus). Current fiber systems are thought to be limited to about 60 miles, which rules out use in a global network.

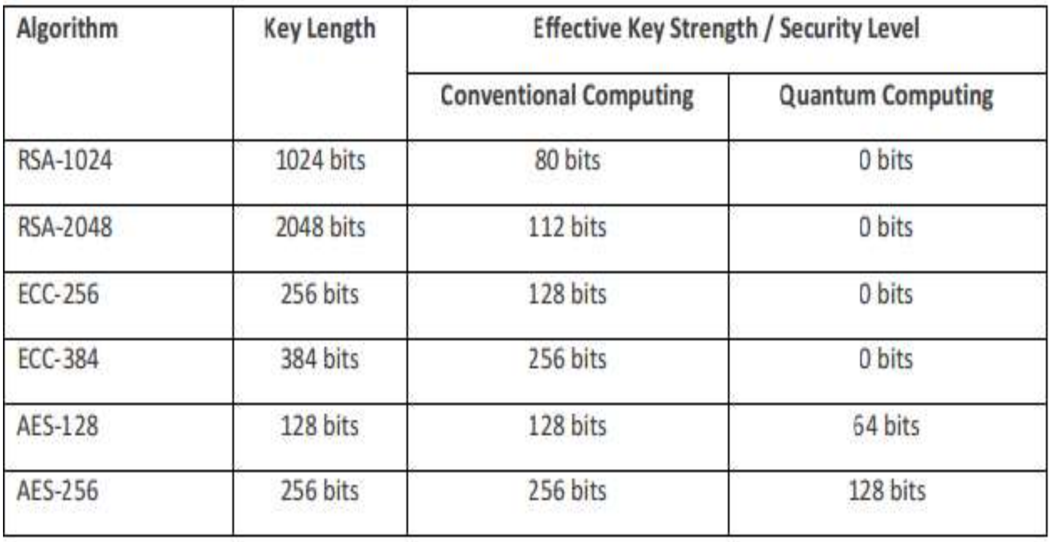
One might think that repeaters could be used to extend the network, but, as stated before, quantum signals cannot be duplicated without changing their properties in some way. Research is also being conducted to speed up the rate of quantum transmissions. At Northwestern University in Illinois, Prem Kumar and Horace Yuen have used standard lasers and existing optical technology to transmit encrypted data at 250 megabits per second over a fiber optic cable (Junnarkar). These researchers came up with the idea of transmitting photons in bundles, rather than single or fractional photons.

Limitations of Quantum Cryptography

Quantum Cryptography has its limitations also. Bruce Schneier, an American cryptographer, says " I don't see any commercial value in it. I don't believe it solves any security problem that needs solving. I don't believe that it's worth paying for. I can't imagine anyone but a few technophiles buying and deploying it. Systems that use it don't magically become unbreakable, because the quantum part doesn't address the weak points of the system.

Security is a chain; it's as strong as the weakest link. Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. Our symmetric and public-key algorithms are pretty good, even though they're not based on much rigorous mathematical theory.

Quantum Cryptography provides a secure communication technique which relies on the quantum physics laws in contrast to the mathematically compute classical cryptography, but there are some limitations to it such as: point to point link & denial of service, losses in quantum channel, high bit error rate, low key distribution rate, photon detectors inaccuracy, sending of one single photon of light at a time, classical authentication and distance limitation which are described above are to be first removed or corrected for better network security. Table 1 represents comparisons of conventional and quantum security levels.



Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Table 1 **The comparison of conventional and quantum security levels of some popular ciphers**

Quantum key distribution is a process that uses an authenticated communication channel together with a quantum communication channel in order to establish a secret key. There are several different protocols for implementing quantum key distribution, all of which require both a quantum channel (to send quantum states of light), and an authenticated classical channel (for the sender, Alice, and the recipient, Bob, to compare certain measurements related to these quantum states and perform certain post-processing steps to distil a correct and secret key). The quantum channel uses optical fibres or free space/ satellite links to send photons (quantum states of light) between Alice and Bob, whereas the classical channel could be a simple (authenticated) telephone line that Alice and Bob use to talk to each other. Interestingly, both of these can be public. The quantum channel necessarily shows Alice and Bob when an eavesdropper has been listening in, and it is a fact of the QKD protocols that the classical channel could be broadcast publicly without compromising security. The Figure 1 represents QKD Communication through quantum channel

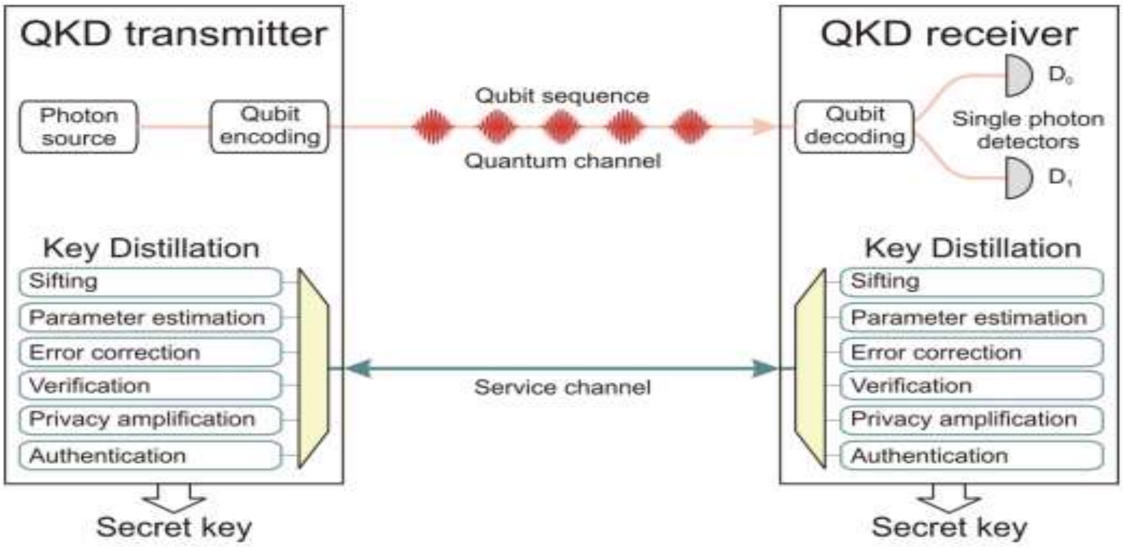


Figure 1 QKD Communication through quantum channel

III. QUANTUM COMPUTING IN INDIA

The laws of quantum physics permit us to process information using what is known as quantum computing. A quantum computer is different from a digital computer that we are so familiar with. While quantum computing sounds like a new technology, the fact is that it is a mathematical approach to finding efficient solutions to computational problems.

To make quantum computing a reality in near future, the following approaches are aggressively studied: Josephson junction circuits, single electron quantum dots, and ion traps. Developments in nanotechnology will, therefore, form the backbone for advancing and realizing quantum computers. In addition, since quantum computing is prone to errors due to imperfections and noise, developing efficient algorithms to take care of quantum error corrections should be an inherent part of any quantum computing initiative. The challenges for the research community, therefore, include creating new models and quantum algorithms, sorting out architectural issues and developing technological solutions if quantum computers are to become a certainty. In conventional information theory and cryptography, it is taken for granted that digital communications can always be monitored and copied, even by someone ignorant of their meaning. Such copies can be stored for an eventual future use, such as helping the decryption of later transmissions enciphered with the same secret key.

However, when elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena, unachievable with traditional transmission media. tions channel whose transmissions in principle cannot be read or copied reliably by an eavesdropper ignorant of certain key information used in forming the transmission. The eavesdropper cannot even gain partial information about such a transmission without altering it in a random and uncontrollable way, likely to be detected by the channel's legitimate users. This principle can be used effectively to design a communication. Such a channel allows the unlimited re-use of a one-time pad without any breach of security, thus contradicting a well-established theorem of Shannon's.

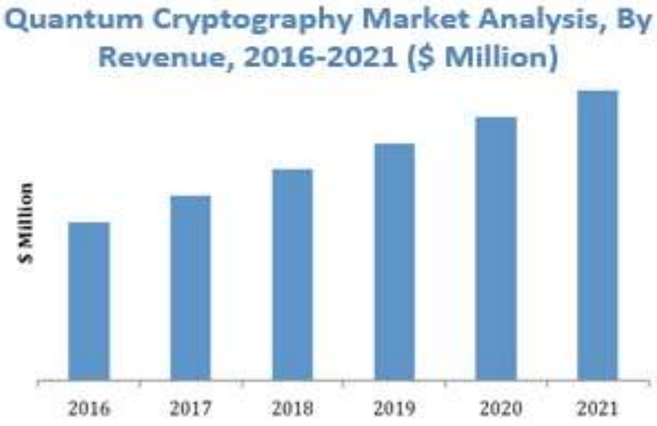


Figure 2 Quantum cryptography market analyses

Figure 2 represents market analysis of Quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact quantum cryptography rests on two pillars of 20th century quantum mechanism, the Heisenberg Uncertainty Principle and the principle of photon polarization. Heisenberg Uncertainty principles say that if you measures one thing, you cannot measure another thing accurately. According to the Heisenberg uncertainty principle it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdropper in a cryptosystem based on quantum cryptography. The photon polarization principle depicts how light photons can be oriented or polarized in specific directions. It is Heisenberg's uncertainty principle that makes quantum cryptography an attractive option for ensuring the privacy of data defeating eavesdroppers.

IV. CONCLUSION

Quantum key dissemination (QKD) is a standout amongst the most well-known uses of quantum cryptography. Quantum mechanics is utilized to secure correspondence between two gatherings and a mystery arbitrary key is utilized to encode and decode the information. QKD just creates and appropriates the arbitrary mystery key and isn't utilized for information correspondence in essence. Standard correspondence channels are utilized for transmission of the information. The requirement for securing information and counter the broad digital security concerns is a central point expanding the development of this market.

Reference

[1] R. Pietro, L. Mancini, A. Mei, Random key assignment for secure wireless sensor networks, in: ACM Workshop of Ad hoc and Sensor networks (SASN'03). 128

[2] Catherine Meadows ―Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends‖ IEEE Journal on selected areas in communication‖ VOL. 21, NO. 1, JANUARY 2003 pp 44-54

[3] P. Caballero-Gil, C. Hen´andez-Goya, C. Bruno-Castaneda ―A rational approach to cryptographic protocols‖ Mathematical and Computer Modelling 46 (2007) pp 80–87

[4] S. Muhammad, R. K. Guha and Z. Furqan "A Simplified Logic Based Framework for Formal Analysis of Cryptographic Protocols". Computer Science Technical Report CS-TR-05-10, School of Computer Science, University of Central Florida, Oct. 2005.

[5] Y.J.Chen,Y.L.Wang, ―The Design of Cluster based group key Management system in wireless networks‖ in proc IEEE,2005

[6] Duursma I, Lee H-S. A group key agreement protocol from pairings. Applied Mathematics and Computation 2005;167:1451–6.

[7] Y. Challal and H. Seba, ―Group key management protocols: A novel taxonomy,‖ International Journal of Information Technology (IJIT), vol. 2, no. 1, pp. 105-118, 2005

[8] I. Hossain and S. M. Mahmud, ―Group key management for secure multicasting in remote software upload to future vehicles,‖ accepted for publication in the 2006 issue of SAE Transactions on Passenger Cars: Electrical and Electronic Systems. 129

[9] Roberto Di Pietro , Luigi V. Mancini , Sushil Jajodia ―Providing secrecy in key management protocols for large wireless sensors networks‖ Elsevier Ad Hoc Networks 1 (2003) 455–468

[10] M. Tatebayashi, N. Matsuzaki, D.B. Newman, Jr., Key distribution protocol for digital mobile communication systems, in: Advances in Cryptology—Crypto'89, Lecture Notes in Computer Science, vol. 435, 1989, pp. 324–334

[11] Issa Khalil , Saurabh Bagchi , Ness Shroff , ―Analysis and evaluation of SECOS, a protocol for energy efficient and secure communication in sensor networks‖ Elsevier Ad Hoc Networks 5 (2007) 360–391

[12] Benny Pinkas,‖ Efficient State Updates for Key Management‖ invited paper proceedings of IEEE, VOL. 92, No 6, June 04 pp 910- 917

[13] Phleeger, C.P., 1997. Security in Computing; ―Mandatory and Discretionary Access Control‖, p. 290; Prentice Hall; Second Edition, 1997.

[14] Microsoft. Microsoft .NET Passport review guide; March 2003.

[15] J. G. Steiner, C. Neuman, and J. I. Schiller, ―Kerberos: An authentication service for open network systems,‖ in Proc. Winter USENIX Tech. Conf, Dallas TX1998 pp191-202 130

[16] Bellovin SM, Merritt M. Limitations of the Kerberos authentication system. ACM Computer Communication Review 1990;20:119e32.

[17] Ashley P, Vandenwauver M. Practical Intranet security overview of the state of the art and available technologies.Norwell, MA: Kluwer Academic Publishers; 1999

[18] J. Hwang and Y. Kim, "Revisiting random key predistribution schemes for wireless sensor networks," ACM workshop on Security of ad hoc and sensor networks, pp. 43-52, 2004.

[19] Hyeokchan Kwon, Sangchoon Kim, Jaehoon Nah, Jongsoo Jang ―Public Key Management Framework for Two-tier Super Peer Architecture‖ 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)

[20] Philip Zimmermann, Hal Finney, Branko Lankester, and Peter Gutman. PGP - Pretty Good Privacy, version 2.3A1 July 1993.

[21] A. Abdul-Rahman, The PGP Trust Model, EDI-Forum: J. Electron. Commerce, 1997 Applied Cryptography by Bruce Schinner 2nd Edition PHI publication 2007

[22] Vengatesan K., and S. Selvarajan: Improved T-Cluster based scheme for combination gene scale expression data. International Conference on Radar, Communication and Computing (ICRCC), pp. 131-136. IEEE (2012).

[23] Kalaivanan M., and K. Vengatesan.: Recommendation system based on statistical analysis of ranking from user. International Conference on Information Communication and Embedded Systems (ICICES), pp.479-484, IEEE, (2013).

[24] K. Vengatesan, S. Selvarajan: The performance Analysis of Microarray Data using Occurrence Clustering. International Journal of Mathematical Science and Engineering, Vol.3 (2) ,pp 69-75 (2014).