Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Using BB84 Quantum Key Distribution Protocols

D N Kartheek
Department of CSE
SVEC
Tirupathi
kartheek521csestar@gmail.com

O Praveen Kumar
Department of MCA
SVEC
Tirupathi

S Srujan
Department of CSE
SVEC
Tirupathi

Abstract— Most cryptographic mechanisms such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key distribution mechanism is weak. Quantum Key Distribution or Quantum Cryptography is attracting much attention as a solution of the problem of Key Distribution; QKD offers unconditionally secure communication based on quantum mechanics. This work presents quantum key distribution protocols (QKDP) to safeguard security in large networks, ushering in new directions in classical cryptography and quantum cryptography.

Keywords: BB84 Protocol, QKD Protocol Implementation, Quantum Cryptography, Qubits.

I. INTRODUCTION

Secure communication link has widely become the most important method of today's modern society and their developments are increasing dramatically. The use of secure link has relied on the confidentiality and security of its data transmission. The emergence of e-commerce including electronic funds transfer, internet marketing, online transaction processing, electronic data interchange (EDI), electronic shopping and bank account management now-a-days are widely used to serve the convenience of users.

Two of the most important problems in cryptography are concerned with the security and authenticity of exchanged messages. Assume that two parties Alice and Bob wishing to communicate over the insecure (public) channel want to share a secret key. It is very important to Alice and Bob to 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 eavesdropper, Eve. Unlike conventional schemes of key distribution that rely on unproven computational assumptions, 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.Quantum Key Distribution (QKD) [1][2] is a technology, based on the quantum laws of physics, rather than the assumed computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels. It does this by using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel.

A QKD system consists of a quantum channel and a classical channel. The quantum channel is only used to transmit Qubits (single photons) and must consist of a transparent optical path. It is a lossy and probabilistic channel. The classical channel can be conventional IP channel (not necessarily optical), but depending on system design it may need to be dedicated and closely tied to the quantum channel for timing requirements.Key Distribution Protocols are used to facilitate sharing secret session keys between users on communication channel. By using these keys secure communication is possible on insecure public networks. However, various security problems exist in poorly designed key distribution protocols. Therefore, designing a 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 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 sender and receiver are involved in session key negotiations.In classical cryptography, three-party key distribution protocols utilize timestamps to prevent replay attacks. However, timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to unpredictable nature of network delays and 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.

In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanics 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.

II. RELATED WORK

There are two three-party QKDPs, one with implicit user authentication and the other with explicit mutual authentication[3], are combined to demonstrate the merits of combining both classical and quantum cryptography. Also when compared with classical three-party key distribution protocols, the proposed QKDPs easily resist replay attacks. This work presents a new direction in designing QKDPs by combining the advantages of classical with quantum cryptography.

There are few quantum key distribution protocols described in[1] such as BB84 quantum cryptographic protocol, B92 quantum cryptographic protocol, Entanglement-based quantum key distribution and Quantum Bit Commitment (QBC) protocols. Also this paper includes protocol evaluating and comparison, using such criteria as error possibility, quantum and classical memory bounds, noise sensitivity.

Some of the advantages of Quantum Cryptography over classical cryptography described in[4] i.e., it gives us perfectly secure data transmission. Also it discusses about Quantum Key Distribution and how important quantum cryptographic protocols are to it. It also tells about how eavesdropping will be in quantum cryptography and its effects.

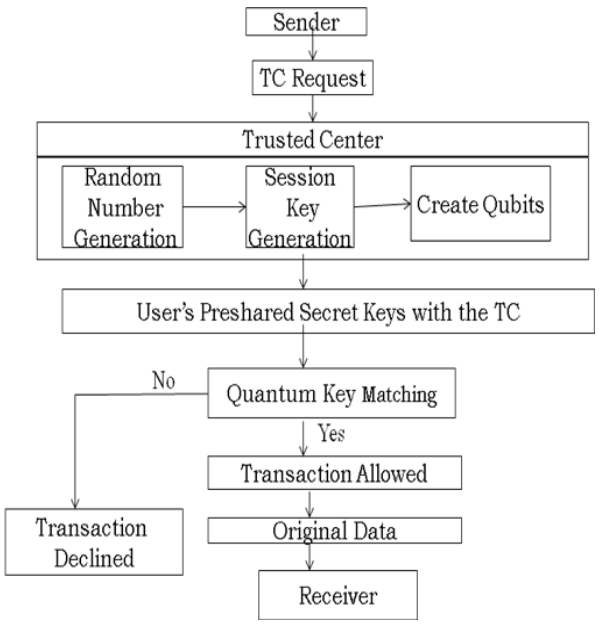


Figure 1: System Architecture

The security of some of the quantum cryptographic protocols such as BB84 protocol, Six-state protocol, SARG04 protocol, Symmetric and Asymmetric three-state protocol is described in[5]. The authors also compare their performances in both the ideal case and a realistic case and found that Efficient BB84 and Six-state protocols tolerate the highest QBER.

III. PROPOSED SYSTEM

Basic Scenario As shown in Figure 1, in the proposed QKDPs, the TC and a participant synchronize their polarization bases according 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.

IV. PROTOCOL IMPLEMENTATION

In 1984, Bennett and Brassard designed a protocol (imaginatively named the BB84 protocol) [1][6] based on the above behavior using four polarization states that works as follows: The sender encodes the information into quantum states using a random sequence of bases and transmits the information to the receiver. Each bit of this data will be in the form of a short burst of light, polarized using the said bases of measurement. The receiver then reads the incoming information using their own random sequence of bases. Once the data has been transferred, it only remains for the sender and receiver to publicly discuss which bases were used and in which order. Whenever the bases agree, it can be shown that the relevant bit of information is identical at both ends of the transfer, except in the following two situations:

a) When random noise disrupts the data channel.
b) When an eavesdropper attempts to intercept the data stream.

For the simulation, each of object (Alice, Bob, Eve, Quantum Channel, Public Channel) play different role. Only the appropriate function is executed in each of workstation, depends on its role. The protocol works as follows:

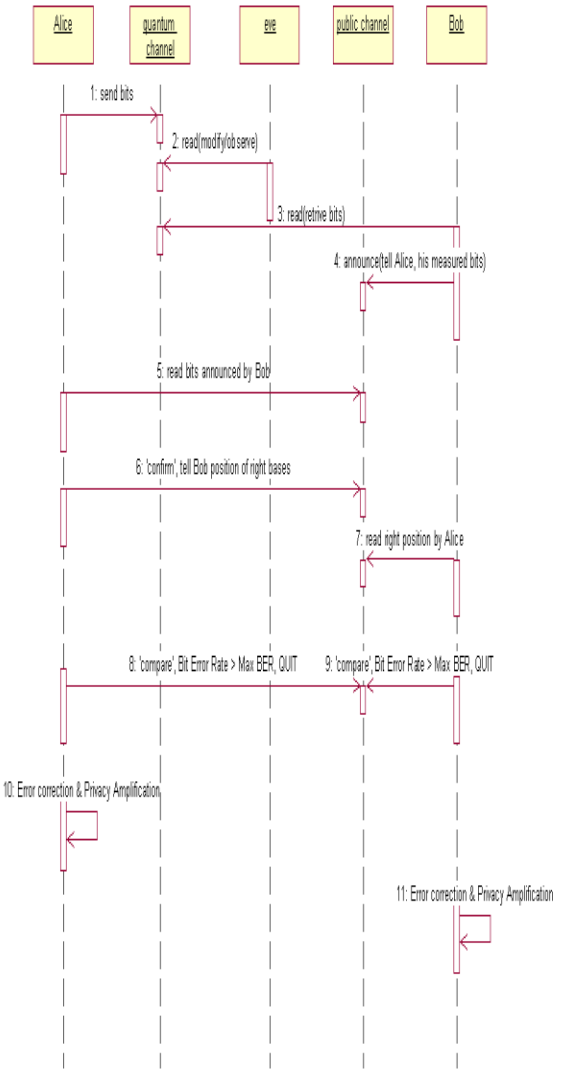
1. Alice generated a length (k) of random number (0 & 1), then sends it on quantum channel to be read by Bob and Eve.

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 kinds 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 measures 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 [7] raw key begin, Alice read Bob's measurement at public channel object and confirm to Bob the position Bob has measures 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 bit error rate (e). If they found that their error rate is higher than maximum bit error rate ($e > e_{max}$), they will suspend the communication and start all over again. (e_{max} has a 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 performs '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.

Finally, they both will get a same string of bits, which is the shared secret key

V. METHODOLOGY

Quantum cryptography, or quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

An important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced which is guaranteed as secure (i.e., the eavesdropper has no information about), otherwise no secure key is possible and communication is aborted.

Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably unbreakable when used with a secret random key.

Quantum Key Generation

To generate the quantum key using qubit and session key that depends on the qubit combinations [2] [3], such as:

A. If the value is 0 and 0, then 0.707(|0> + |1>)

B. If the value is 1 and 0, then 0.707(|0> - |1>)

C. If the value is 0 and 1, then |0>

D. If the value is 1 and 1, then |1>

Hashing Algorithm:
//Hashing Function to Convert Quantum Key into 8 digit

quantumkey hashing(key)

input: key
output: 8 digit Quantum Key

Beign

QK = key;
If QK Lenght is 8 digit
return QK;
Else


```
Begin
      rnd1 <-- getRandomInt();
      rnd2 <-- getRandomInt();
      QK = key * rnd1 * rnd2;
     While QK Length is not equalto 8
     Begin

      If QK Length > 8 then
          retrun QK.substring(0,8);
      Else If QK Length = 7 then
          QK <-- rnd1 * rnd2 * QK * 7;

      Else If QK Length = 6 then
          QK <-- rnd1 * rnd2 * QK * 9;
     Else If QK Length = 5 then
          QK <-- rnd1 * rnd2 * QK * 11;
     Else If QK Length = 4 then
          QK <-- rnd1 * rnd2 * QK * 13;
     Else If QK Length = 3 then
          QK <-- rnd1 * rnd2 * QK * 15;
     Else If QK Length = 2 then
          QK <-- rnd1 * rnd2 * QK * 17;
     Else If QK Length = 1 then
          QK <-- rnd1 * rnd2 * QK * 19;
     Else
          rnd1 <-- getRandomInt();
          rnd2 <-- getRandomInt();
     END IF
   End While
 return QK;
 End IF
End
```

Key Distribution

It distributes the original session key and Qubit to the sender for encryption. Also, it distributes the Qubit and session key to the receiver side for decryption.

A. TC(Trusted Center)

a) The TC generates a random number and a session key SK.

b) The TC creates the Qubits based on secret key for both the users.

B. User

a) Both the users measure the received Qubits.

b) Then they compute session key based on the received Qubits and random string.

VI. SIMULATION RESULTS

This paper is assured to give the following results without fail:

1. Quantum Key Distribution (QKD) uses quantum mechanics to guarantee secure communication.

2. Quantum Key Distribution enables two parties to produce a shared key known only to them, which can be used as a key to encrypt and decrypt messages.

3. The ability of the two users to detect the presence of any third party who is trying to eavesdrop the shared key.

4. Authenticate each other after the data transmission with the help of session keys, to prevent man-in-the-middle attack.

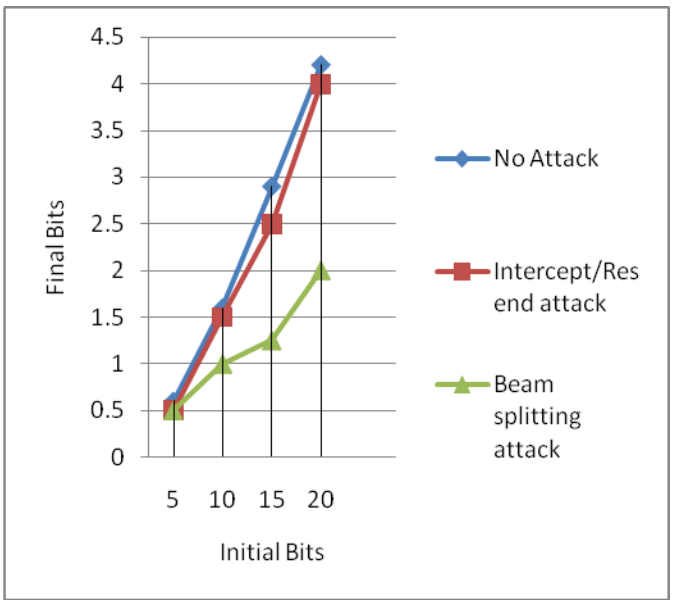


Figure 2: Initial Bits length vs Final Bits Length

In Figure 2, x-axis represents initial bits which its length is input from user (Alice), while y-axis represents final bits length that have been generated throughout the protocol. Three types of attacks are considered, that includes no-attack, intercept/resend and beam splitting that have been used within this simulation to examine the effect of attack existence.

From the Figure 2 we can see that even if there is no attack Bob still cannot gain perfect bits length send by Alice, this is because in Quantum Channel itself, there are also other effect that cause to imperfect channel. So, there is still a little error on their bits during the transmission.

Intercept/resend attack gives length of final bits almost equal to no-attack. In intercept/resend attack, Eve will generate a new string of random key and send it to Bob as if the key string has been send by Alice. So, the probabilities for Alice and Bob can detect Eve exist is 50% (increased). The probability that key string that generated by Eve similar to Alice is 50%. They both still can detect that error rate (e) is still lower than the maximum error rate ($e < e_{max}$) and continued to error correcting process.

Number of final bits length in beam splitting attack is much lower than the other two attacks because; in this attack a random number of Alice's bits are split by Eve. Thus more error can be detected by Alice and Bob in 'error correction' process. Although the error rate (e) is still lower than the maximum error rate ($e < e_{max}$), Alice and Bob can detect as much as 50% of error in their sifted key. The length of corrected key is higher than other two attack leads to most of the bits have to eliminate in 'error correction' process to minimize the information for Eve.

VII. CONCLUSION AND FUTURE WORK

This work presents quantum key distribution protocols (QKDPs) to safeguard security in large networks, ushering in new directions in classical and quantum cryptography. In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanics to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. By using Quantum Channel we can eliminate passive attacks like eavesdropping and therefore replay attacks. This in turn can be used to reduce communication rounds.

It proposes two three-party QKDPs to demonstrate the advantages of combining classical cryptography with quantum cryptography. The proposed QKDPs easily resist replay and passive attacks and also efficiently achieve key verification and user authentication. In this a secret key preshared by a TC and a user can be long term (repeatedly used). Although the requirement of quantum channel can be costly in practice, it may not be costly in future. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDPs.

Further in this work by using Privacy Amplification in public channel we can reduce the number of bits known to the eavesdropper so that final bits obtained will be almost equal to the initial bits.

REFERENCES

[1] Lelde Lace, Oksana Scegulnaja-Dubrovska, Ramuns Usovs, Agnese Zalcmane, "Quantum Cryptographic Key Distribution Protocols", The European Social Fund(ESF), 2008.

[2] Quantum Key Distribution Protocols: A Survey.

[3] Tzonelih Hwang, Kuo-Chang Lee, 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.

[4] Rajni Geol, Moses Garuba and Anteneh Girma, " Research Directions in Quantum Cryptography", International Conference on Information technology, 2007.

[5] Chi-Hang Fred Fung, Hoi-Kwong Lo, "A survey on quantum cryptographic protocols and their security", IEEE, 2007.

[6] Wikipedia,http://en.wikipedia.org/wiki/Quantum_cryptogr phy "Quantum Cryptograpxhy".

[7] http://swissquantum.idquantique.com/?Key-Sifting

