ISSN:0975-9646

Secured Communication Protocol via Encrypted Key Ensuring Message Integrity

DEVARAKONDA JOHN LIVINGSTONE, P.RAJA SEKHAR
Department of CSE, Avanthi College of Engg & Tech, Tamaram, Visakhapatnam, A.P., India

Abstract: The Secured communication protocol via encrypted key ensuring message integrity combination of Authentication of Third Party Authentication Quantum Key Distribute Protocol (implicit) and Third Party Authentication Quantum Key Distribute Protocol Mutual Authentication (explicit) quantum cryptography is used to provide authenticated secure communication between sender and Receiver. In quantum cryptography, quantum key distribution protocols 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. The advantage of quantum cryptography easily resists replay and passive attacks. A Third Party Authentication Quantum Key Distribute 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. In implicit quantum key distribution protocol Third Party Authentication Quantum Key Distribute have two phases such as setup phase and distribution phase to provide three party authentications 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 Third Party Authentication Quantum Key Distribute Mutual Authentication have phases such as setup phase and distribution phase to provide three party authentications with secure session key distribution. I have mutual understanding between sender and receiver. Both sender and receiver should communicate directly authentication of trusted center. Disadvantage of separate process 3AQKDP and 3AQKDPMA were providing the authentication only for message, to identify the security threads in the message. Not identify the security threads in the session key.

Keywords: **Quantum key distribution protocols (QKDPs), SCPEKMI, TC**

1. INTRODUCTION

Key distribution protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication is possible on insecure public networks .However, various security problems exist in poorly designed key distribution protocols; for example, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key is correct or fresh and alegitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocol sin communication security is a top priority. In some key distribution protocols, two users obtain a shared session key via a trusted center (TC). Since three parties (two users and one TC) are involved in session key negotiations, these protocols are called three-party key distribution protocols, as in contrast with two-party protocols where only the sender and receiver are involved in session key negotiations.

1.1 Contributions of This Work

As mentioned, quantum cryptography easily resists replay and passive attacks, whereas classical cryptography enables efficient key verification and user authentication. By integrating the advantages of both classical and quantum cryptography, this work presents two QKDPs with the following contributions:

1. man-in-the-middle attacks can be prevented, eavesdropping can be detected, and replay attacks can be avoided easily;
2. User authentication and session key verification can be accomplished in one step without public discussions between a sender and receiver;
3. The secret key pre-shared by a TC and a user can belong term (repeatedly used); and
4. The proposed schemes are first secured communication protocol via encrypted key ensuring message integrity under the random oracle model.

In the proposed QKDPs, the TC and a participant synchronize their polarization bases according to a pre-shared secret key. During the session key distribution, the pre shared secret keys 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 pre-shared secret key can be preserved and, thus, this pre-shared secret key can be long term and repeatedly used between the TC and 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 QKDPs require the fewest communication rounds among existing QKDPs. The same idea can be extended to the 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 primitives are secure, then the proposed three-party QKDPs are also secure.

2. QUANTUM MEASUREMENT

Let Alice and Bob be two participants in a quantum channel, where Alice is the sender of qubits and Bob is the receiver. The R basis and the D basis (defined in Section 3.1) are required to produce or measure qubits. If Alice wants to send a classical bit b, then she creates a qubit and sends it to Bob, based on the following rules:

1. If b=0(1) and Alice chooses R basis, the qubit is |0> (|1>).
2. If b=0(1) and Alice chooses D basis, the qubit is $1/\sqrt{2}$ (|0>+|1>) ($1/\sqrt{2}$ (|0>-|1>)).

When Bob receives the qubit, he randomly chooses an R basis or D basis and measures the qubit to get the Measuring result b'. If Bob measures the qubit using the same basis as Alice, then b'=b will always hold; otherwise, b'=b holds with a probability 1/2. Note that Bob cannot simultaneously measure the qubit in an R basis and D basis, and any eavesdropper activity identified by measuring the qubit will disturb the polarization state of that qubit .quantum state with a negligible probability to facilitate security proof of the proposed QKDPs.

3. SECURED COMMUNICATION PROTOCOL VIA ENCRYPTED KEY ENSURING MESSAGE INTEGRITY (SCPEKMI)

This section presents a Third Party Authentication Quantum Key Distribute Protocol 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 secured communication protocol via encrypted key ensuring message integrity and its security theorem.

3.1 Notation

1. R: The rectilinear basis, polarized with two orthogonal directions, |0> and |0>.
2. D: The diagonal basis, polarized with two orthogonal directions, $1/\sqrt{2}$(|0> + |1>) and $1/\sqrt{2}$(| 0>- |1>).
3. *Ui* : The *k*-bit identity of a participant. In this paper, we denote *UA* as the identity of *Alice*, *U*B as the identity of *Bob*, and *U* as a nonfixed participant.
4. h (.): The one-way hash function. The mapping of h(.) is $\{0,1\}^* \rightarrow \{0,1\}^m$.
5. r_{TU} : An l-bit random string chosen by the TC.
6. KTU: The n-bit secret key shared between the TC and a participant, such that KTA is the secret key shared between the TC and *Alice*. It should be noted that $n = l+m$
7. *SK*: The u-bit session key shared between legitimate participants in 3AQKDP. It should be noted that $m = u+2k$.

Here the bases *R* and *D*, the identity *Ui*, and the one-way hash function *h(.)* are public known parameters.

3.2 The Proposed SCPEKMI

This section describes the details of the SCPEKMI by using the notations defined in previous sections. Here, we assume

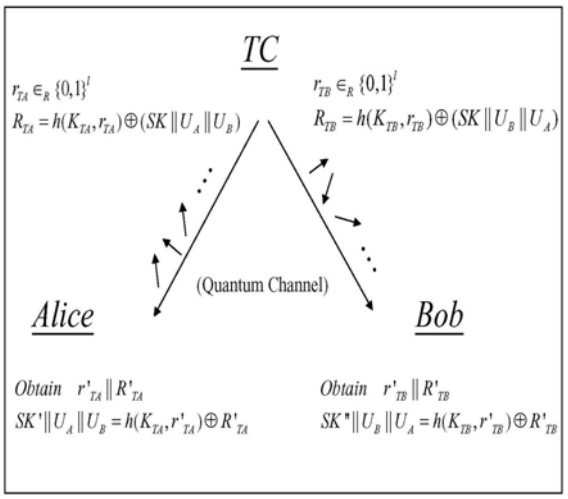

Fig. 1. The Key Distribution Phase of Encrypted message that every participant shares a secret key with the TC in advance either by direct contact or by other ways.

3.2.1 Setup Phase

Let Alice and Bob be two users who would like to establish a session key:

- KTU is the secret key shared between TC and user U.
- Bit sequence in KTU is treated as the measuring bases between user U and the TC. If (KTU)i = 0, the basis D is chosen; otherwise, the basis R. Notice that (KTU)i denotes the i_{TH} bit of the secret key KTU.

3.2.2 Encrypted Key Distribution Phase

The following describes the details of key distribution phase (see also Fig. 1). Assume that the TC has been notified to start the 3AQKDP with Alice and Bob. TC and the users have to perform the 3AQKDP as follows:

Trusted Center:

1. The TC generates a random number r_{TA} and a session key SK. TC then compute R_{TA}= h($K_{TA,}$ r_{TA}) XOR (SK||U_A||U_B) for Alice and, similarly, r_{TB} and R_{TB} = h($K_{TB,}$ r_{TB}) XOR (SK||U_B||U_A) for Bob.
2. The TC creates the qubits, Q_{TA}, based on (r_{TA} || R_{TA})$_i$ and (K_{TA})$_i$ for Alice 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 then (Q_{TA})$_i$ is $1/\sqrt{2}$ (|0>+|1>)
   - if (r_{TA} || R_{TA})$_i$ =1, (K_{TA})$_i$ =0 then (Q_{TA})$_i$ is $1/\sqrt{2}$ (|0>-|1>)
   - if (r_{TA} || R_{TA})$_i$ =0, (K_{TA})$_i$ =1 then (Q_{TA})$_i$ is |0>.
   - if (r_{TA} || R_{TA})$_i$ =1, (K_{TA})$_i$ =1 then (Q_{TA})$_i$ is |1>.

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

Users:

1. Alice measures the received qubits Q_{TA} depending on K_{TA}. If $(K_{TA})_i$ =0 , then the qubit is measured based on the basis D; otherwise, the basis R. Similarly, Bob measures the receiving qubits Q_{TB} depending on K_{TB}.
2. Once Alice obtains the measuring results $r'_{TA} \| R'_{TA}$,she then computes $SK'\|U_A\|U_B = h(K_{TA,} r'_{TA}) \text{ XOR } R'_{TA}$ .The session key SK' can be obtained and the values U_A and U_B can be verified. Similarly, Bob gains $r'_{TB} \| R'_{TB}$ and computes $SK"\| U_B\|U_A = h(K_{TB,} r'_{TB}) \text{ XOR } R'_{TB.}$ Then, Bob obtains the session key SK" and checks the correctness of U_B and UA.

In item 1 of TC, the hash value, $h(K_{TA,} r'_{TA})$ (or $h(K_{TB,} K_{TB})$), is used to encipher the sequence $SK\|U_A\|U_B$ (or $SK\| U_B\|U_A$). Therefore, a recipient will not receive the same polarization qubits even if an identical session key is retransmitted. This also makes an eavesdropper not be able to perform offline guessing attacks to guess the bases over the quantum channel and, thus, the secret key, K_{TA} (or K_{TB}), can be repeatedly used.

In item 2 of Users, only Alice (or Bob), with the secret key K_{TA} (or K_{TB}), is able to obtain $SK'\|U_A\|U_B$ (or $SK"\| U_B\|U_A$) by measuring the qubits QTA (or QTB) and computing $h(K_{TA,} r'_{TA}) \text{ XOR } R'_{TA}$(or $h(K_{TB,} r'_{TB}) \text{ XOR } R'_{TB}$. Hence, Alice (or Bob) alone can verify the correctness of the ID concatenation $U_A\|U_B$ (or $U_B\|U_A$).

4 Encrypted Key Distribution Protocol with Mutual Authentication (3QKDPMA)

In the previously proposed 3AQKDP, Alice and Bob cannot mutually authenticate each other until the session key is used in the further communications, i.e., implicit mutual authentication. In this section, an authenticator is added to the 3AQKDP so that the modified protocol 3QKDPMA can achieve explicit user authentication. The following presents protocol details.

4.1 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

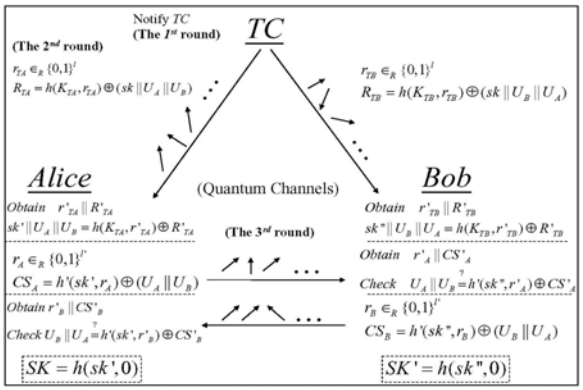

Fig. 2. The Key Distribution Phase of 3QKDPMA.

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.

4.1.1 Setup Phase

The setup phase is the same as in the SCPEKMI.

4.1.2 Key Distribution Phase

The following describes the details of key distribution phase (see also Fig. 2). Assume that the TC has been notified to start the 3QKDPMA with Alice and Bob (the first communication round). A communication round consists of all messages that can be sent and received in parallel within one time unit [1].

TC: (The Second Communication Round)

1. The TC generates an l-bit random number rTA and a u-bit sk. Moreover, TC computes. $R_{TA}= h(K_{TA,} r_{TA}) \text{ XOR } (SK\|U_A\|U_B)$ for Alice and, similarly, r_{TB} and $R_{TB} = h(K_{TB,} r_{TB}) \text{ XOR } (SK\|U_B\|U_A)$ for Bob.

2.The TC creates the qubits, Q_{TA}, based on $(r_{TA} \| R_{TA})_i$ and $(K_{TA})_i$ for Alice 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 then $(Q_{TA})_i$ is $1/\sqrt{2}$ (|0>+|1>)
- if $(r_{TA} \| R_{TA})_i$ =1, $(K_{TA})_i$ =0 then $(Q_{TA})_i$ is $1/\sqrt{2}$ (|0>-|1>)
- if $(r_{TA} \| R_{TA})_i$ =0, $(K_{TA})_i$ =1 then $(Q_{TA})_i$ is |0>.
- if $(r_{TA} \| R_{TA})_i$ =1, $(K_{TA})_i$ =1 then $(Q_{TA})_i$ is |1>.

QTB in the same way for Bob.

Users: (The Third Communication Round)

1. Alice measures the receiving qubits QTA depending on KTA. If (KTA)i =0, then the qubit is measured based on the basis D; otherwise, the basis R.Similarly, Bob measures the receiving qubits QTB depending on KTB.
2. Once Alice gains the measuring results r'TA || R'TA, she then computes sk'||UA||UB = h(KTA, r'TA) XOR R'TA .Then, Alice obtains sk' and verifies UA, UB. Similarly, Bob gains r'TB || R'TB and computes sk''||UB||UA = h(KTB, r'TB) XOR R'TB .Then, Bob obtains sk'' and checks the correctness of UB, UA.
3. Alice generates the l'-bit random number rA and computes CSA=h'(sk', rA) XOR (UA||UB). Similarly,Bob generates rB and computes CSB=h'(sk", rB) XOR (UB||UA).
4. Alice creates the qubits based on (rA || CSA)i and (sk')i and i = 1; 2; . . . ; u. It should be noted that u=l'+2k.
   - if (rA || CSA)i =0 and (sk')i =0 , the qubit is $1/\sqrt{2}$ (|0>+|1>)
   - if (rA || CSA)i =1 and (sk')i =0 , the qubit is $1/\sqrt{2}$ (|0>-|1>)
   - if (rA || CSA)i =0 and (sk')i =1 , the qubit is |0>.
   - if (rA || CSA)i =1 and (sk')i =1 , the qubit is |1>.

Then, Alice sends the u qubits to Bob. Similarly,Bob creates qubits for Alice based on rB ||CSB and sk".

5. Once they've received the qubits, Alice and Bob measure the qubits depending on (sk')i and (sk")i respectively.
6. Alice gains r'B || CS'B and checks whether UB||UA=h'(sk',r'B) XOR CS'B , r'B≠rA .If the equation holds the Alice will compute the session key SK=h(sk',0).Similarly, Bob checks whether UA||UB=h'(sk",r'A) XOR CS'A , r'A≠rB and then builds the session key SK'=h(sk",0).

Items 1 and 2 of TC and Users in 3QKDPMA are similar to those in 3AQKDP. In item 3 of Users in 3QKDPMA, the hash value, h'(sk',rA) h'(sk',rB) is used to encrypt the concatenation UA||UB (or UB||UA). Thus, Bob (or Alice) will not receive the same polarization qubits even if a retransmission of qubits from Alice (or Bob) is required. Consequently, an eavesdropper will not be able to perform offline guessing attacks to guess the bases over the quantum channel.

Moreover, the checksum CSA prepared by Alice is different from CSB prepared by Bob. Thus, an adversary cannot intercept qubits sent from Alice (or Bob), reflect these qubits to Alice (or Bob) and pass the authentication in item 6 of Users. Besides, CSA (or CSB) is used for the explicit user authentication that Alice (or Bob) alone can authenticate Bob (or Alice) and detect eavesdroppers.

4.2 Comparison between 3QKDPMA and Other Protocols

This section compares the properties of 3QKDPMA with those of other three-party key distribution protocols, which also achieve explicit mutual authentication without considering the hardware costs for the quantum channel (see Table 1).

Among classical three-party key distribution protocols

Focuses on the low bounds of communication rounds of three-party key distribution protocols, such as the low bound of timestamp-based protocols (Case 2) and the low bound of nonce-based protocols (Case 8). Therefore, this work compares the communication rounds for and with the proposed protocol. Additionally, is the only three party QKDP that allows explicit mutual authentication and, thus, is chosen for comparison. The three-party QKDP in avoids passive and replay attacks due to the quantum phenomena. Zeng and Zhang use preshared EPR pairs between the TC and participants to prevent man-in-the-middle attacks. However, not only must participants perform public discussions to verify the correctness of the session key but the preshared EPR pairs must be reconstructed for each session. The classical three-party key distribution protocols utilize challenge-response mechanisms or timestamps to prevent replay attacks, such as in Case 8 (or Case 2) of [1]. However, challenge-response mechanisms require at least two communication rounds between the TC and participants, and clock synchronization is impractical. Furthermore, classical cryptography cannot detect passive attacks such as eavesdropping.

By integrating the advantages of both the classical and quantum cryptographies, the proposed 3QKDPMA can avoid man-in-the-middle, passive, and replay attacks. Furthermore, since the challenge-response mechanism is no longer necessary, the number of communication rounds in 3QKDPMA is reduced to three, the same as the low bound in the timestamp-based protocol (Case 2), and one fewer than the low bound of the challenge-response protocol (Case 8) in [1]. Furthermore, the secret key preshared between the TC and a participant is long-term in 3QKDPMA, whereas the EPR pairs shared between TC and a participant are temporary.

TABLE 1
Comparison among 3QKDPMA and Other Protocols

	3QKDPMA	ZZ00 [15]	Case 8 of [1]	Case 2 of [1]
Cryptographic Mechanism	Quantum+Classical	Quantum	Classical	Classical
Pre-shared Secret Key	Long-termed	EPR pairs	Long-termed	Long-termed
Communication Rounds	3	6	4	3
Quantum Channel	Y	Y	N	N
Clock Synchronization	N	N	N	Y
Vulnerable to man-in-the-middle Attack	N	N	N	N
Vulnerable to Passive Attack	N	N	Y	Y
Vulnerable to Replay Attack	N	N	N	N
Formal Security Proof	Y	N	N	N

5 Conclusions

This study proposed two three-party QKDPs to demonstrate the advantages of combining classical cryptography with quantum cryptography. Compared with classical three-party key distribution protocols, the proposed QKDPs easily resist replay and passive attacks. Compared with other QKDPs, the proposed schemes efficiently achieve key verification and user authentication and preserve a long term secret key between the TC and each user. Additionally, the proposed QKDPs have fewer communication rounds than other protocols. Although the requirement of the quantum channel can be costly in practice, it may not be costly in the future. Moreover, the proposed QKDPs have been shown secure under the random oracle model. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDPs.

Acknowledgments

The authors would like to thank the anonymous reviewers for their very helpful and valuable comments to enhance the clarity of the manuscript.

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.

Mr. D. John Living Stone received the MCA Post Graduate degree from the Department of Computers, from Andhra University, in 2005 and He is currently pursuing M.Tech in the Department Of Computer Science and Engineering, Avanthi Institute of Engineering and Technology, Vishakhapatnam, JNT University His research interests include computer Networking.

Mr. P.Rajsekhar M.Tech degree from the Department of Computer Science and technologyG.I.T.MUniversity, Vishakhapatnam, in 2009 and working as a Asst. Prof in Avanthi Institute of Engineering and Technology, Vishakhapatnam His research interests include data mining.