International Journal on Applications in Information and Communication Engineering
Volume 8 : Issue 1 : June 2022, pp 14 – 18 www.aetsjournal.com ISSN (Online) : 2394 - 6237

ENCRYPTION - SECURE COMMUNICATION USING PUBLIC KEY INFRASTRUCTURE VIA TCP/IP NETWORK PROTOCOL

ASWATHI . A, Dr. T. VELUMANI

***Abstract*—** Key distribution protocols to safeguard security in large networks, ushering in new directions in classical cryptography and cryptography. Two three-party Key distribution protocols, one with implicit user authentication and the other with explicit mutual authentication, are proposed to demonstrate the merits of the new combination, which include the following: 1) security against such attacks as man-in-the-middle, eavesdropping and replay, 2) efficiency is improved as the proposed protocols contain the fewest number of communication rounds among existing Key distribution protocols, and 3) two parties can share and use a long-term secret. To prove the security of the proposed schemes, this work also presents a new primitive called the Unbiased-Chosen Basis (UCB) assumption. The public key shared between the two users via TCP/IP Protocol. Quantum cryptography, or quantum public 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. These results from a fundamental part of quantum mechanics: the process of measuring a quantum system in general disturbs the system. 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.

***Keywords*—** Cryptography, Quantum Public Key, Unbiased-Chosen Basis.

I. INTRODUCTION

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. 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 the other participant. Designing secure key distribution protocols in communication security is a top priority.

Overview of the System:

Key Distribution Protocol (KDPs) which works on network security by the use of key agreement. Secrete Key which is used by each user in the network. Each user has unique Secrete and which will be shared by each user to Trusted Center. In Trusted Center we have generate a Key for network Security with the Help of Algorithms and Quantum Mechanics. Through that we have to prove how secure the data has been transmitted over network to receiver.

Description of the System:

This work presents Key Distribution Protocols (KDPs) to safeguard security in large networks, ushering in new directions in classical cryptography

Aswathi A, Student, M.Sc Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India – 641021, (e-mail: aswathi8248@gmail.com).

Dr. T. Velumani, Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India – 641021, (e-mail: velumani.cs@rathinam.in).

and quantum cryptography. Two three-party KDPs, one with implicit user authentication and the other with explicit mutual authentication, are proposed to demonstrate the merits of the new combination, which include the following:

1) Security against such attacks as man-in-the-middle, eavesdropping and replay,
2) Efficiency is improved as the proposed protocols contain the fewest number of communication rounds among existing QKDPs, and
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.

Key Distribution (KD) is a method of securely distributing cryptographic key material for subsequent cryptographic use. In particular, it is the sharing of random classical bit strings using quantum states. Its use of a set of non-orthogonal quantum states then requires this key material to be considered quantum information. The quantum encoding of cryptographic keys for distribution is valuable because the no-cloning theorem and the superposition principle governing quantum states confer a uniquely powerful form of information security during transmission of key bits. For maximal security, it can be followed by one-time pad message encryption, which is the only cryptographic method that has been proven to be unbreakable once a random key has been securely shared.

Key distribution—the creation of secret keys from quantum mechanical correlations—is an example of how physical methods can be used to solve problems in classical information theory.

Key Distribution (KD), 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. This result from a fundamental part of quantum mechanics: the process of measuring a quantum system in general disturbs the system. 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.

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security.

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.

II. PROPOSED WORK

A. System Description:

This project contains four modules. They are:

1. Login
2. Sender
3. Trusted Center
4. Receiver

B. Module Description:

Login Module

1. User Login
2. Admin Login

Sender Module

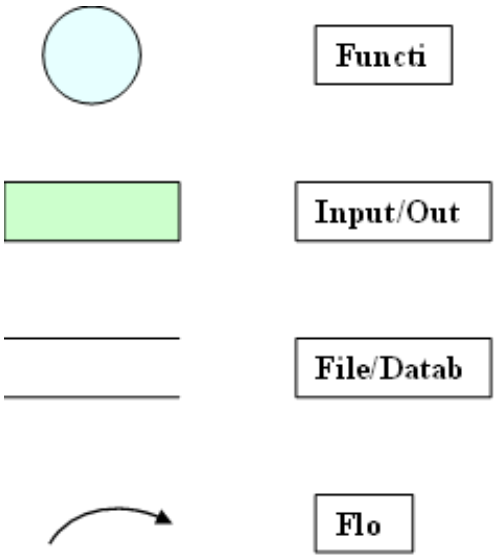
1. Secret key Authentication

2. The sender give the secret key to the trusted center, then the TC will verify the secret and authenticate to the corresponding sender and get the session key from TC or else TC not allow the user transmission
3. Encryption
4. The message is encrypted by the received session key and appends the qubit with that encrypted message, then transmit the whole information to the corresponding receiver.

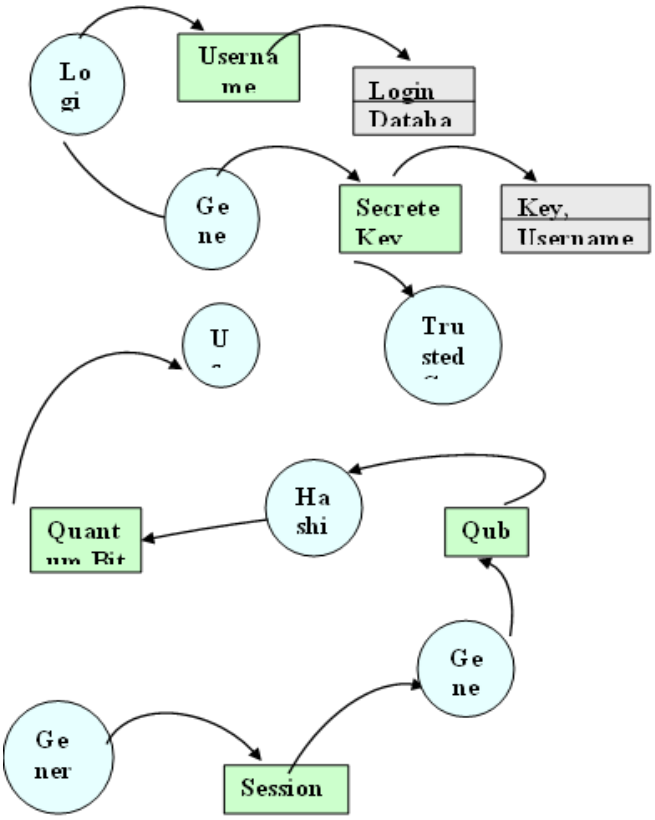
C. Trusted Center Module:

1. Secret Key Verification
2. Verify the secret key received from the user and authenticate the corresponding user for secure transmission.
3. Session Key Generation
4. 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
5. Qubit Generation
6. Quantum Key Generation
7. Hashing
8. Key Distribution

D. Data Flow Diagram Notations:

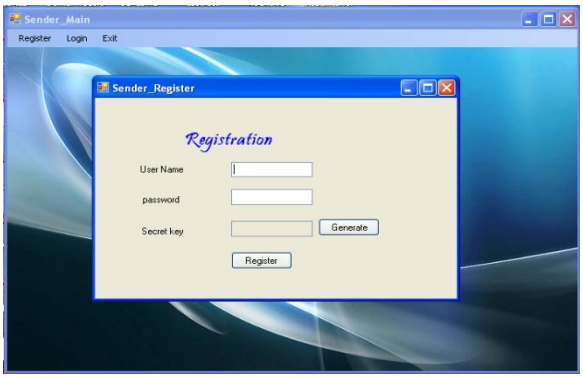


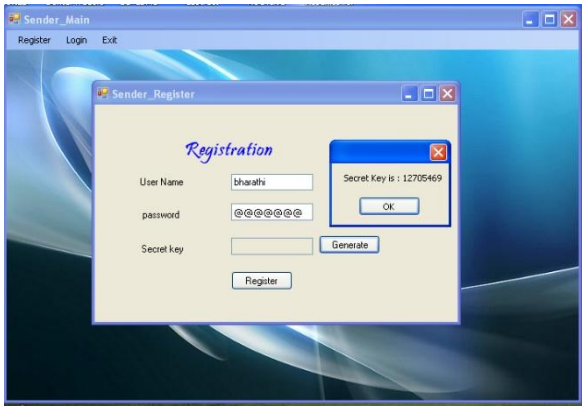
E. User Sender/Receiver:

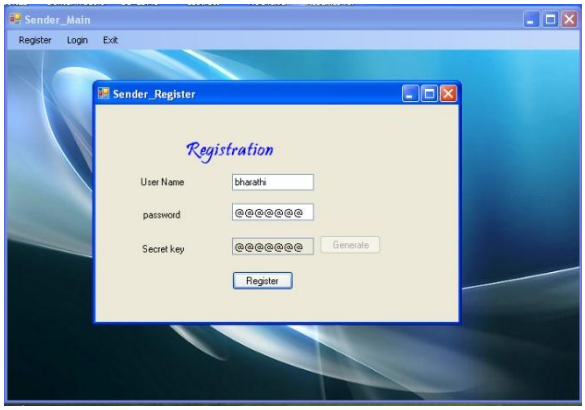


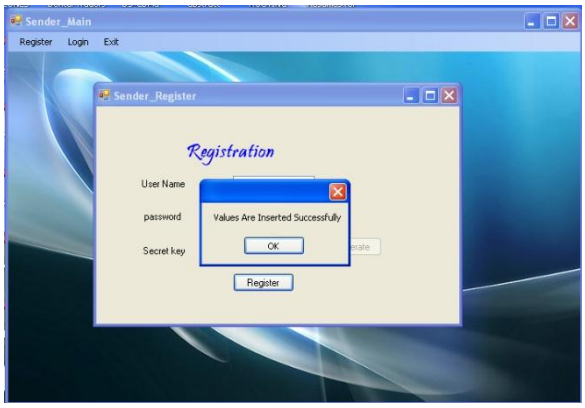
III. EXPERIMENTAL RESULTS

Sender:

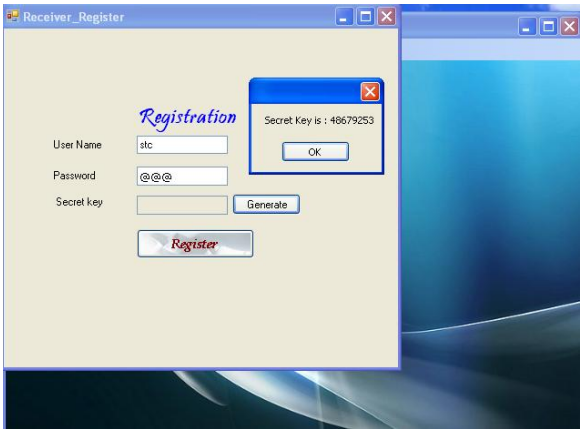


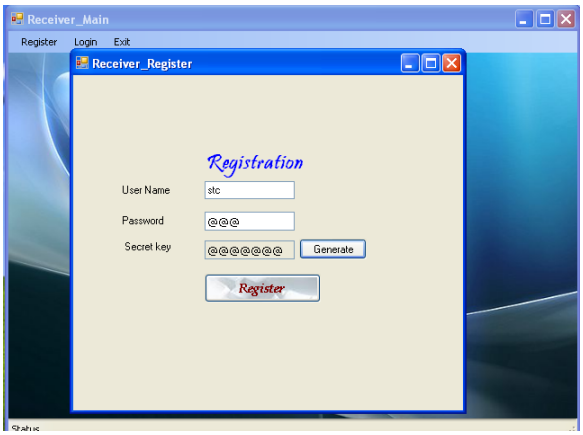


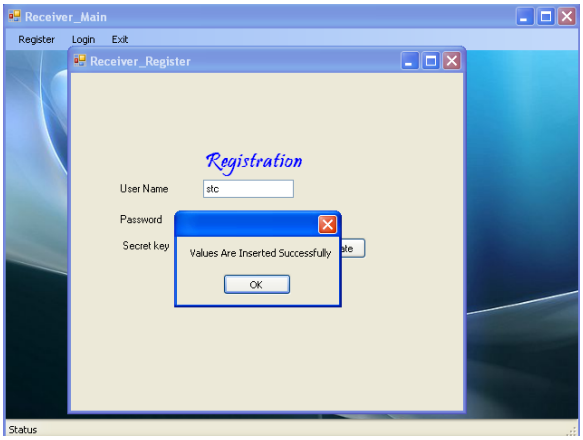




Receiver







IV. CONCLUSION

This study proposed public key infrastructureto demonstrate the advantages of combining classical cryptography with quantum cryptography. Compared with classical three-party key distribution protocols, the proposed PKI easily resist replay and passive attacks. Compared with other PKIs, 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 PKIs 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 PKIs 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 PKIs.

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.