International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 4, Jul. - Aug. 2013 pp-2327-2329 ISSN: 2249-6645

Three Party Authenticated Key Distribution using Quantum Cryptography

V. Padmaja[1], Sayeed Yasin[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Asst. Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India*

***ABSTRACT*:** *Cryptography is the science of writing in secret message and is an ancient art. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly over the Internet. Over the last two decades an interesting field of the cryptography has raised from non classical atomic theory, Quantum Physics. This field is known as Quantum cryptography. Unlike the classical cryptography of public and private key ciphers which analyse the strength of a cipher by means of mathematical attacks and formulas, the security of the quantum cryptography is ensured by laws of Quantum Physics. In this paper, we present a method for three party authentication using quantum cryptography. Our method depends on partial trusted third party, so that the key is not revealed to the trusted third party.*

KEYWORDS*:** *Authentication,* ***Cryptography, Photon, Secret key.

I. INTRODUCTION

Cryptography[1] plays an important role in modern life as it allows for secure communication over insecure channels, even in the face of powerful adversaries. Cryptography has been used for the military and government communications for more than 2000 years, but only in the past 20 years has cryptography come to be used in day-to-day life. The expansion of the Internet from a small scale academic network to a global network enabling hundreds of billions of dollars of the electronic commerce was due in no small part to the availability of cryptography. The successful design of the multitudes of secure cryptographic algorithms — public key agreement, digital signatures, block and stream ciphers, hash functions, message authentication codes — and secure protocols that employ these primitives is a remarkable achievement. Of those that have been widely adopted, the majority have remained fundamentally secure despite years of intensive cryptanalysis and the advancing computer technology.

Various security problems abound on the Internet. The servers of governments and the major corporations are subjected to denial of service attacks. Spyware, viruses, and malware are installed on the users' computers. Individuals fall victim to phishing attacks and the identity theft. Devices are subject to attacks that exploit the subtle variations in their power usage. These security problems do not arise as a result of a break of the cryptographic algorithms or protocols. Rather, they arise by working around the cryptography- why exert billions of hours of computer effort to break an advanced encryption protocol to crack a user's password when you can simply trick the user into telling you their password directly?

In symmetric key cryptography, both parties must possess a secret key(shared key) which they must exchange prior to using any encryption. Distribution of the secret keys has been problematic until recently, because it involved face-to-face meeting, use of a trusted courier, or sending the key through an existing encryption channel. The first two are often impractical and always unsafe, while the third depends on the security of the previous key exchange. One solution is based on the mathematics, public key cryptography**.** In public key cryptography, the key distribution of the public keys is done through public key servers. When a person creates a key-pair, he/she keeps one key private and the other, public-key, is uploaded to a server where it can be accessed by anyone to send the user a private, encrypted, message. Another approach is based on physics- quantum cryptography. While public-key cryptography relies on the computational difficulty of certain hard mathematical problems, quantum cryptography relies on the laws of the quantum mechanics**.**

II. QUANTUM CRYPTOGRAPHY

Quantum cryptography[2] uses quantum mechanics to guarantee a secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a shared key to encrypt and decrypt messages. An important and unique property of the quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental part of quantum mechanics- the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing a detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in the quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold a key can be produced which is guaranteed as secure, otherwise no secure key is possible and the communication is aborted.

The security of the quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. Quantum cryptography is only used to produce and distribute the key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt and decrypt the message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with the secret, random key.

III. RELATED WORK

There are two three party quantum key distribution protocols(QKDps), one with implicit user authentication and the other with explicit mutual authentication[3], are combined to demonstrate the merits of combining both classical and quantum cryptography. Also when compared with the classical three-party key distribution protocols, the proposed QKDPs easily resist replay attacks. This work presents a new direction in designing QKDPs by combining the advantages of classical with the quantum cryptography. There are few quantum key distribution protocols described in [4] such as B92 quantum cryptographic protocol, BB84 quantum cryptographic protocol, Entanglement-based quantum key distribution and Quantum Bit Commitment (QBC) protocols. Also this paper includes protocol evaluating and comparison, using such criteria as the error possibility, quantum and classical memory bounds, noise sensitivity.

Some of the advantages of the Quantum Cryptography over classical cryptography described in[5] i.e., it gives us perfectly secure data transmission. Also it discusses about Quantum Key Distribution and how important the quantum cryptographic protocols are to it. It also tells about how eavesdropping will be in quantum cryptography and its effects. The security of some of the quantum cryptographic protocols such as Six-state protocol, BB84 protocol, SARG04 protocol, Symmetric and Asymmetric three-state protocol is described in [6]. The authors also compare their performances in both the ideal case and in the realistic case and found that Efficient BB84 and Six-state protocols tolerate the highest QBER.

IV. EXISTING SYSTEM

In [3], the authors proposeda three-party quantum authenticated key distribution protocol (QAKD). This three-party QAKD is immune to the man-in-the-middle attack, while it performs both authentication and the key distribution with one step by utilizing a trusted third party. The weakness of this scheme is that it relies 100% on the trusted third party(TTP). The TTP has the ability to read all communication packets. In cryptography or network security, an authentication between parties unknown to each other is not possible without the third party that guarantees the identities of the participating parties. Thus, a TTP, which is a disinterested party trusted to complete a protocol [7], needs to be introduced. However, in a real world, such an idealized assumption cannot be always possible. For example, it may be too optimistic to make an assumption in key distribution schemes for medical applications. Patient information should be shared only between the patient and the doctors, so the third party for the key distribution system should not be able to read the encrypted confidential data. There must be a safeguard to protect the confidentiality even from the trusted third party in such applications.

V. PROPOSED SYSTEM

Let Alice and Bob intended to share an authenticated shared key 'K', which is an n- bit random number. Here we assume that every participant shares a secret shared key with the trusted centre in advance. Let $K_{A,T}$ is the key shared between the Alice and Trusted Centre(TC), and $K_{B,T}$ is the key shared between Bob and TC. Let h(K,M) is a hash value of a message M with key "k", generated using a hash function(e.g., SHA-1 or MD5). Assume that the TC has been notified to start the authentication session as follows:

The TC generates two random numbers r_A and r_B and then computes:

$$X = h(K_{A,T}, r_A) \oplus (U_A \| U_B)$$

$$Y = h(K_{B,T}, r_B) \oplus (U_B \| U_A)$$

Now $r_A \| r_B \| X$ is polarized and encrypted using the pre- shared key $K_{A,T}$ and the result is transmitted to Alice over a Quantum channel. Also $r_B \| r_A \| Y$ is polarized and encrypted Using the pre- shared key $K_{B,T}$ and the result is transmitted to Bob over another Quantum channel.

Alice decrypts and measures the received qubits. She computes a hash value using $K_{A,T}$ and r_A and obtain the values of $U_A \| U_B$. Then she verifies the values of U_A and U_B.

Bob decrypts and measures the received qubits. She computes a hash value using $K_{B,T}$ and r_B and obtain the values of $U_B \| U_A$. Then she verifies the values of U_A and U_B. Thus after the successful completion of the session, both Alice and Bob are implicitly authenticated using the TC.

A secret key 'K' is going to be established between Alice and Bob. The secret key will not revealed to others, even to Trusted centre. Key establishment is based on Shamir's three- pass protocol and Quantum superposition states. Here classical Shamir's three- pass protocol is combined with superposition states, because classical shamir's protocol is vulnerable to attacks[8].

In the following discussion, without losing generality, we can assume that message M is single photon encoded as M= |0> (i.e.., n=1 and i_1=0) and Alice initiates a key distribution.

(i) First, Alice and Bob generate their session keys $K_A = \theta_A$ and $K_B = \theta_B$.

(ii) Alice encrypts M with her encryption key K_A. The resulting state can be described as

E_{K_A} [M] : R(θ_A)|0>= $\begin{pmatrix} \cos\theta_A & \sin\theta_A \\ -\sin\theta_A & \cos\theta_A \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

= cos θ_A . |0> - sin θ_A . |1>= $|\psi_1\rangle$,

Where E_{K_A} indicates an encryption with K_A. Such a resulting state is called as a superposition state . Alice sends the resulting state $|\psi_1\rangle$ to Bob.

(iii) Bob receives the photon in $|\psi_1\rangle$ and encrypts it with his key K_B .

E_{K_B} [E_{K_A} [M]]: R(θ_B).$|\psi_1\rangle$

= cos($\theta_B + \theta_A$) |0> - sin ($\theta_B + \theta_A$) |1>

= $|\psi_2\rangle$

The resulting state $|\psi_2\rangle$ is still a superposition state. Bob send it back to Alice.

(iv) Alice receives and decrypts it by rotating it back with the angle θ_A (i.e., rotation of - θ_A)and sends the resulting superposition state $|\psi 3\rangle$ to Bob.

D_{K_A} [E_{K_B} [E_{K_A} [M]]]= E_{K_B} [M]: R(- θ_A).$|\psi_2\rangle$

= cos θ_B . |0> - sin θ_B . |1> = $|\psi 3\rangle$

Where D_{K_A} indicates a decryption with K_A.

(v) Bob receives and decrypts it by rotating it back with the angle θ_B (i.e., rotation of - θ_B).

D_{K_B} [E_{K_B} [M]]: R(- θ_B). $|\psi 3\rangle$

= $\begin{pmatrix} \cos(-\theta_B) & \sin(-\theta_B) \\ -\sin(-\theta_B) & \cos(-\theta_B) \end{pmatrix}.\begin{pmatrix} \cos\theta_B \\ -\sin\theta_B \end{pmatrix}$

= $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ = $|0\rangle$.

Now, Bob has the original message M= $|0\rangle$.

After the key distribution phase, both the participants ave the key 'K'.

VI. CONCLUSION

This paper presents a Quantum authenticated key distribution protocol that can perform key distribution and also ensure that the participants of the communication are authentic, both implicitly and explicitly. This protocol provides new directions in Classical cryptography and Quantum cryptography. The Participants of the protocol trust the third party regarding the authentication part only. Thus the proposed protocol will be preferable for network systems which deal with highly sensitive information, such as military, hospitals, research facilities. Our protocol utilizes polarized photons in superposition states for authentication and key distribution which provides high security against many attacks.

REFERENCES

[1]. W. Stallings, Cryptography and Network Security: Principles and Practice 3/e. Prentice Hall, 2003.
[2]. C.H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing, in: Proc. IEEE Int. Conf. on computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, 1984.
[3]. Tzonelih Hwang, Kuo-Chang Lee, chuan-Ming Li, "Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols," IEEE Transactions on Dependable and Secure Computing, vol. 4, No. 1, January-March 2007.
[4]. Lelde Lace, Oksana Scegulnaja-Dubrovska, Ramuns Usovs, Agnese Zalcmane, "Quantum Cryptographic Key Distribution Protocols", The European Social Fund(ESF), 2008.
[5]. Rajni Geol, Moses Garuba and Anteneh Girma, " Research Directions in Quantum Cryptography", International Conference on Information technology, 2007.
[6]. Chi-Hang Fred Fung, Hoi-Kwong Lo, "A survey on quantum cryptographic protocols and their security", IEEE, 2007.
[7]. B. Schneier, Applied Cryptography, John Wiley, New York, 1996.
[8]. Rolf Oppliger "Contemporary Cryptography", Artech House, Computer security series, 2005, pp. 408- 410.