ISSN:0975-9646

Lavannya Varghese et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 14-17

Quantum Cryptography

Lavannya Varghese[1]. , Raisa Varghese[2], Vince Paul[3], Sankaranarayanan P N[4]

[1]Student, [2,4] Assistant Professor, [3] Head of Department

[1,2,3,4]Computer Science Department,
Sahrdaya College of Engineering and Technology
Thrissur (District), Kodakara,
Kerala- 680683, INDIA

***Abstract*— For ages,mathematicians have searched for a system that would allow two people to exchangemessages in perfect privacy.Quantum cryptography wins to make data secure using fundamentalphysical principles such Heisenbers uncertainty principle and cloning theorem.probably its bestknown application today is quantum key distribution ,which allow two parties to protect theirsecret communication from prying eyes of an evesdropper.Transport layer security is designedto provide communication security over the internet.TLS use X.509 certi_cates and hence asymmetric cryptography to authenticate the counterparty with when they are communicating andto exchange a symmetric key.In this paper,I introduce new approach to provide a secure connection between internetbrowsers and website allowing people to transmit private data online,by integrating quantumcryptography in TLS protocol.Quantum cryptography technologies both securely authenticateclients and servers and exchange trade secret symmetric key and provide secure communication**

***Keywords*—Quantum key distribution,TLS**

I. INTRODUCTION

Cryptography is the art of the principles and method of transforming an intelligible,and then retransforming that message back to its original form.Cryptography is an essential part of today's information systems.Quantum cryptography is recent technique ,that can be used to ensure the confidentiality of information transmitted between two parties.Using laws of quantum mechanics such as Heisenberg uncertainty principle and cloning theorem .Quantum mechanics fundamentally change the way we must see our world.At atomic scales,elementary particles do not have precise location or speed as we would intuitively expect.According to Heisenberg uncertainty principle we can't measure position and angular momentum of a particle simultaneously.In quantum cryptography both sender and receiver having polarizers.Using light emitting source sender sends photon to receiver .If both both sender and receiver use the same polarizer ,then we select that bit value as a one bit of the key.

Internet banking have very important role in our day to day life.TLS,(Transport Layer Protocol)or SSL(Secure Socket Layer) are based on public key cryptography. In the authentication process,aTLS/SSL client sends a message to a TLS/SSL server and sever responds with the information that the server needs toauthenticate itself.The client andserver perform an additional exchanges of session keys and authenticationdilogues ends.When authentication completes SSL-communication can begin between the server and client using symmetric keys ,that established during authentication process.In TLS generate a session key by using RSA.So instead of RSA ,we can integrate quantum cryptography in TLS inoder to increase the security.

II. QUANTUMCRYPTOGRAPHY(BB84 PROTOCOL)

Using cryptography, we can keep private information from unautherized access of ensuring data integrity and authentication and other taskes.There are various type of classical cryptography. In ceaercipher,key followed is every letter is replaced by third letter.So it is easy to understand the evesdroppernad easy break the code.In classical cryptography permutation s and substitution techniques are used.Soot is easy for eves to break the code.There are two type of cryptographic algorithm.Symmetric key nad public key algorithm.In symmetric key algorithm,one key is shared by both sender and receiver and used for both encryption and decryption.Inassymetric key algorithm or pubic key algorithm use two keys.One is public key ,used in public and private key is known only to individual user.

In Quantumcryptography ,there are two channel,optical channel and public channel.Optical channel is used for transferring photons between sender and receiver. Public channels used for discussing about which polarizer is both sender and receiver used.In quantum cryptography ,it ensure secure communication between two parties across optical network.Both sender and receiver two polarizers and light emitting source.There are two polarizer,vertical polarizer and diagonal polarizer.At the sender side light emitted from light emitting source will passed through one of the polarizer,either through vertical polarizer or through diagonal polarizer across optical netwok.Light waves are propagated as discrete quanta called,photons.They are massless and have energy,momentum and angular momentum called spins.Spin carries the polarizeration photon may or may not pass through he polarizer using a detector to check whether the photon polarized or not.At receiver side also having polarizer and it polarize the photon.If the sender and receiver using the same polarizer,then match occurred and that bit value become one of the bit of the key.

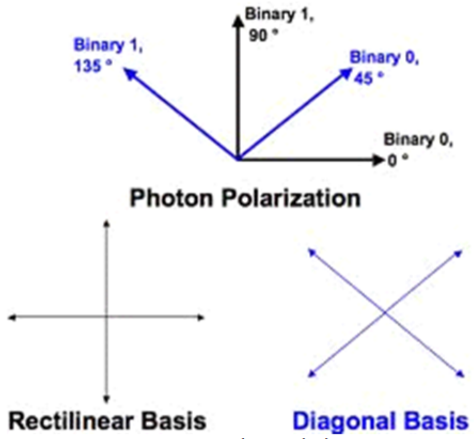

Fig.1 Polarizers

There are two polarizer,vertical polarizer and horizontal polarizer.In vertical polarizer photon movement is in 90^0 then bit value become 1 and photon movement is in 0^0 ,then bit value wil be 0.Inacse of diagonal polarizer photon movement is in45^0 bit value will be 1 and if photon movement is in 135^0 bit value becomes 0

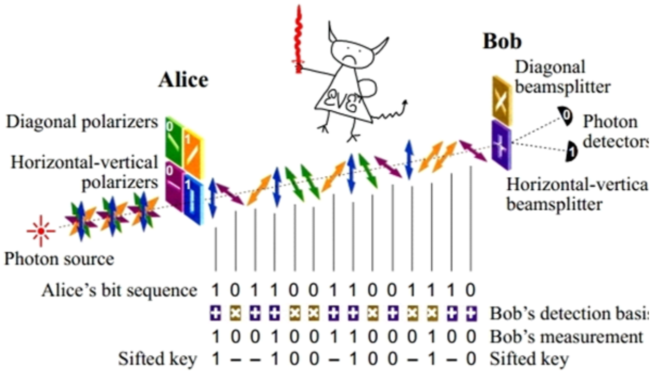

Fig.2 Example of quantum key distribution

Figure2 shows an example of quantum key distribution.Alice(sender)side light from light emtting source passed through the vertical polarizer and its direction in vertical,so it having bit value 1.Second photon passed through vertical polarizer and its direction is in horizontal,so it having bit value 0.Third photon passed through dioganal polarizer and the photon movement in 45^0. So bit value becomes 1.Fifth photon passed through the dioganal polarizer and photon movement in 135^0,so that the bit value becomes 0.At the same time the receiver side will use the polarizer for each photon, what sender send.Incae of first photon ,receiver use vertical polarizer nad photon movement in 90^0 direction,so match occurred and that bit is selected for the key.Incase of second photon receiver use the diagonal polarizer a nd sender use the vertical polarizer ,so no match found and discard that bit.Sender and receiver using the same polarizer and bit value is taken for one of the key.

III.INTEGRATING QUANTUM CRYPTOGRAPHY IN TLS PROTOCOL

TLS protocol developed by Netscape and its used for web security.Transport layer protocol provides secure communication between two communicating entities.TLS protocol provide data encryption and authentication between application and sever in scenarios,where that data is being sent across an insecure network.TLS having Record,protocol,Handshake protocolChange spec protocol,Alert protocol and Applicatipn protocol.

Record protocol will fragment the upper layer message into block and applies MAC ,encrypt & transmit the result.Handshake protocol allow sever and client to authenticate each .In change cipher protocol,when byte becomes 1 means pending state to be copied into the current state.Alert protocol will produce error message.

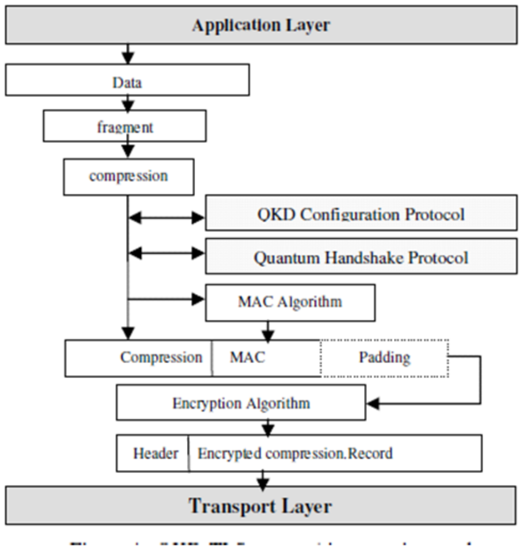

Fig.3QKD-TLS in operation mode

Inoder to integrate QKD in TLS protocol we need optical chanel,opticalmedium,QKDprotocol.Transmission of photon occurs through optical fiber or free space.Opticalfiber reduces noises than free air.Optical medium having photon detector,polarizer and photon emitter.To generate a key, it is necessary to implement a protocol of QKD between the two optical modems. The key once generated, it is stored in a flash memory in order to be used in the phase of enciphering data.

IV.QKDCONFIGURATION PROTOCOL

OKD configuration protocol having message format which includes Type,that specifies type of quantum cryptography protocol is used.ie,protocol is based on Heisenberg uncertainty principle or Bells theorem.Protocol field specifies the quantum key protocol used.Version specifies the current version of the protocol used .Length field specifies length of the key and TTL field is help to generate a new key ,when time is expired or maximum of message is reached.

Type		Protocol	Version
Length			
Key-Length			
TTL	T	Authentication	Encoding
Content			

Fig.4 message format of QKD configuration protocol

V .QUANTUM TLS HANDSHAKE PROTOCOL

In QKD-TLS Protocol, we have added certain changes in the TLS Handshake Protocol.Our main goal is to generate security parameters by the mechanism of QKD and to remove all structure based on PKI.Firstly, we suppose the client and the server share a secret noted S. Secondly, we have replaced in TLS Handshake Protocol the procedure of classical process of key exchange (such RSA or Di_e-Hellman) by the mechanism of QKD using the BB84 protocol. We give the modified TLS Handshake Protocol the new name of Quantum TLS Handshake Protocol.As BB84 is vulnerable to a man in the middle attack, we verify if an eavesdropper is detected once the execution of BB84 protocol is finished, by calculating the TLS finished in both sides of the client and the server. This is done by using the shared secret S and the key K derived from the BB84 Protocol.During the Quantum TLS Handshake Protocol and when the server receives the ClientHello, it sends to the client a series of polarized photons.

The number of photons to be transmitted depends on the length of the desired key, the error correction algorithm and the privacy amplification algorithm used.

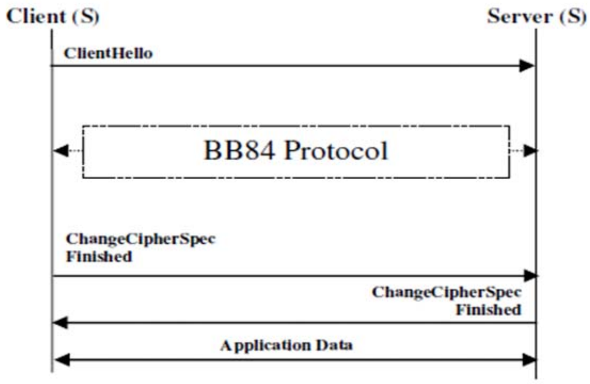

Fig.5 messages exchanged in quantum TLS handshake protocol

VI.QKD-IN INTERNET BANKING

The Internet is an integral part of our daily lives,and the proportion of people who expectto be able to manage their bank accounts anywhere,anytime is constantly growing. As such,Internet banking has come of age as a crucial component of any financial institutions multichannel strategy.Information about financial institutions, their customers,and their transactionsis, by necessity, extremely sensitive; thus, doing such business via a public network introducesnew challenges for security and trustworthiness.Any Internet banking system must solve theissues of authentication, confidentiality, integrity, and non repudiation,which means it mustensure that only qualified people can access an Internet banking account, that the informationviewed remains private and cant be modified by third parties, and that any transactions madeare traceable and verifiable. For confidentiality and integrity,Secure Sockets Layer/TransportLayer Security(SSL/TLS) is the de facto Internet banking standard,whereas for authenticationand non repudiation, no single scheme has become predominant yet.

Online channel-breaking attacks,introder is trying to get the users credentials, the intruderunnoticeably intercepts messages between the client PC and the banking server by masqueradingas the server to the client and vice versa. Although the server is normally authenticated via a public-key certificate when a SSL/TLS session is established, users sometimes naively ignore messages about invalid or untrusted certficates or, even worse, are fooled to trust onlinegenerated fake server certificates from a nested intruder certification authority(CA).As a result, an intruder could hijack the authenticated banking session or silently manipulate transaction data.in internet banking Authentication based on a hardware-token public key infrastructure (PKI) also avoids the risk of onine credential-stealing attacks against insuficiently secured PCs.Specifically, these schemes effectively cross the onlinechannel-breaking-attack boundary independently of user behavior via a SSL/TLS channel-parameter-dependent challenge. PKI uses asymmetric cryptographic algorithms such as Rivest Shamir Adlemann (RSA) or Elliptic Curve Cryptography (ECC).

Initially, the bank fits each user with a pair of matching private and public keys for which some trusted authority issues a matching digital certificate.The certificate attests that the username is associated with the given public key and that the user holds the corresponding private key. The private key and certificate then establish a mutually authenticated SSL/TLS channel between the user's PC and the banks server, effectively eliminating online channel breaking attacks. The only critical issue is the protection of the users private key against malicious software.so we generate security parameter by the mechanism of QKD and to remove all structure based on PKI.suppose the client and server share a secret key S,then we have replaced in TLS Handshake protocol the procedure of classical process of key exchange by Quantum Cryptography mechanism of QKD using BB84 protocol.During quantum TLS handshake protocol and when server receives the clienthello,it sends to the client series of polarized photons.the number of photons to be transmitted depends on the length of the desired key.By using QKD,we tend to achieve unconditional security because QKD is proven scientifically to be unconditional secure.

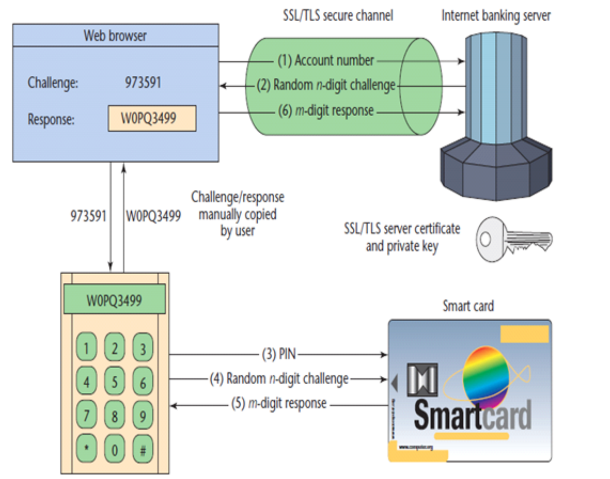

Fig. 6 Internet banking scenario

VII. CONCLUSION

Quantum cryptography ensure secure communication by providing security based on the fundamental law of physics,intead of the current state of mathematical algorithms or computing technology.unlike classical encryption algorithm quantum cryptography does not depend factoring large integers into primes but on the fundamental principles of quantum physics.Quantum cryptography is more secure,because an intruder is not able to replicate the photon to recreate the key.

Integrating QKD in TLS protocol will ensure financial transaction.instead of using RSA,in TLS protocol .We can use QC securely exchange the secret data and avoid an attack of
intruder

ACKNOWLEDGMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this seminar report. I am thankful for their aspiring guidance, invaluably constructive criticism and friendy advice during the seminar work.I deeply express my sincere thanks to my seminar guide Ms.Raisa Varghese for her support and guidance.

REFERENCES

[1] V.Scarani et al."The Security Of Practical Quantum Key Distribution",Rev.Modern Physics,vol.81,2009,pp1301-50.
[2] M.Niemeic,"Quantum Cryptography-The analysis of Security Requirements", Int'l.Conf.Transparent Optical Networks,S miguel,portugal,2009.
[3] S.Ghernaouti-Helie and M.A.Sfaxi,"Guaranteeing Security of _nancial Transaction by Using Quantum cryptography in banking environment",E=business andTelecomunication.Networks,vol.3,2007,pp.139-49
[4] Gisin,N.,etal;"Quantum cryptography",Rev.Mod.phys.,2002,74,pp.145-195
[5] Bennet,C.H.,etal:"Experimental quantum cryptography", J.Cryptol., 1992,5,pp..3-28
[6] M.Elboukhari,M.Azzi,A.Azzi"Integration of Quantum Key Distribution in TLS Protocol",IJCSNS,Vol.9 No.12 pp.21-28,2009
[7] C.Elliott,D.Pearson,G.Troxel,"Quantum Cryptography in Practice"Proc.ACM SIGCOMM2003
[8] C.Elliot,"Building the quantum network"NewJ.Phys.4(July 2002)46
[9] C.H Bennett and G.Brassad,"Quantum cryptography:PublicKey Distribution and cointossing"inProc.IEEEInt.Conf.Computers,Systems and Signal Processing New York1984,pp.175-179
[10] Gisin ,N.and R.Thew, Quantum Communication. NATURE PHOTONICS, 2007.1(3):pp .165