A note on Quantum Cryptography

G. Ananda Rao [a], Muduganti Rathan Reddy [b], Y.Srinivas [c], J.Vijayasekhar [d], N.Vamsi Krishna [d], Ramakrishna Jaliparthi [e], V Manoj Shekhar [f], Venu Saggurthi [g], S. Usha Rani [h]

[a] Department of Applied Mathematics, GITAM University, Vishakhapatnam, India.
[b] Department of Computer Science & Engineering GITAM University, Hyderabad, India.
[c] Department of Computer Applications, GITAM University, Hyderabad, India.
[d] Department of Engineering Mathematics, GITAM University, Hyderabad, India.
[e] Programmer Analyst, JCG Technologies, Beaverton, Oregon, USA.
[f] Software Engineer, Verizon , Texas, USA.
[g] Software Consultant, Wipro Technologies, Beaverton, Oregon, USA.
[h] **Senior Lecturer,** Sri Chaitanya Mahila Kalashala, Miyapur, Hyderabad.

Abstract

Cryptography provides security for the information and personal details. The combination of 3AQKDP (implicit) and 3AQKDPMA (explicit) quantum cryptography is used to provide authenticated secure communication between sender and receiver. Cryptography provides following merits establishment of a secure connection which can prevent attacks such as eavesdropping, man-in-the-middle and replay. Applications of cryptography include computer passwords, bank account passwords, ATM machines, etc. However there are many other classical cryptography ways for securing ones particular data but they are currently unsafe and they cannot detect the existence of passive attacks such as eavesdropping, man-in-the-middle and replay. So by combining the classical cryptography with quantum cryptography we can achieve more benefits.

KEYWORDS: Cryptography, Quantum cryptography, 3AQKDP(implicit), 3AQKDPMA(explicit).

1. Introduction

It is a process of protecting information by converting the information into unreadable format known as cipher text. It can be converted into readable format if and only if proper secret key is entered then only it can decrypt. Encryption is a process converting of original data (called plain text) into unintelligible form by means of reversible translation ie based on translation table or algorithm, which is also called enciphering. Decryption is the process of translation of encrypted text (called cipher text) into original data (called plain text), which is also called deciphering. This is the meaning of the term cryptography.

Authenticity means that when a user receives a message, it is assured about the identity of the sender. The authenticity requirement can be translated in the context of secure multicast.

Key authenticity: only the center can generate a session key.

Data authenticity: the users can distinguish among the data sent by the center and the malicious data sent by an attacker

KEY distribution protocols are used in the communication network by providing sharing secret session keys between users. By using this shared secure keys we can have a secure communications over a insecure networks. In some cases users establish a Trusted center (TC) which verifies the secured keys and allow access these condition is called three party where we have two users and one trusted center. 3AQKDP with implicit user authentication, which ensure that confidentiality is only possible for legitimate users and mutual authentication is achieved only after secure communication using session key start. In implicit quantum key distribution protocol (3AQKDP) have two phases such as setup phase and distribution phase to provide three party authentication with secure session key distribution. In this system there is no mutual understanding between sender and receiver. Both sender and receiver should communicate over trusted center. In explicit quantum key distribution protocol (3AQKDPMA) have two phases such as setup phase and distribution phase to provide three party authentication with secure key distribution. Here there is mutual understanding between user and sender they should communicate directly with authentication of trusted center. Classical cryptography provides convenient techniques that enable efficient key verification and user authentication but it doesn't identify eavesdropping. Here, the enhanced key distribution protocol using classical and quantum cryptography will improve the authentication and help identify eavesdropping. Disadvantage of separate process 3AQKDP and 3AQKDPMA were provide the authentication only for message, to identify the security threads in the message. Not identify the security threads in the session key.

2.The advantages of key distributed protocol authentications for three party using implicit and explicit quantum cryptography

Advantage of combining implicit and explicit quantum cryptography is used to verify the session key from

trusted center and which improve key verification and secure the communication. Also identify the security threads in session key verification. Another advantage is to avoid noise in message transmission by identifying the size of bytes transmitted over the network from sender to receiver and remove the extra byte content received from network. Enhanced key distribution protocol using classical and quantum cryptography will improve the security and authentication.

3. Details about existing system

.In classical cryptography, three party key distribution protocol utilize challenge response mechanisms or time stamps to prevent replay attacks. However challenge mechanisms require at least two communication rounds between the TC and participants, and timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems.(due to the unpredictable nature of network delays and potential hostile attacks) .Furthermore, classical cryptography cannot detect the existence of passive attacks such as eavesdropping. This fact can then be used to reduce the number of rounds of other protocols based on challenge-response mechanisms to a trusted center.

4. Limitations of existing system

Disadvantage of separate process 3AQKDP and 3AQKDPMA were provide the authentication only for message, to identify the security threads in the message. Not identify the security threads in session key.

5. Details about proposed system

Methodology:

Quantum key distribution protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication.

Algorithm:

There are two types Quantum Key Distribution Protocol, they are

a. The proposed 3AQKDP:

This prosed 3AQKDP describes the details of the 3AQKDP by using the notations defined in previous sections. Here, we assume that every participant shares a secret key with the TC in advance either by direct contact or by other ways.

b. The Proposed 3QKDPMA :

The proposed 3QKDPMA can be divided into two phases: the Setup Phase and the Key Distribution Phase. In the Setup Phase, users pre share secret keys with the TC and agree to select polarization bases of qubits based on the pre shared secret key. The Key Distribution Phase describes how Alice and Bob could share the session key with the assistance of TC and achieve the explicit user authentication.

6. ANALYSIS AND DESIGN

Design Overview

6.1. Sender module:

a)Secret Key authentication:

A secret key is given to the trusted center by the sender. TC verifies the key and authenticate to the corresponding sender and get the session key from the TC or else TC not allow the user transmission.

b) Encryption

The message is encrypted by the received session key and appends the qubit with that encrypted message, then transmits the whole information to the corresponding receiver.

Diagram for sender module:

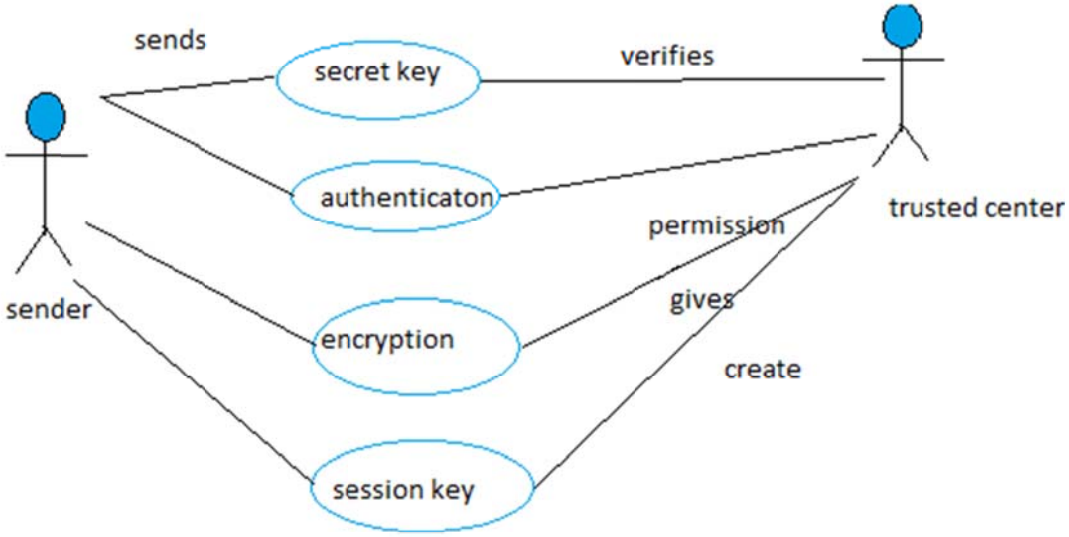


Diagram for sender module

6.2. TrustedCenter: Here users share secret key with the Trusted center

Secret Key Verification:

It verifies the secret key provided by the user and then authenticate the user for secure transmission.

a) Session Key Generation:

A secret key is shared between the users and is used for encryption and decryption. In this case the session key size is 8bits. This session key is generated from pseudo random prime numbers and exponential values of random numbers.

b) Qubit Generation:

We have to convert the secret key and random string into Hex-code and then into binary code in order to get them. Find the least bit of two binary values and get the quantum bit of 0 and 1.

To generate the quantum key using the qubit and session key this depends on the qubit combinations, such as:

i. If the value is 0 and 0, then $1/\sqrt{2}(p[0] + p[1])$.
ii. If the value is 1 and 0, then $1/\sqrt{2}(p[0] - p[1])$.
iii. If the value is 0 and 1, then p[0].
iv. If the value is 1 and 1, then p[1].

c) Hashing:

In Hashing the session key is encrypted using master key and store all the values to TC storage.

d) Key Distribution:

The original session key and qubit is distributed to the sender for encrypting the message. The key and qubit is also distributed to the corresponding receiver to decrypt the received messages.

6.3. Receiver Module:

a) Secret key Authentication:

An encrypted message is received with Hashed session key and qubit with TC and generates the master key and reverses the hash,the session key and also reverse hash the session key which improve the key authentication.

b) Decryption:

Using session key the message is decrypted and showed to the user.

Diagram for receiver module:

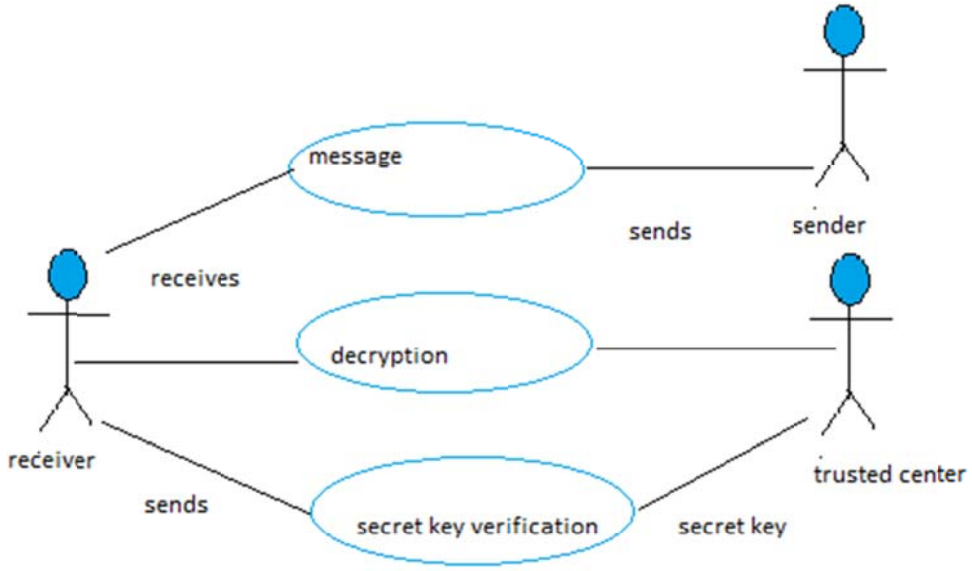
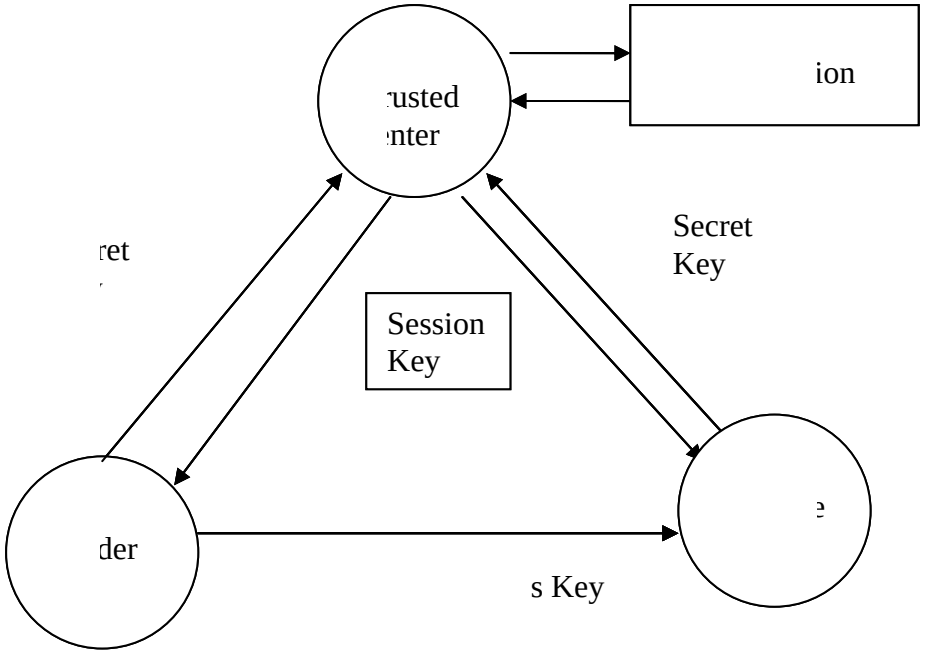


Diagram for receiver module

7. The main architecture of a system.

From the below pictorial representation we can clearly see how the sender shares hi secret key with the trusted center where the key generation takes place and is passed to the receiver .in the same way receiver can send a secret key to the trusted center and trusted center verifies it and generates a key and allows sender for secure transmission.

System Architecture:



8. Conclusion

The proposed System is very efficient and is secure. It cannot be attacked by the hackers and prevent passive attacks such as eavesdropping, man-in-the-middle and replay. And moreover the proposed system is an efficient, authenticated, scalable key agreement for large and dynamic multicast systems, which is based on the bilinear map. Compared with the Existing system, we use an identity tree to achieve the authentication of the group member. Since a large group is divided into many small groups. Each subgroup is treated almost like a separate multicast group with its own subgroup key. All the keys used in each subgroup can be generated by a group of KGC's in parallel. The intuitively surprising aspect of this scheme is that, even the subgroup controller aborts, it does not affect the users in this subgroup. Because every user in the subgroup can act as a subgroup controller. This is a significant feature especially for the mobile and ad hoc networks. From the security analysis we can see that our scheme satisfies both forward and backward secrecy. By introducing this system we can do secure transmission over insecure networks.

9. References

[1] J.T. Kohl, "The Evolution of the Kerberos Authentication Service, "EurOpen Conf. Proc., pp. 295-313, 1991.
[2] B. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Comm., vol. 32, no. 9, pp. 33-38, 1994.
[3] W. Stallings, Cryptography and Network Security: Principles and Practice 3/e. Prentice Hall, 2003.
[4] K.-Y. Lam and D. Gollmann, "Freshness Assurance of Authentication Protocols," Proc. European Symp. Research in Computer Security
(ESORICS '92), pp. 261-271, 1992.
[5] R. Shirey, Internet Security Glossary, IETF RFC 2828, May 2000.
[6] J. Nam, S. Cho, S. Kim, and D. Won, "Simple and Efficient GroupKey Agreement Based on Factoring," Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '04), pp. 645-654, 2004.
[7] H.A. Wen, T.F. Lee, and T. Hwang, "A Provably Secure Three-Party Password-Based Authenticated Key Exchange Protocol Using Weil Pairing," IEE Proc. Comm., vol. 152, no. 2, pp. 138-143,2005.
[8] J. Nam, S. Cho, S. Kim, and D. Won, "Simple and Efficient Group Key Agreement Based on Factoring," Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '04), pp. 645-654, 2004.