ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Three Party Authentication for Key Distributed Protocol Using Classical and Quantum Cryptography

Dr. S.Thajoddin
Associate Professor in Mathematics,
Osmania College, Kurnool.

Arif Khan
Assistant Professor in Mathematics,
Osmania College, Kurnool.

ABSTRACT:

In the existing study of third party authentication, for message transformation has less security against attacks such as man- in-the-middle, efficiency and so on. In this approach, we at hand give a Quantum Key Distribution Protocol (QKDP) to safeguard the security in larger networks, which uses the combination of merits of classical cryptography and quantum cryptography. Two three-party QKDPs, one implemented with implicit user authentication and the other with explicit mutual authentication, which include the following:

1.Security against such attacks as the man-in-the-message, the resulting cipher text message is sent over the
2.Efficiency is improved as the proposed protocols contain the fewest number of communication rounds among the existing QKDPs.
3.Two parties can share and use a long-term secret (repeatedly).

To prove the security of the proposed schemes, this work also presents a new primitive called the Unbiased-Chosen Basis (UCB) assumption.

INTRODUCTION:

Computer networks are typically a shared resource used by many applications for many different purposes. Sometimes the data transmitted between application processes is confidential, and the applications would prefer that others be unable to read it. For example, when purchasing a product over the WWW (World Wide Web), users sometimes transmits their credit card numbers over the network. This is a dangerous thing to do since it is easy for a hacker to eavesdrop on the network and read all the packets that fly by. Therefore, users sometimes want to encrypt the messages they send, with the goal of keeping anyone who is eavesdropping on the channel from being able to read the contents of the message. The idea of encryption is simple enough. The sender applies an encryption functions to the original plain text network, and the receiver applies a reverse function known as the decryption to recover the original plain text. The encryption/decryption process generally depends on a secret key shared between the sender and the receiver. When a suitable combination of a key and an encryption algorithm is used, it is sufficiently difficult for an eavesdropper to break the cipher text, and the sender and the receiver can rest assured that their communication is secure. The familiar use of cryptography is designed to ensure privacy- preventing the unauthorized release of information and privacy. It also is used to support other equally important services, including authentication (verifying the identity of the remote participant) and integrity (making sure that the message has not been altered).

Classical Cryptography:

In classical cryptography, three-party key distribution protocols utilize challenge response mechanisms or timestamps to prevent replay attacks. However, challenge response mechanisms require at least two communication rounds between the TC and participants, and the timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to unpredictable nature of network delays and potential hostile attacks).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Furthermore, classical cryptography cannot detect the existence of passive attacks such as eavesdropping. On the contrary, a quantum channel eliminates eavesdropping, and therefore, replay attacks. This fact can then be used to reduce the number of rounds of other protocols based on challenge-response mechanism to a trusted center.

Quantum Cryptography:

In quantum cryptography, Quantum Key Distribution Protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the corrective ness 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. Previously proposed QKDPs are the theoretical design security proof and the physical implementation. A three-party QKDP proposed in requires that the TC and each participant preshare a sequence of EPR pairs rather than a secret key. Consequently, EPR pairs are measured and consumed, and need to be reconstructed by the TC and a participant after one QKDP execution.

The Preliminaries:

Two interesting properties, quantum measurement and no-cloning theorem on quantum physics, are introduced in this section to provide the necessary background for the discussion of QKDPs.

QKDP's Contributions:

As mentioned, quantum cryptography easily resists replay and passive attacks, where as classical cryptography enables efficient key verification and user authentication. By integrating the advantages of both classical and quantum cryptography, this work presents 2 QKDPs with the following contributions:
Man-in-the-middle attacks can be prevented, eavesdropping can be detected, and replay attacks can be avoided easily.

User authentication and session key verification can be accomplished in one step without public discussions between the sender and the receiver. The secret key preshared by a TC and a user can be long term which is repeatedly used. The proposed schemes are first probably secure QKDPs under the random oracle model. In the proposed QKDPs, the TC and a participant synchronize their polarization bases accordingly to a preshared secret key. During the session key distribution, the preshared secret key together with a random string are used to produce another key encryption key to encipher the session key. A recipient will not receive the same polarization qubits even if an identical session key is retransmitted. Consequently, the secrecy of the preshared secret key can be preserved and, thus, this preshared secret key can be long term and repeatedly used between the TC and the participant.

Due to the combined use of classical cryptographic techniques with the quantum channel, a recipient can authenticate user identity, verify the correctness and freshness of the session key, and detect the presence of eavesdroppers. Accordingly, the proposed communication rounds among existing QKDPs. The same idea can be extended to design of other QKDPs with or without a TC. The random oracle model is employed to show the security of the proposed protocols. The theory behind the random oracle model proof indicates that when the adversary breaks the three-party QKDPs, then a simulator can utilize the event to break the underlying atomic primitives. Therefore, when the underlying.

Quantum Measurement:

Let Tom and Tin be two participants in a quantum channel, where Tom is the sender of qubits and Tin is the receiver. The R basis and the D basis are required to produce or measure qubits. If Tom wants to send a classical bit b, then she creates a qubit and sends it to Tin, based on following rules.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

If b = 0 (1) and Tom chooses R basis, the qubit is ((|0)(|1)).

If b = 0 (1) and Tom chooses D basis, the qubit is ((√2 (|0) + (|1)) (√2 (|0) - (|1))).

When Tin receives the qubit, he randomly chooses an R basis or D basis and measures the cubit to get the measuring result лb. If Tin measures the qubit using the same basis as Tom, then лb = b will always hold; Otherwise, лb = b holds with a probability ½. Note that Tin cannot simultaneously measure the qubit in an R basis and D basis, and any eavesdropper activity identified be measuring the qubit will disturb the polarization state of that qubit.

No Cloning Theorem:

One cannot duplicate an unknown quantum state. i.e., a user cannot copy a qubit if he/she does not know the polarization basis of the qubit. Bases on this no cloning theorem, we propose the UCB assumption, in which one can identify the polarization basis of an unknown quantum state with a negligible probability to facilitate security proof of the proposed QKDPs.

Three-Party Authenticated Quantum Key Distribution Protocol (3AQKDP)

This section presents a 3AQKDP with implicit user authentication, which ensures that confidentiality is only possible for legitimate users and mutual authentication is achieved only after secure communication using the session key start. The proposed three-party QKDPs are executed purely in the quantum channel and this work does not consider errors caused by environmental noise. The following describes the notation, the first proposed 3AQKDP and its security theorem.

The following are the notations, proposed 3AQKDP:
R: The rectilinear basis, polarized with two orthogonal directions, (|0) and (|1).

D: The diagonal basis, polarized with two orthogonal directions,

((√2 (|0) + (|1)) and (√2 (|0) - (|1))). (1)

U_i: The k-bit identity of a participant.

In this paper, we denote U_A as the identity of Tom, U_B as the identity of Tin and U as a non-fixed participant.
h(.): The one-way hash function. The mapping of

$$h(.) \text{ is } \{0,1\}^* \rightarrow \{0,1\}^m \quad (2)$$

r_{TU}: An 1-bit random string chosen by the TC.6.
K_{TU}: The n-bit secret key shared between the TC and a participant, such that K_{TA} is the secret key shared between the TC and Tom. It should be noted that m = u + 2k.
Note that the bases R and D, the identity U_i, and the one-way hash function h(.) are publicly known parameters.

The Proposed 3AQKDP

Setup Phase

Let Tom and Tin be 2 users who would like to establish a session key:
K_{TU} is the secret key shared between TC and user U.
Bit sequence in K_{TU} is treated as the measuring bases between user U and the TC. If $(K_{TU})_i = 0$, the basis D is chosen; otherwise, the basis R. Note that $(K_{TU})_i$ denotes the ith bit of secret key (K_{TU}).

The following describes 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.

Key Distribution Phase

The following describes the details of key distribution phase. Assume that the TC has been notified to start the 3AQKDP with Tom and Tin. TC and the users have to perform the 3AQKDP as follows:

TC

- The TC generates a random number rTA and a session key SK. TC then computes

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

R_{TA} = $h(K_{TA},r_{TA})$ $K||U_A||U_B)$ for Tom and, similarly r_{TB} and

$R_{TB} = h(K_{TB},r_{TB})$ $(SK||U_B||U_A)$ for Tin.

2. The TC creates the qubits, Q_{TA}, based on $(r_{TA}||R_{TA})_i$ and $(K_{TA})_i$ for Tom where

i = 1;2;……..;n and $(r_{TA}||R_{TA})_i$ denotes the ith bit of the concatenation $r_{TA}||R_{TA}$.

If $(r_{TA}||R_{TA})_i=0$, $(K_{TA})_i=0$.

If $(r_{TA}||R_{TA})_i=0$, $(K_{TA})_i= 0$,
then $(Q_{TA})_i$ is $(1/\sqrt{2}(|0) + (|1))$. (3)

If $(r_{TA}||R_{TA})_i=1$, $(K_{TA})_i=0$,
then $(Q_{TA})_i$ is $(1/\sqrt{2}(|0) - (|1))$. (4)

If $(r_{TA}||R_{TA})_i = 0$, $(K_{TA})_i= 1$,

then $(Q_{TA})_i$ is $(|0)$. (5)

If $(r_{TA}||R_{TA})_i = 1$, $(K_{TA})_i= 1$,

then $(Q_{TA})_i$ is $(|1)$. (6)

TC then sends Q_{TA} to Tom. TC creates qubits Q_{TB} in the same way for Tin.

CONCLUSION:

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. Further, it solve the scalability problem in multicast communications. 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.

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.

[6] J.T. Kohl, "The Evolution of the Kerberos Authentication Service," EurOpen Conf. Proc., pp. 295-313, 1991.

[7] B. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Comm., vol. 32, no. 9, pp. 33-38, 1994.

[8] W. Stallings, Cryptography and Network Security: Principles and Practice 3/e. Prentice Hall, 2003.

[9] K.-Y. Lam and D. Gollmann, "Freshness Assurance of Authentication Protocols," Proc. European Symp. Research in Computer Security (ESORICS '92), pp. 261-271, 1992.

[10] R. Shirey, Internet Security Glossary, IETF RFC 2828, May 2000.