Available online at www.sciencedirect.com

ScienceDirect

Materials Today: Proceedings XX (2016) XXX–XXX

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

PMME 2016

Integrated Classical and Quantum Cryptography Scheme Using Three Party Authenticated Key Distribution Protocols

D.Renuka[1], Dr.P.Chenna Reddy[2]

[1]*Department of Computer Science & Engineering,*
[2]*Professor of CSE Department,*
[1]*JNTUCEP college, Pulivendla,Andhrapradesh, India.*
[2] *JNTUniversity, Ananthapuramu, Andhrapradesh, India.*

Abstract

Now a day's Cryptography is most widely used technique for providing security. Classical Cryptography and Quantum Cryptography are two techniques that are widely used. Digital signatures provides best authentication in Classical cryptography. Quantum cryptography provides photons and polarization (these are quantum mechanical properties) for best security. By combining both, we can provide best authentication and security and also number of communication rounds can be reduced. Passive attacks cannot be solved by classical cryptography and large number of rounds of communication is another major problem. Eaves dropping can be eliminated with quantum channel and reduce the number of rounds for communication. But in quantum cryptography digital signatures are difficult to use, and it has distance limitation. This paper presents security and authentication by using Three Party Authentication Scheme i.e., three parties are involved. Implicit User Authentication and Explicit Mutual Authentications are used previously for providing authentication. In this paper digital signatures add to explicit mutual authentication to show new combination. This paper has the objective to solve authentication problem and also provide solutions to attacks such as man-in-the middle attacks, eaves dropping, and replay attacks.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Keywords: Classical Cryptography; Quantum Cryptography; Three-party authenticated key distribution protocols; Provable security; passive attack; digital signatures; communicaton rounds.

1. Introduction

Classical cryptography uses simple mathematical methods to provide security and there is possibility for many attacks such as passive attacks, man in the middle attacks, and replay attacks. To prevent replay attacks challenge-response mechanism is used in classical cryptography, but it cannot solve the passive attacks and also requires two additional rounds for communication. Classical cryptography solves replay attacks, passive attacks, and

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

reduces the number of rounds for communication [1]. In quantum cryptography, quantum mechanical properties are used to provide security. It uses qubits for encoding information. It uses photons and polarization to generate qubits. The session key correctness can be verified by using public discussion in quantum cryptography [2].

Quantum cryptography suffers from man-in-the-middle attacks if the authentication is not proper in manner [3]. By using digital signatures, classical cryptography can solve the problem. Digital signatures provide key verification and user authentication in classical cryptography. In this paper we combine the classical cryptography and quantum cryptography to provide best security and authentication [4]. Previously proposed quantum key distribution protocols (QKDP) solves the authentication by using implicit and explicit mutual authentication. In this paper we propose to add digital signatures at explicit mutual authentication to provide more security and we can solve the problems such as passive attacks, man-in-the-middle attacks and replay attacks [5]. We can use third party authentication to solve replay attacks, digital signatures are used to solve man-in-the-middle attacks, and quantum cryptography solves eaves dropping and reduces number of rounds for communication [6].

Previously two party authentications are used [7]. Here we use three party authentication which means that we can use three parties in the communication [8]. They are sender, receiver and Third party (Trusted center). Participants obtain a session key by using trusted center.

1.1. Related Work

In [1], authors proposed that in large networks, security is provided based on quantum key distribution protocols by relating classical cryptography and quantum cryptography. They proposed implicit and explicit mutual authentication schemes to discuss their suggested works. Their works include securing replay, and eavesdropping attacks. Efficiency can be improved in their proposed protocols by providing least number of rounds among Quantum Key Distribution (QKD). Using Unbiased Chosen Basis (UCB) notion, a new technique for providing security is established. In the view of UCB, QKD uses no-cloning technique and quantum measurement to provide a secure key against the attacks between the participants. Quantum measurement measures the qubits based on bias i.e., Rectangle or Diagonal basis. Unknown quantum state can't be duplicated and can't copy the qubits if attacker is unaware of the polarization as per the statement of no-cloning proposal.These proposed works acts as a new way for evaluating QKDPs.
In [4], in quantum cryptography to understand authentication strongly universal hash functions are studied. Vulnerabilities related to man-in-the-middle attacks are studied. Authentication lifetime is used to estimate the encrypted tags. This suggests primitive measures like using extra key for extra authentication, reducing information leakage, and changing secret hash function frequently. Further research ideas are given to use less key-consuming authentication with strong security.

In [5], as in [1, 2] authors focus on developing a secure model for large networks. Here, they combine mechanics of both classical cryptography and quantum cryptography.QKD framework with network design and services that provides security is discussed here. For security proof of QKDP, UCB is used. It states that, QKD provides more security by using polarization. A session key is used to share the secret keys repeatedly for a long time. This model can resist replay attacks and passive attacks effectively.
In [6], as in classical cryptography the methods used currently are unsafe and liable to passive attacks, and these attacks can be solved by quantum cryptography. The combination of implicit QKDP and explicit QKDP are proposed by combining both classical cryptography and quantum cryptography to provide secured transmission between the participants. Dynamic multicast systems are used in this proposed technique that are based on bilinear maps, which can further solve scalability issues. Authentication is achieved by using Identity-tree. In this scheme

both forward and backward secrecy can be achieved.

In [7], the concept of multi-server is suggested, in which a user in parallel can communicate with many servers for the purpose of authentication. This presents a two server system that directly interacts with the user and is visible to service server. In this, Classical Key Exchange (CKE) and QKD models are used. It proposes the use of integrating both the models.

2. Proposed Integration Of Classical and Quantum Cryptography

In this integrated classical cryptography and quantum cryptography, the participant and TC agree their polarization by using the pre-shared secret key. These secret key with random string can be used to produce another encryption key to encode session key at the time of key distribution Even if similar session keys are transmitted the same polarization of qubits could not be received by the receiver.

It presents implicit user authentication and explicit user authentication. The implicit user authentication ensures that confidentiality is only possilble to accepted users. After secure communication using session key, explicit user authentication is possible. Additionally add digital signatures at explicit authentication.

1.2. Notation

R: Rectilinear basis

Polarizations: 0 and 1

D:Diagonal basis

Polarizations: $1/\sqrt{2}$ (|0> +|1>) and $1/\sqrt{2}$ (|0> -|1>)

$r_{TU:}$Random string

$K_{TU:}$ Secret key used between TC and user

SK: Session key

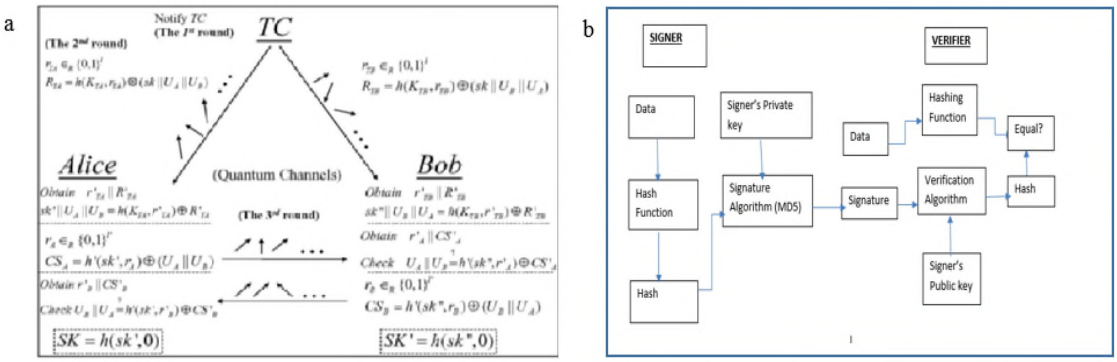

Fig1. (a) Key distribution phase (Source: [1]); (b) Digital signatures

1.3. Setup Phase

- Consider two users who shared the session key securely.
- K_{TU} is secret key between trusted center and user for measuring bias
- IF $(K_{TU})_i$ =0 then D basis
- Otherwise R basis can be considered.

1.4. Key Distribution Phase

1. First implicit user authentication can be done such as participants can authenticate through trusted centre based on their login credentials.
2. Trusted centre shares the sender and receiver keys. This is referred as pre-shared secret key.
3. Random number and session key are generated by trusted centres. Then it computes
   $R_{TA}=h(K_{TA},r_{TA})\oplus (sk||U_A||U_B)$for sender and computes
   $R_{TB}=h(K_{TB}, r_{TB})\oplus (sk||U_A||U_B)$ for receiver.

4.The qubits generated by using trusted center for sender as

- If $(r_{TA} || R_{TA})$ i= 0, (K_{TA})I = 0,
  Then (QTA)i is $1/\sqrt{2}$ $(|0> +|1>)$
- If $(r_{TA} || R_{TA})$i=1, (K_{TA})i=0,
  Then (Q_{TA})I is $1/\sqrt{2}$ $(|0>-|1>)$.
- If $(r_{TA} || R_{TA})$i=0, (K_{TA}) I=0,
  (K_{TA})i=1, then (Q_{TA}) i is $(|0>)$.
- If$(r_{TA} || RTA)$ i=1, (K_{TA}) I=1,
  Then (Q_{TA}) i is | 1)

5. Trusted center generates qubits for receiver is same as above
   Participants receive qubits depending on secret key and measured based on bias D or R
   Once qubit is measured then computes
   $sk'||U_A||U_B=h(K_{TA},r'_{TA}) \oplus R'_{TA}$ for sender
   $sk'||U_B||U_B=h(K_{TB},r'_{TB})\oplus R'_{TB}$ for receiver
6. Checksum can be computed is
   $CS_A=h'$ $(sk', r_A) \oplus (U_A||U_B)$ for sender
   $CS_B=h'(sk'',r_B) \oplus U_B||U_A)$ for receiver
7. Checks the checksum for two participants as
   Check $U_A||U_B=h'(sk'',r'_A) \oplus CS'_A$ at receiver side
   Check $U_B||U_A= h'$ $(sk', r_{'B}) \oplus CS'_B$ at sender side
8. Then build the session key SK and SK'
   $SK=h(sk',0)$
   $SK'=h(sk'',0)$

2.4. Digital Signatures Phase

1. By using the session key sender computes the digital signatures
   Digital signatures are generated by using MD5 algorithm as follows
   - Append the length and padding bits
   - MD buffer can be initialized
   - Message is processed in 16-word blocks
   - Finally, digital signatures is created

2. The encrypted message can be send to receiver
   Receiver verifies digital signatures by using the sk'' generated by receiver.
   The message is decrypted at the receiver if the signature and key is verified.

3. Security Proof

1.5. Protocol participant

The trusted center and authorized set of participants can be used in integration of classical cryptography and quantum cryptography. In concurrent execution trusted center and number of participants can exist.

1.6. Long-term secret key

It is a long random binary string which is shared between trusted centre and participants.

4. Implementation

The implementation is done in JDK 1.6 and SWING API are used for building GUI. The application is executed in Windows XP. Following figure depicts the trusted centre for UI

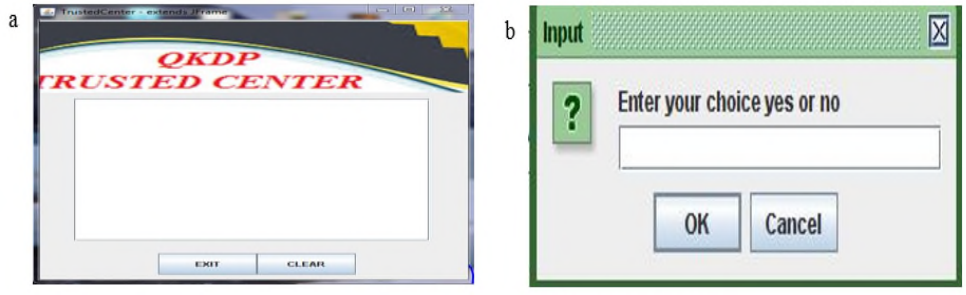

Fig 2. (a)Trusted Center; (b) Check the receiver's willingness

Here the participants should register with port number and secret key is stored in separate databases maintained for them whenever each user either makes a login request through secret key. Then the sender can be asked the willingness of receiver to send the data through trusted center to know the receiver's secret key. The trusted center authenticates the sender and finds the receivers willingness as shown in fig2 (b)**.**

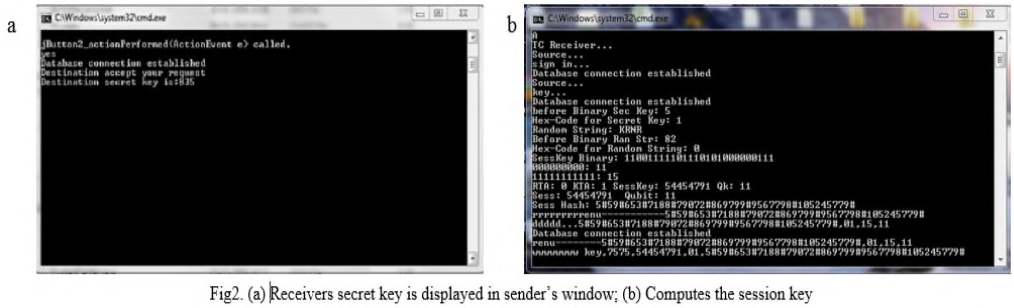

Fig2. (a) Receivers secret key is displayed in sender's window; (b) Computes the session key

If receiver is willing to receive the data from sender then the trusted center retrieves the secret key from the database and displays the secret key on sender window as in Fig3 (a)

So 835 is destination secret key. This can be displayed only on sender's window. Based on these we can provide the security. Then message is send by the sender through secret key. Session key is generated through trusted center by using random number, secret key, qubits etc., as

$sk'||U_A||U_B=h(K_{TA},r'_{TA}) \oplus R'_{TA}$ for sender

$sk'||U_B||U_B=h(K_{TB},r'_{TB})\oplus R'_{TB}$ for receiver

In sender digital signatures can be added to provide authentication as shown in fig 4(a). By using the digital signature and the key we encrypt the data by using DES as in Fig 4(b)

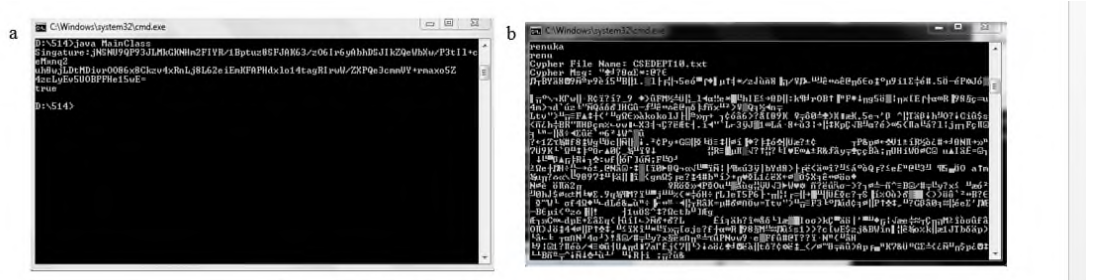

Fig4. (a) Digital signature is generated for given data; (b) Encrypted data

Then trusted centre sends data to the receiver. At receiver side it asks the secret key to provide more authentications. The sender's secret key is known by the receiver through trusted center and enters that key as shown in fig5 (a); here secret key of sender is 977, the session key generated by trusted center for sending the data.

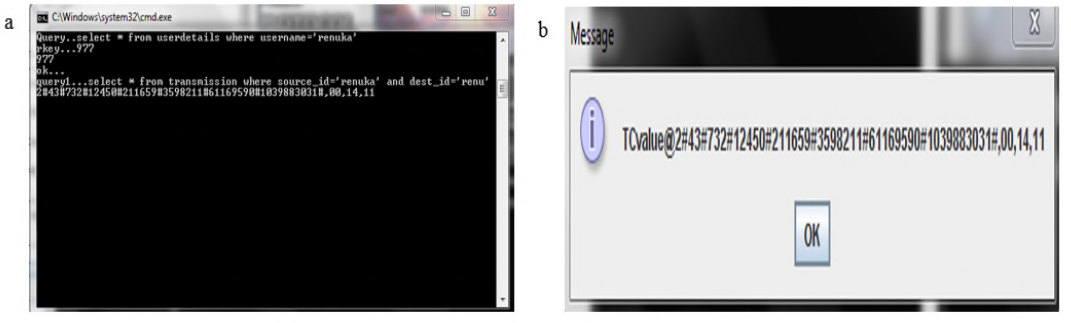

Fig5. (a)Sender's secret key displayed in receiver's window; (b) Generated session key value

The decrypted data can be received by the receiver.

5. Results and Discussions

Table1: Comparisons with other protocols

Comparison	Proposed Quantum key and classical key	Quantum key	Model Classical key Model
Pre-shared Secret key	Longer Duration	EPR Pairs	Longer Duration
Communication Round	2	5	3
Quantum Channel	Yes	Yes	No
Clock Synchronization	No	No	No
Vulnerable to Passive Attack	No	No	Yes
Security Proof			

Digital Signatures	Yes	No	No
Vulnerable to man-in –the middle attack	Yes	No	Yes
	No	Yes	No

The table shows that pre-shared secret key is used in longer duration, because without the authentication trusted center cannot display the secret key. Quantum cryptography uses pre-shared EPR pairs between trusted center and participants to solve man-in-the-middle attack. In proposed scheme we can use best digital signatures authentication scheme.

Results revealed that by combining the classical cryptography and quantum cryptography the number of rounds for communication can be reduced. It can solve the man-in-the-middle attacks, replay attacks, and it provides best authentication.

The trusted center solves the replay attacks i.e. the trusted center checks the data sent from sender to receiver by generating quantum bits and random key. QKD solves the passive attacks.

The pre-shared secret key is used by users to provide authentication. This pre-shared secret key can be used for long duration because it can't be revealed by trusted center without authentication.

6. Conclusion

By combining the classical cryptography and quantum cryptography we can provide the authentication and number of rounds for communication can be reduced. Authentication is possible through digital signatures in classical cryptography. Quantum cryptography solves the large number of rounds for communication and secret-key distribution. Proposed model can be more effective as compared to other, particularly with digital signatures and quantum channels. Qubits cost can be reduced in future. Trusted center can be more effective to solve replay attacks and to provide secure session key using secret key, random number and qubits. In large networks security can be attained by combining techniques with digital signatures.

7. References

[1] 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,pp. 71-80, Vol. 4, No. 1, March2007

[2] C.H.Bennett, "Quantum Cryptography Using any Two orthogonal States, "Physical Rev. Letters, vol.68,no. 3121, 1992.

[3] N.Asokhan, V.Niemi, and K. Nyberg, ""Man-in-the-Middle in Tunnelled Authentication Protocals," Proc. Int'l Workshop Security Protocols, 2003.

[4] Aysajan Abidin, "Weaknesses of Authentication in Quantum Cryptography and Strongly Universal Hash Functions," Linköping studies in science and technology, 2010

[5] Tasleem et al., "Hybrid Approach: Combining Classical Cryptography and QKD for Password Authentication," International Journal of Computer Science & Communication Networks, Vol. 2, No. 4, pp. 512-515

[6] Dr.G.Ananda Rao et al., "Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography," Indian Journal of Computer Science and Engineering, pp.143-145, Vol. 2, No. 2, May 2011

[7] T.S.Thangavel and A. Krishnan, "Integrated Quantum and Classical Key Scheme for Two Servers Password Authentication," Journal of Computer Science, Vol. 6, No. 12, pp. 1396-1405, 2010

[8] M. Bellare and P. Rogaway, "Provably Secure Session Key Distribution: The Three Party Case," Proc. 27th ACM Symposium Theory of Computing, pp. 57-66, 1995.