Secure Communication Using Two Party Authenticated Quantum key Distribution Protocols

S.Venkatramulu[†], S.Veena[††]

[†]Department of Computer Science and Engineering,
[††]KakatiyaInstitute of Technology and Science, Warangal-506002

Abstract
This work presents quantum key distribution protocols (QKDPs) to safeguard security in large networks, efficiency is improved as the proposed protocols contain the fewest number of communication rounds and two parties can share and use a long-term secret Key. Quantum cryptography is basically based on a trusted channel in communication between two parties compared to classical channel. Recently, Quantum Key Distribution (QKD) has become more secure transmission method used to transmit secret key between two legitimate parties. This paper discusses the implementation of (QKD) protocol with the existence of an eavesdropper. The implementation simulates the communication of two parties who wish to share a secret key with the existing of eavesdropper. The existing of eavesdropper is simulated with two kinds of attacks, which is used as parameter to measure the length of final key agreed by both authenticated parties at the end of the communication.

Keywords:
simulate attacks, provable security, Quantum cryptography, two-party key distribution protocol, provable security.

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. Secure communication link has widely become the most important method of today's modern society and their developments are increasing dramatically [14]. The use of secure link has relied on the confidentiality and security of its data transmission. The communication between two parties using the insecure (public) channel to exchange data is easy enough to the intruders who wish to get the information about the exchanging data. In two-party key distribution protocols only the sender and receiver are involved in session key negotiations. Two of the most important problems in cryptography are concerned with the security and authenticity of exchanged message. Assume that two parties named Alice and Bob wishing to transmit the data to each other. Alice and
Bob should make sure that any potential intruders did not successfully achieve the information of the key. This is where the key distribution step is used to Alice and Bob to establish a secret key prior to exchange any message within the public channel. Quantum key distribution (QKD) protocols provide a way for two parties, a sender, Alice, and a receiver, Bob, to share an unconditionally secure key in the presence of an eavesdropper, Eve. In some key distribution protocols, two users obtain a shared session key via a trusted center (TC)[14]. A uantum channel eliminates eavesdropping, unlike conventional schemes of key distribution, the security of QKD protocols is guaranteed by the principles of quantum mechanics. In conventional scheme, one can only hope that the eavesdropper simply does not have enough computational resource to gain knowledge of the information in transit.

2 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.

2.1 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 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

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

the polarization state of that qubit.

2.2 No-Cloning Theorem

In 1982, Wootters and Zurek proved that one cannot duplicate an unknown quantum state; that is, a user cannot copy a qubit if he/she does not know the polarization basis of the qubit. Based 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.

3 The Proposed theory

This section presents the notations used for bits while they are transmitted in quantum channel. The proposed two-party QKDPs are executed purely in the quantum channel and this work presents secure communication of information even with the existence of an eavesdropper. The following describes the notations used for transmission of bits:

3.1 Notation

1. R: The rectilinear basis, polarized with two orthogonal directions |0> (|1>).
2. D: The diagonal basis, polarized with two orthogonal directions 1/sqrt (2) (|0>+|1>) 1/sqrt (2) (|0>-|1>).
3. U_i: The k-bit identity of a participant. In this paper, we denote U_A 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.
5. SK: The u-bit session key shared between legitimate participants. 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 public known parameters.

3.2 Quantum Key Distribution

In classical cryptography, 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 participants, and the 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. 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 which are based on challenge-response mechanisms. Here in his paper we are going to show how secure communication is possible using quantum channel even with the existence of an eavesdropper.

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 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.

Quantum cryptography differs from the classical cryptography because it is focus on the physic of information. The process of sending and storing information in quantum cryptosystem are carried out by physical means, for example in optical fiber in electric current. It uses secure channel (e.g.: optical fiber)[15] to transmit a polarized photon which then will create the secret key. This secret key generated from a form of a random string of bits. These bits then will be used as a secret key in a conventional cryptography scheme. The coding schemes used according to BB84 protocol [15] are four non orthogonal polarization states (0°, 90°, 45° and - 45°) that will polarize each of the photon that will be transmitted. In this protocol, Alice and Bob have to communicate within two channels, Quantum channel (e.g.: optic fiber or free space) and public channel (e.g.: Internet) to share a secret key. First, Alice and Bob have to communicate (one way communication) via Quantum channel, and then they both will establish connection within public channel (two way communication). It works as follows:

1) Via Quantum Channel a) Alice will send polarize photons (measure as bit) to Bob using the Quantum channel.

b) After all the photon transmission finished, Bob will measure the bits he received using the rectilinear or diagonal basis.

2) Via Public Channel a) They both will establish a communication via a public channel. Bob will announce his measurement (states) at the public channel with or without the presence of Eve.

b) Alice will reply the correct measurement that Bob have measure with or without presence of Eve.

c) Alice and Bob now share a raw key, which is considered not fully secret, bits maybe tampered by Eve during the transmission.

d) They both then will continue to communicate in public channel to find and correct the bits that they have by these 4 processes:

- Shifting Raw Key
- Error Estimation

• Error Correction
• Privacy Amplification

4. Types of Attack

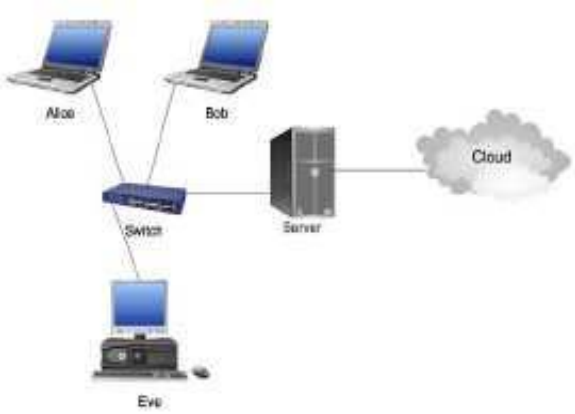
A. Intercept/Resend
Intercept/resend attacks are where Eve intercepts (tapping) pulse from the sender and read them in her chooses bases. The eavesdropper Eve measures each pulse which measure as ubits in one of the two bases precisely as Bob doe s. Then, Eve will pretend as Alice and resend to Bob another qubits in the state corresponding to her measurement result. The use of two bases gives Eve chances to get half of her measurement compatible with the state prepared by Alice. In this case, Eve will successfully resend to Bob a qubit in the exact state as Alice does without traces of eavesdropping. In another remaining case, Eve will unfortunately measure the qubits mismatched with as have been prepared by Alice. Eve works same as Bob, which they both did not know the random-number generator that Alice used. So, they both will have the equal chance to measure the ubits send by Alice.
B. Beam Splitting
In practical quantum cryptography, it is very difficult to prepare precise calculation of one-photon states. Coherent state are use to represent average photon number below than one. More than one photon may appear in some pulses impact of use the coherent states. Because of this, Eve can have the opportunities to split the signal and learn partial information on the key without disturbing the transmission from Alice to Bob. Number of bits Eve can gain is same as Alice, which is average of one half of the number of all pulses containing more than one photon.

5. Implementation

A. Software Structure
For the implementation, Alice and Bob will communicate within Quantum channel and public channel with or without the presence of Eve. This software works in two Channels, Quantum channel and public channel. Alice play as the sender role, Bob as the receiver and Eve as the eavesdropper. This software consists of 5 objects, which are Alice, Bob, Eve, Quantum channel and Public channel. Alice is a sender who will provide (transmit) bits to Quantum channel.
This Quantum channel acts just like the physical implementation, which is if there is a tap from eavesdropper, the bits will be changed. Assuming that Alice wants to transmit bits to Bob without any knowledge of the Eve's existence, Bob then reads the Quantum channel object to retrieve the bits either it have been modify by Eve or it is originally from Alice. Alice and Bob then communicate in public channel to find error bits and correct it. Bob use public channel object to communicate with Alice with existence of Eve. But, at the public channel, Eve only can observe the communication; no modification will be made by Eve
In this implementation, devices that have been used are:
• 3 workstations.
• 1 switch

Figure 1: Hardware Implementation

knowledge of the Eve's existence, Bob then reads the



Quantum channel object to retrieve the bits either it have been modify by Eve or it is originally from Alice. Alice and Bob then communicate in public channel to find error bits and correct it. Bob use public channel object to communicate with Alice with existence of Eve. But, at the public channel, Eve only can observe the communication; no modification will be made by Eve
In this implementation, devices that have been used are:
• 3 workstations.
• 1 switch
All devices are setup in the same room. Switch are use to connect all workstations. Each workstation represents Alice, Bob and Eve respectively. Static IP are used so that all workstation can communicate via the switch. So, Eve will recognize Alice and Bob by their IP addresses.
B. Hardware Setup
Developed software is installed on each of workstations to simulate the protocol.
C. The Protocol
For this simulation, each of object (Alice, Bob, Eve) play different role. Only the appropriate function is executed on each of workstation, depending on its role. The Quantum channel and public channel objects are executed on Alice's, while Eve and Bob objects are execute on different workstation respectively. This program works as follow:

1) Alice generated a length (k) of random number (0 & 1) then sends it on Quantum channel object to be 'read' by Bob and Eve.
2) If there is eavesdropping from Eve, Eve is the one who have to 'read' the Quantum channel object first. Eve can
modify the bits with two kind of attacks; intercept/resend or beam splitting.
3) Then, Bob reads the updated version from Quantum channel object, assuming that Bob doesn't know about the tapping from Eve.
4) Bob then measure the bits he 'read' from Quantum channel object with his selected own bases. Then, Bob 'announces' the bases he made to Alice via public channel, which located at Alice's.
5) Sifting raw key begin, Alice 'read' Bob's measurement at public channel object and 'confirm' to Bob the position Bob has measured in the right bases (m bits) by announcing it at public channel.
6) Next, Alice and Bob estimate error to detect eavesdropper. They both calculate and compare their bits error rate (e). If they found that their error rate is higher than maximum bits error rate (e>emax), they will suspend the communication and start all over again. (emax has predetermined value) 7) Now, both Alice and Bob will have a shared key, which is called 'raw key'. This key is not really shared since Alice and Bob's version are different. They eliminate the m bits from the raw key.
8) Both Alice and Bob then perform 'error correction' on their raw key to find erroneous bits in uncompared parts of keys and 'privacy amplification' to minimize the number of bits that an eavesdropper knows in the final key.
9) Finally, they both will get a same string of bits, which is the shared secret key.

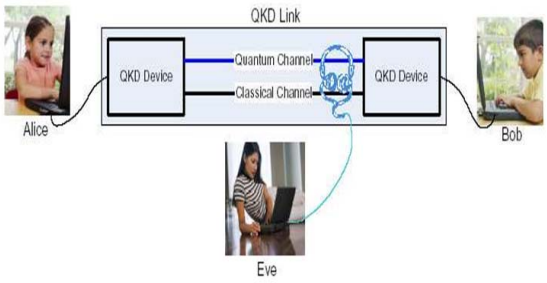
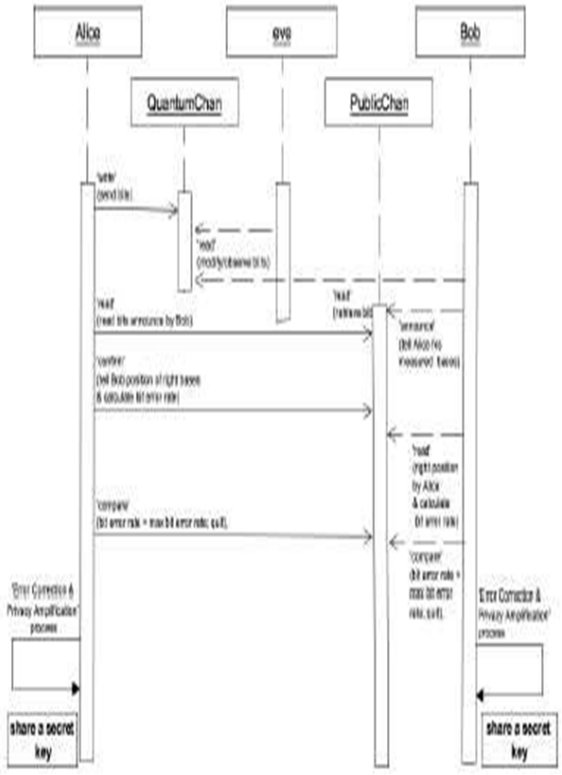


Figure 3 Structure of QKD link

Here we can describe the structure and the principle of operation of the basic practical QKD system: a QKD link. As depicted on Fig. 3 a QKD link is a point-to-point connection between two users, commonly called Alice and Bob that want to share secret keys. The QKD link is constituted by the combination of a quantum channel and a classical channel. Alice generates a random stream of classical bits and encodes them into a sequence of nonorthogonal quantum states of light, sent over the quantum channel. Upon reception of those uantum states, Bob performs some appropriate measurements leading him to share some classical data correlated with Alice's bit stream. The classical channel is then used to test these correlations. If the correlations are high enough, this statistically implies that no significant eavesdropping has taken place on the quantum channel and thus that with very high probability, a perfectly secure symmetric key can be distilled from the correlated data shared
by Alice and Bob. In the opposite case, the key generation process has to be aborted and started again. QKD is a symmetric key distribution technique. QKD requires, for authentication purposes, that Alice and Bob share, in advance, a short secret key (whose length scales only logarithmically in the length of the secret key generated by a QKD session. QKD systems are being developed with an increasing reliability and with increasing performances.

Figure 2: Software Protocol



D. Measurement
This simulation program measures the key length of the raw key and secret key depending on different kinds of attacks by Eve:

1) No Attack: When there is no attack, Eve didn't do anything; Bob receive all bits as send by Alice. Alice will send all her generated bits to Quantum channel to be 'read' by Bob.
2) Beam Splitting: When Eve attempts beam splitting, it returns either 0 or 1 randomly, we assume that beam in Quantum channel have been split successfully. This will randomly change bits that have been written by Alice in Quantum channel according to how strong mirror strength have been set by Eve to split the beam (bits actually).
3) Intercept/resend: In this attack, Eve has to read all the bits that have been written by Alice, Eve then should continue such sending new string of random bits as long as Alice does. Practically, Alice and Bob can detect 25% of error rate in their sifted key and Eve can get 50% information from Alice. But, because we use random bits generated by Eve, it will depend on the result when Bob and Alice compare their bits.

6. Conclusion

This study proposed two-party QKDPs to demonstrate the advantages of combining classical cryptography with uantum cryptography. Compared with classical cryptography the proposed QKDP easily resist replay and passive attacks. Compared with other QKDPs, the proposed scheme efficiently achieve key verification and user authentication and preserve a long-term secret key shared between users on communication network. 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. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDPs.
In this software development, it is clearly shown the function of Quantum Key distribution Protocol with the existence of eavesdropper. This simulation is driven to give an alternative to physical implementation of the protocol. From the result that has been generated, we can see that different type of attack does affect the final bits length of the input. Thus the erroneous bits error indicate that this kind of attacks affect the protocol efficiency.
Quantum cryptography offers the promise of unconditional security without face-to-face exchanges. Rather than relying on problems believed to be computationally "difficult," quantum cryptography uses basic physical laws to provide provable unconditional security. It is impossible for anyone to eavesdrop on a quantum key exchange and copy the key without being detected.

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] C.H Bennet and G.Brassard "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceeding of IEEE International Conference on Computer System and Signal Processing, Bangalore India, December 1984, pp 175- 179.
[11] Nicolas Gisin,Gre' goire Ribordy, Wolfgang Tittle,and Hugo Zbinden, "Quantum cryptography", Reviews of Modern Physics, Volume 74, January 2002.
[12] Miloslav Dusek, Ondrej Haderka, Martin Hendrych, "Generalized beam-splitting attack in quantum cryptography with dim coherent states", Optics Communication 169 (1999), 103-108.
[13] C.H Bennet et al.,"Experimental Quantum Cryptography," J.Cryptology, vol. 5, no. 1, 1992, pp.3-28.
[14] Tzonelih Hwang, Kuo-Chang Lee, and Chuan-Ming Li "Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols", IEEE transactions on dependable and secure computing, vol. 4, no. 1, january-march 2007
[15] Nur Atiqah Muhammad, Zuriati Ahmad Zukarnain, "Implemetation of BB84 Quantum Key Distribution Protocol's with Attacks" ,European Journal of Scientific Research ISSN 1450-216X Vol.32 No.4 (2009), pp.460-466
[16] D. Mayers, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channel," Proc. Advances in Cryptology (CRYPTO '96), pp. 343-357, 1996.
[17] D. Gottesman and H.-K. Lo, "Proof of Security of Quantum Key Distribution with Two-Way Classical Communications," IEEE Trans. Information Theory, vol. 49, p. 457, 2003.

[18] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," J. Cryptology, vol. 5, pp. 3-28, 1992.
[19] P.D. Townsend, "Secure Key Distribution System Based on Quantum Cryptography," Electronics Letters, vol. 30, pp. 809-811, 1994.
[20] R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, and C. Simmons, "Quantum Cryptography over Underground Optical Fibers," Proc. Advances in Cryptology (CRYPTO '96), pp. 329-342, 1996.