Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography

Dr.G.Ananda Rao
Department of Applied Mathematics
GITAM University, Vishakapatnam

Y.Srinivas
Department of Computer Applications
GITAM University, Hyderabad

J.Vijaya Sekhar
Department of Mathematics
GITAM University, Hyderabad

Ch.Pavan Kumar
Department of Computer Science & Engg.
GITAM University, Hyderabad

Abstract
Cryptography is the science of information security. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The combination of Implicit quantum key distribution protocol (3AQKDP) and explicit quantum key distribution protocol (3AQKDPMA) are used to form the new combination and demonstrate the following merits:
Establishment of a secure connection which can prevent attacks such as eavesdropping, man-in-the-middle and replay.
Reduction in communication rounds among existing QKDPs, improves efficiency of proposed protocols. A long term secret key can be used and shared between two parties repeatedly.
Classical cryptography methods currently used are unsafe and cannot detect the existence of passive attacks such as eavesdropping. Hence the combination of both classical as well as quantum cryptography is proposed.
KEYWORDS: 3AQKDP (implicit) /3AQKDPMA (explicit)/cryptography/Quantum Cryptography

1.INTRODUCTION

Quantum cryptography employs quantum mechanisms to distribute the session keys and public discussions to check for passive attacks such as eavesdroppers and to verify the correctness of a session key. Implicit quantum key distribution protocol (3AQKDP) provides a three party authentication with a secure session key distribution. In this system there is no mutual understanding between sender and receiver as they both communicate over a trusted center. While in explicit quantum key distribution protocol (3AQKDPMA) there is a mutual understanding between sender and receiver. Both sender and receiver should communicate directly with the authentication of trusted center.
KEY distribution protocols are used to facilitate the sharing of secret session keys between users on communication networks. By using these shared session keys, secure communication link is established over an insecure public networks. However, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key[1] is correct or fresh and a legitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocols in communication security is a top priority.
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.

2. METHODOLOGY

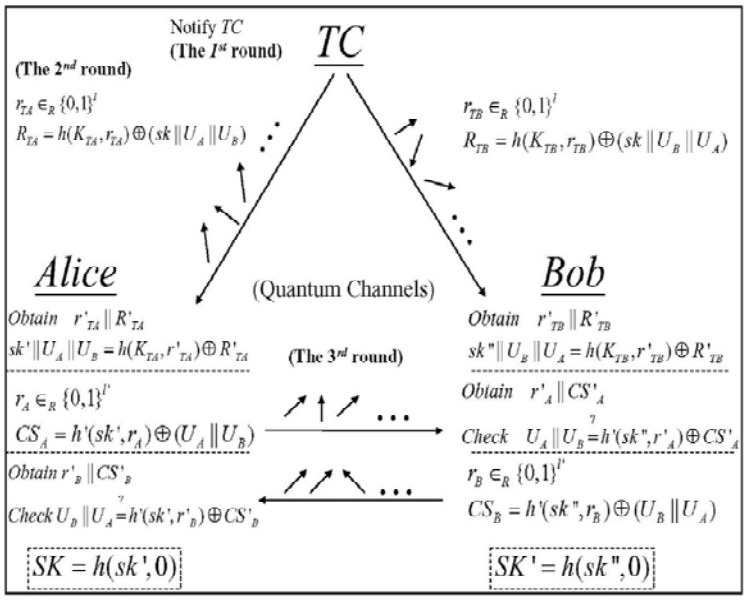
However, public discussions[2] require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication.
There are two types of Quantum Key Distribution Protocol, they are:

2.1 The Proposed 3AQKDP

This section 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.

2.2 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 preshare secret keys with the TC and agree to select polarization bases of qubits based on the preshared secret key. The Key Distribution Phase describes how the user and could share the session key with the assistance of TC and achieve the explicit user authentication.



3.ANALYSIS AND DESIGN

3.1Design Overview

3.1.1Sender Module

a)Secret key Authentication

The sender submits the secret key to the trusted center (TC), then the TC will verify the secret key and authenticate to the corresponding sender and gets the session key from TC, else TC doesn't 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.

3.1.2 Trusted Center

Secret Key Verification

Verify the secret key received from the user and authenticate the corresponding user for the secure transmission.

a) Session Key Generation

[3]It is a shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential values of random number.

b)Qubit Generation

To get the secret key and random string, then convert it into hex-code and then convert it into binary, find the least bit of the 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[4]

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
It's a technique to encrypt the session key by using the master key and store all the values to TC storage.

d)Key Distribution
It distributes the original session key and qubit to the sender for encrypting the message. It also distribute the key and qubit [5] to the corresponding receiver to decrypt the received messages

3.1.3Receiver Module

a)Secret key Authentication
It receives the encrypted message with hashed session key and qubit, then verifies the qubit with TC and generates the master key and reverses the hash, the session key and also reverse hash the session key from sender then compare the session key which improve the key authentication.

b)Decryption
Then finally decrypt the message using session key and show it to the user.

4.CONCLUSION

The Proposed system is an efficient, authenticated, scalable key agreement for large and dynamic multicast systems, which is based on the bilinear map. It also demonstrates the following merits, establishment of a secure connection which can prevent passive attacks such as eavesdropping, man-in-the-middle and replay attacks, reduction in communication rounds among existing QKDPs, improves efficiency of proposed protocols. A long term secret key can be used and shared between two parties repeatedly compared with the existing system; we use an identity tree to achieve the authentication of the group member. Further, it solves the scalability problem in multicast communications. Since a very large group is divided into many small groups each subgroup is treated practically 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.

5.REFERENCES

[1] G. Li, "Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations," Distributed Computing, vol. 9, no. 3, pp. 131-145, 1995.
[2] A. Kehne, J. Schonwalder, and H. Langendorfer, "A Nonce-Based Protocol for Multiple Authentications," ACM Operating Systems Rev., vol. 26, no. 4, pp. 84-89, 1992.
[3] M. Bellare and P. Rogaway, "Provably Secure Session Key Distribution: The Three Party Case," Proc. 27th ACM Symp. Theory of Computing, pp. 57-66, 1995.
[4] 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.
[5] 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.