IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010
ISSN (Online): 1694-0814
www.IJCSI.org

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

Suganya Ranganathan[1], Nagarajan Ramasamy[2] , Senthil Karthick Kumar Arumugam[3], Balaji Dhanasekaran[4], Prabhu Ramalingam[5], Venkateswaran Radhakrishnan[6], and Ramesh Karpuppiah[7]

Assistant Professor's, Master Of Computer Applications, Bharathiar University, Nehru College Of Management Coimbatore, Tamilnadu 641105, India.

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-middle, eavesdropping and replay.
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.

Keywords: *.Third Party Authentication, QKDP, Preliminaries, 3AQKDP, Unbiased-Chosen Basis, Eavesdropping and Replay Efficiency.*

1. 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 message, the resulting cipher text message is sent over the 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).

2. Key Distribution Protocol and Its Mechanism with Classical & Quantum Cryptography

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 a legitimate participant cannot confirm the identity of other participant. Designing secure key distribution protocols in communication security is a top priority. In some key distribution protocols, two users obtain a shared session key via a Trusted Centre (TC). Since three parties (two users and one TC) are involved in session key negotiations, these protocols are called third-party key distribution protocols, as in contrast with two-party protocols where only the sender and receiver are involved in session key negotiations.

2.1 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). 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.

2.2 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.

3. 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

primitives are secure, then the proposed three-party QKDPs are also secure.

4. 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.

4.1 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.

- 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 љ. If Tin measures the qubit using the same basis as Tom, then љ = b will always hold; Otherwise, љ = 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.

4.2 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.

5. 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.

6. The Proposed 3AQKDP

6.1 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.

6.2 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:

6.2.1 TC

1. The TC generates a random number r_{TA} and a session key SK. TC then computes

$$R_{TA} = h(K_{TA}, r_{TA}) \oplus (SK||U_A||U_B)$$

for Tom and, similarly r_{TB} and

$$R_{TB} = h(K_{TB}, r_{TB}) \oplus (SK||U_B||U_A)$$

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

6.2.2 Users

- Tom measures the received Q_{TA} qubits depending on K_{TA}. If $(K_{TA})_i=0$, then the qubit is measured based on the basis D. otherwise, the basis R. Similarly, Tin measures the receiving qubits Q_{TB} depending on K_{TB}.
- Once Tom obtains the measuring results $r'_{TA}||R'_{TA}$ she then computes $SK'||U_A||U_B=h(K_{TA},r'_{TA}) \oplus R'_{TA}$ (7)

The session key SK' can be obtained and the values U_A and U_B can be verified. Similarly Tin gains $r'_{TB}||R'_{TB}$ then, Tin obtains the session key SK" and checks the correctness of U_B and U_A. In item 1 of TC, the hash value, $h(K_{TA},r_{TA})$ (or $h(K_{TB},r_{TB})$), 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 Tom (or Tin), 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 Q_{TA} (or Q_{TB}) and computing $h(K_{TA},r'_{TA}) \oplus R'_{TA}$ (or $h(K_{TB},r'_{TB}) \oplus R'_{TB}$). Hence, Tom (or Tin) alone can verify the correctness of the ID concatenation

$$U_A||U_B \text{ (or } U_B||U_A)$$

7. Security Proof of 3AQKDP

This section presents a theorem to demonstrate the security of 3AQKDP. A new primitive, Unbiased-Chosen Basis (UCB) assumption, based on the non-cloning theorem is used to facilitate the proof. The UCB assumption describes that one can distinguish the polarization basis of an unknown quantum state with only a negligible probability.

Theorem

- Let $adv^{AQKD}_{3AQKDP}(A)$ be the advantage in breaking the AQKD security of 3AQKDP.
- Let $adv^{UCB}_{\Delta}(\Delta)$ be the advantage in breaking the UCB assumption used in 3AQKDP.

If the adversary A breaks the AQKD security of 3AQKDP after q_{ini} Initiate queries, q_{se} Send queries and q_h Hash queries within time t, a UCB assumption attacker Δ will have an advantage to break the UCB security of ψ. That is,

$$adv^{AQKD}_{3AQKDP}(A) \le 2(q_{ini} + q_{se})^2/q_{ini} \cdot adv^{UCB}_{\Delta}(\Delta)$$

Where $t' \le t + q_{ini}\, T_{rn}$: T_{rn} is the time to generate a random number.

8. Conclusion

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 replays and passive attacks. This proposed scheme efficiently achieves key

verification and user authentication and preserves a long term secret key between the TC and each user. Additionally, the requirement of 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.

References

[1] G.Li "Efficient network authentication protocols: Lower bounds and Optimal implementations", Distributed computing, Vol 9, No. 3 pp.1995.
[2] J.T.Kohi, "The evolution of the Kerberros Authentication Service" European conf. proc pp 295-313-1991. B.Nuemann and T. Ts'o "Kerberros" An authentication service for computer networks" IEEE comm., Vol 32, No.9 pp33-38 1994.
[3] W.Stallings, Cryptography and network security: principles and practice, prentice hall 2003.
[4] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, "Reversibility of local transformations of multiparticle entanglement", quant-ph/9912039
W. Dür, J. I. Cirac, and R. Tarrach, "Separability and distillability of multiparticle quantum systems", Phys. Rev. Lett. 83, 3562 (1999)
[5] Ll. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Unconditional security of key distribution from causality constraints", quant-ph/0606049
[6] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer", Lecture Notes in Computer Science 576, 351 (1991)
[7] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem", Phys. Rev. Lett. 83, 3081 (1999)
[8] P. W. Shor, "Equivalence of additivity questions in quantum information theory", Commun. Math. Phys. 246, 453 (2004)
[9] M. B. Hastings, "A counterexample to additivity of minimum output entropy", Nature Physics 5, 255 (2009)

Suganya Ranganathan is pursuing her Ph.D at Karpagam University. She holds her MCA degree from Anna University, Chennai. Also completed her B.Sc Computer Science degree from Bharathiar University, Coimbatore. Being her research area is in Software Testing she also has interest on Security Oriented networks, Digital Image Processing and whole of Software Engineering. She was working as a Software Engineer in UST-Global for 2 years. And recently entered into academics with 1 year of teaching experience. Organized and also presented papers in national level conferences.

A.Senthil Karthick Kumar is a Ph.D. Research Scholar. He completed his B.Sc in Information Technology from Madurai Kamaraj University in 2003. Did his MCA from Bharathiar University in 2006; M.Phil in Computer Science in 2010. He is Pursing MBA in Human Resource Management, from Bharathiar University through DDE. Prior to joining in NCM he worked for 3 years as a Human Resource Technical Staffing Person in various companies like (Perot Systems), Bangalore. Currently he is working as an Assistant Professor in Nehru College of Management, Coimbatore under Bharathiar University. He enrolled his Life time Member ship with ISTE, and Member in CSI. He has published and presented around 10 papers in National level Seminars. His interest in research area includes Cloud computing, Mobile computing (security).

R. Prabhu is pursuing his Ph.D. He received his professional degree M.C.A, in Computer Applications and also completed his B.Sc in Computer Science from Bharathiar University, Tamilnadu, India. Previously he worked as Technical Recruiter for 2 years. Currently working has as an Asst. Professor of Computer Applications, Nehru College of Management, Coimbatore, Tamilnadu, India from the year 2010. He presented & published papers more than 5 papers in National level seminar. His area of interest in research is Cryptography and Network Security, Information Security, Software Engineering.

R. Nagarajan is pursuing his Ph.D. He completed his Post graduate degree in MCA in computer Applications in Bharathidasan University, and he completed his B.Sc in Applied Science (Faculty of Engineering) from Bharathiar University. He has 20 years of experience as Manager-Operations in Bannari Amman Group. Currently working has as an Asst. Professor of Computer Applications, Nehru College of Management, Coimbatore, Tamilnadu, India from the year 2009.Currently He is concentrating on Space Communications using Optic Techniques. He presented & published papers more than 6 papers in National level seminar. His area of interest in research is Cryptography and Network Security, Information Security, Robotics.

Dr.D.Balaji presently working as a Director – Department of Computer Applications, Nehru College of Management, Coimbatore. He has graduated from Madura College, Madurai, which was established in the year 1887. He has completed his post graduation from the Computer centre, Madurai Kamaraj University. He has also completed M.Phil, and M.B.A., from Madurai Kamaraj University. He has completed Ph.D titled "Project Based Organizational Teaching and Learning". He is having overall 13 years of academic experience. He has worked for University of Bedfordshire, UK for 7 years and 1 year for ABB India limited. He has published his research work in 2 international journals, and presented 9 papers in the International conferences and 14 papers in the national conferences. His area of specialization is IT applications in Higher Education and Programming Languages. He has visited many countries like Romania, Jordan, Srilanka, Malaysia, etc., for his research work.

Venkateswaran Radhakrishnan pursing Ph.D currently in the Karpagam Academy of higher Education, Karpagam University, Tamilnadu, India, in the field of Cryptography and Network Security. He received his professional degree M.C.A, in Computer Applications and also completed his MBA (Information Technology) from Bharathiar University, Tamilnadu, India, and he received his M.Phil Degree in Computer Science from Bharathidasan University, Tamilnadu, India. He has also worked as an Asst. Professor of Computer Applications, Nehru College of Management, Coimbatore, Tamilnadu, India from the year 2006. He is the institution member of Computer Society of India. He published papers in International Journals and Conferences and also presented paper in more than 10 national seminars and conferences. His research interest area in Cryptography and Network Security, Information Security, Software Engineering, and Relational database Management Systems.

Ramesh Kumar.K pursing M.B.A at M.S University, Tirunelveli. Completed his B.E in Computer Science at Anna University. He has experience in teaching for 2 yrs at NCM, Coimbatore and Worked as Software Engineer and has 3yrs of experience in Jayakailash group of companies and also 2 yrs of experience in solid solutions. He has interest on Asp .net, C, C++, Java, Data

mining and Data Structures. He has also attended many conferences and done certification courses which will support the carrier growth.