Three Party Authentication Using Quantum Key Distribution Protocol

Pratap M S, Drishya Nair, Ponnu Narayanan, Nitha Kamar, Aneesa C V
Department of Computer Science, Kvg College of engineering, sullia
pratapms17@gmail.com, drishyabhaskar25@gmail.com, ponnun7@gmail.com, nitharashad26@gmail.com, aneesa132@gmail.com

ABSTRACT-Cryptanalysis is an important branch in the study of cryptography, including both the Classical Cryptography and the Quantum one. In this paper, we analyze the security of Three-Party Quantum Key Distribution Protocol proposed recently, and point out that they are susceptible to a simple and effective Dense-Coding attack, through its architectural implementation in Classical Cryptography. The protocol focuses the operations of key generation and measurement in the trusted center‘s lab. With a symmetric key encryption method, the intruder is resisted from eliciting the confidential information transmitted between the legal users. It is shown that the eavesdropper Eve can totally obtain the session key by sending bits as the fake signal to sender and performing collective measurements after sender‘s encoding. The attack process is just like a dense-coding communication between Eve and sender, where a special measurement basis is employed. Furthermore, this attack does not introduce any errors to the transmitted information and consequently will not be discovered by sender and receiver. The attack strategy is described in detail and a proof of its correctness is given. Finally, the root of this insecurity and possible way to improve the protocol are discussed.

Keywords – encryption, decryption, Quantum Cryptography, QKDP

1. INTRODUCTION

As the most important application of system quantum cryptography, Quantum key distribution is 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. It allows two users, generally called Alice and Bob, to privately share a random key through quantum key distribution protocol (QKDP) through which they obtain a shared session key through a trusted center. Hence the protocol is termed as Three-Party QKDP.

The existing scenario deals with the transmission of data directly from the sender to receiver where data communication software plays its intermediate role. It has been noticed so many issues concerning the privacy, such as dense-coding attack over the communication channel in transmitting large volume of personal and sensitive information. As the intruder encounters in the midst of the legal users in hacking the data, the communication is no longer reliable and secure. Three-party QKDPs proposed yet are susceptible to this attack in the sense that the third-party can totally acquire the session key which is being shared between the communicating users, by sending the entangled bits as the fake signal to the sender. Either of these users can never discover that eavesdropping has occurred since it won‘t introduce any error to the transmitted information. The protocol supports no measurement apparatus for the sender and receiver with the reason that they cannot take measures to detect eavesdropping. The attack process is just like a dense-coding communication between the third party and sender.

In order for a secure communication, prevention of dense-coding attack is necessary. To overcome these limitations of the existing system the new system is developed which in turn guarantees the legal users from eavesdropping.

Network Security is fast looming on the horizon as a potentially massive problem over the communication network. It covers a multitude of sins such as concerned with intruders trying to access remote services that they are not authorized to use or secretly modifying messages intended for other recipients. Many techniques are used to overcome the problems faced in communication and data transfer. In this paper we analyze the security of three-party quantum key distribution protocols proposed recently, which were susceptible to a the dense-coding attack.

Encryption is the standard method for making a communication private. Anyone wanting to send a private message to another user encrypts or enciphers the message before transmitting it. Only the intended recipient knows how to correctly decrypt or deciphers the message. Anyone who was eavesdropping on the communication would only see the encrypted message. Because they would not know how to decrypt it successfully and the message would make no sense to them. Cryptography uses this method in cryptosystems to maintain confidentiality of information. Since the security of most classical cryptosystems is based on the assumption of computational complexity, they might be susceptible to the strong ability of quantum computation and will become no longer secure once quantum computer appears. This in turn led to the advent of quantum cryptography. Different from its classical counterpart, quantum cryptography is the combination of quantum mechanics and cryptography, where the security is assured by physical principles which can stand against the threat from an attacker with the ability of quantum computation. QKD constitutes one of the branches of quantum cryptography. Shared keys are used for secure communication on insecure public network since the legitimate participant cannot ensure that the received session key is correct and cannot confirm the identity of the user. It focuses on the operations of key generation and its measurement in the trusted center‘s lab as the case here is

that the information is encoded in bits. So also they are insecure under Dense Coding Attack. Since cryptographic methods cannot be proven secure, Rijindael methods security rests on the fact that it is extremely difficult for an attacker to hack the key. With the implementation of a secure symmetric key encryption method named Rijindael algorithm, it is shown that eavesdropper is being prevented from obtaining the session key which is shared among the two communicating users.

2. METHODOLOGY

The system defines a secure Third-Party Quantum Key Distribution Protocol which is resistant to Dense-Coding Attack. In the protocol, the operations of bits generation and measurements are focused in the Trusted Center‘s lab. It verifies the correctness of the secret session key and authenticates the user to ensure that confidentiality is only possible for legitimate users. The sender encodes the session key into bits by performing parity checking. After the receive of key, decoding operation is being performed at the receiver terminal. With the implementation of a symmetric key encryption algorithm, the proposed QKDP detects Man-in-the-middle attacks on the data, thus offering a reliable communication between the legal users. User authentication and session key verification is being done in single step without any public discussion with the sender and receiver. There are two types of Quantum Key Distribution Protocol, they are:

The Proposed 3AQKDP

This section describes the details of the 3AQKDP. Here, we assume that every participant shares a secret key with the TC in advance either by direct contact or by other ways.

The Proposed 3QKDPMA

The proposed explicit quantum key distribution protocol 3QKDPMA can be divided into two phases: the Setup Phase and the Key Distribution Phase. In the Setup Phase, users pre-share secret keys with the TC and agree to select polarization bases of qubits based on the pre-shared secret key. The Key Distribution Phase describes how the user and could share the session key with the assistance of TC and achieve the explicit user authentication.

3. RELATED WORK

Cryptography is the science of information security. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The combination of Implicit quantum key distribution protocol (3AQKDP) and explicit quantum key distribution protocol (3AQKDPMA) are used to form the new combination and demonstrate the following merits:
It will establish secure connection which can prevent attacks such as eavesdropping, man-in-the-middle and replay.
Reduction in communication rounds among existing QKDPs, improves efficiency of proposed protocols. A long Term secret key can be used and shared between two parties repeatedly.
Classical cryptography methods currently used are unsafe and cannot detect the existence of passive attacks such as eavesdropping. Hence the combination of both classical as well as quantum cryptography is proposed.
Research in authentication protocol has focused largely on developing and analyzing protocol that are secure against certain types of attacks. There is little and only scattered discussion on protocol efficiency. For each proven lower bound, an authentication protocol achieving the bound is also given, thus proving that the bound is a tight bound if the given optimal protocol is secure. Moreover, impossibility results of obtaining protocols that are simultaneously optimal with respect to the numbers of messages and rounds are given [6].

4. SYSTEM ANALYSIS

In Registration phase after providing username and password, user must generate one unique key for identification. That is Secrete key. This key will take part in our final key **(Quantum Key)**. At this instance our system will store every details such as username, password, secrete key, Registration Date and Registration Time.
After Registration for New User system redirects the user to Login Stage. At this stage the user must provide the relevant details which was noted or given through registration. The secret key generation is in separate class which will return.

Trusted Center Module

Trusted center module generates the key.it comprises of following modules:

Secret Key Verification

Verify the secret key received from the user and authenticate the user for secure transformation.

Session Key Generation

It is shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential value of random number.

Qubit Generation

To get secret key and random string, then convert into hex-code and then convert it into binary, find the least bit of two binary values and get the quantum bit of 0 and 1.

Quantum Key Generation

To generate the quantum key using the qubit and session key which depends on qubit combinations, such as :

1. If the value is 0 and 0, then 1/0.707(p[0]+p[1])
2. If the value is 1 and 0, then 1/0.707(p[0]-p[1])
3. If the value is 0 and 1, then p[0]
4. If the value is 1 and 1, then p[1]

Key Distribution

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

Receiver

Getting Authorization is the first stage in receive phase. If a user wants to receive a text from source user, he wants unique Identification. By using that Identification System, we can identify that that the person is an authorized person. This phase or Receiver Module has Sub Modules. They are:

Registration
Login and
Receive Data

Registration

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. And System provides one more credentials that is Secrete key which is generated by the system for each user. By using **username**, **Password** and **Secrete key** system will identify the Authorized person. These values are stored in the Database quantum key in which **reg** table.

Login

If a user wants to send a file, he/she must log in by using his/her authentication credentials. In this module we have to give **username**, **password** and **Secret key** which was generated by the system.

If the user does not provide proper information or the given information is mismatched with database then our system shows Exception message immediately.

If the user‘s details are verified and matched with the existing database then our system allows the person to transmit the file.

After login the TCP program calls i.e. our Trusted Center program starts listen the client or sender. Through Login we send the sender‘s secrete key for Identification.

Receive Data

The main aim of this module is to decrypt a file. Decryption will happen only if the system gets a key from **Trusted Center (TC)**. So after verification of user identification system will send the current user‘s name and his/her secret key to **Trusted Center (TC).**

In Registration phase after providing username and password, user must generate one unique key for identification. That is Secret key. This key will take part in our final key **(Quantum Key)**. At this instance our system will store every detail such as username, password, secret key, Registration Date and Registration Time.

After Registration for New User system redirects the user to Login Stage. At this stage the user must provide the relevant details which was noted or given through registration.

5. SYSTEM MODEL

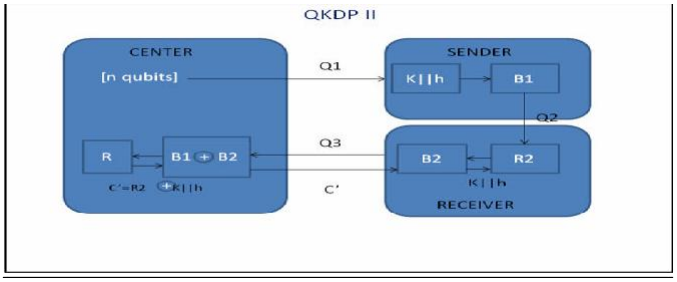

Fig 1: system model for QKDP

Algorithm for Logic Implementation

The Protocol is composed with the following steps:

1) The Trusted Center generates n bits and sends this sequence (Q1) to Sender (Alice).
2) After receiving Q1, Alice selects a u-bit random session key K and computes its m-bit hash value h=H (K) as the checksum, where u+m=n. Then Alice performs unitary operation U0=I on the i^{th} bit in Q1 if the i^{th} bit in K||h is 1. Furthermore, Alice generates an n-bit random string B1, and performs unitary operation U0=I on the i^{th} bit in Q1 if the i^{th} bit in B1 is 0. After these coding operations Alice sends the new sequence (denoted as Q2) to Receiver (Bob). Here

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

3) After receiving Q2, Bob selects two n-bit random strings R2 and B2. Then he performs unitary operation U0 in each bit in Q2 according to R2, and then operation U0 on each bit according to B2. Afterwards Bob sends the new bits sequence (denoted as Q3) to the Trusted Center.
4) The Center informs Alice and Bob after the receiving of Q3.
5) Alice and Bob tell the Center B1 and B2 respectively.
6) According to B⊕B2, the Center recovers the original bases of bits by performing U0 on each bit as in step 2 and 3. Then the center measures all the bits in basis R= {0, 1}, obtaining the measurement results , C‘=R2⊕ (K||h). Finally, C will be announced to Bob by center.
7) Bob recovers K||h= R2 ⊕C‘ and verifies whether h=H(K). If it is correct, Bob obtains the session key K and tells Alice it is successful.

6. CONCLUSION

The fast streaming evolutions in the cyber world is undergoing drastic revolutions over the technologies and network environment. The demands are on the hike in the field of communication from Classical to Quantum networks. Yet the problem of utmost security over the confidential information and the Key remained as such. Key exchange is weak spot in many cryptosystems. Even the strongest cryptography is useless, if the key used to encrypt and decrypt the data are not secure. Mechanisms for key exchange exist yet are unsusceptible over powerful computers. QKDP II is tuned to cater this need, without putting additional overheads, affecting the network topology. The protocol implements a system assuring a reliably secure communication between the sender and receiver by analyzing the security of the existing QKDP which were susceptible to Dense-Coding Attack. The protocol focuses the operations of key generation and measurement in the trusted center‘s lab. With a symmetric key encryption method, the intruder is resisted from eliciting the shared

session keys between the legal users and thus used to encrypt and decrypt the message which in turn transmits over a standard communication channel. The Trusted Center constitutes a module that verifies the correctness of the secret session key and authenticates the user to ensure that confidentiality is only possible for legitimate users. It generates the random secret key from which Session key and dispenses it to the sender for encryption. Accordingly, announces the measure of bits to the receiver end by distributing it along with the session key for decryption. Generation of the Session Key is entrusted to the Sender module. Mean while, the Receiver module recovers the session key which is being formally generated by the Sender

.

7. FUTURE WORK

The current protocol has been chosen Classical Cryptography as its implementation domain. It will well suits if the same is applied on Quantum computers since the architectural design is constructed to cope with the Quantum Cryptographic scenario. Accordingly, improved bit rates can be achieved in exchanging secure keys. Any improvements in the hardware can favor for exploiting the opportunities at the application level. Quantum key distribution (QKD) systems have the advantage of being automatic, with greater reliability and lower operating cost than other secure networks.

The protocol is well fit to compete to future amendments at the software aspect so can be re-structured. Advanced Cryptographic algorithms can be implemented evaluating its security over credential information. If improved achievements are reflected, the benefits will be immense.

REFERENCES

[1] Dr Anand Rao, –Three party authentication key distribution protocol using implicit and explicit quantum cryptography , Vol. 2 No. 2 143-145, 2011.

[2] G. Li, –Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations,‖ Distributed Computing, vol. 9, no. 3, pp. 131-145, 1995.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7]. System Analysis and Design, Ellias M Award

[8]. C#.Net Programming Bible, Jeff Ferguson, Bian Patterson and Meeta Gupta

[9]. Software Engineering, Ian Somerville

[10]. SQL Server 7-The Complete Reference, Gayle Coffman