Industrial Engineering Journal
ISSN: 0970-2555
Volume : 49, Issue 8, No. 1, August : 2020

# A QUANTUM CRYPTOGRAPHY BASED SECURITY FOR DIGILOCKER USING HYBRID QUANTUM CRYPTOGRAPHY

**PULATIPALLI SHABANA**
Associate Professor
Shabana.mtech@gmail.com

**P BHARATH KUMAR**
Assistant professor
Bharathkumar1218@gmail.com

**E ANITHA**
Assistant Professor
Anitha.alts@gmail.com

## Abstract

The provision of security in big networks often makes use of cryptography as a method. Both traditional cryptography and its more modern counterpart, quantum cryptography, are methods that see widespread use. Traditional cryptography provides security via the use of straightforward mathematical procedures. As a result, it is much more susceptible to a variety of assaults, including eavesdropping, man-in-the-middle attacks, and others. However, in traditional cryptography, digital signatures are the method of choice for providing the highest level of authenticity. Quantum cryptography is a method of providing security that makes advantage of the features of quantum mechanics. Although it makes use of photons and polarisation, it needs additional communication rounds. Therefore, by combining traditional encryption with quantum cryptography to demonstrate a novel combination. When it comes to providing the highest level of authentication, we have the option of using both implicit user authentication and explicit mutual authentication, as well as digital signatures. The government developed the programme known as DigiLocker in order to safeguard a variety of important papers, including Aadhaar and income certificates, amongst others. We may thus create a combination of conventional and quantum encryption in order to give the highest level of protection and authentication for DigiLocker.**1.**

## Introduction

The "Digital Locker" service known as DigiLocker was first introduced by the Government of India in February of 2015. Its purpose is to make available to resident Indian people a safe online repository in which they may save their official papers. We may keep important documents like Aadhaar cards, PAN cards, voter id cards, and so on at this location. Each user has access to 1 gigabyte (GB) of storage space inside DigiLocker to save their papers. By using this, we will have the ability to attach the capability for electronic signature of the papers. DigiLocker provides its users with the ability to store their important documents. Therefore, we are obligated to provide the authentication and security. In order to do this, we may utilise a technique that is a combination of classical and quantum cryptography. Traditional cryptography provides security via the use of straightforward mathematical procedures. As a result, it is more susceptible to several assaults, including passive attacks and man-in-the-middle attacks, among others. Traditional cryptography relies on a challenge-response method to protect against replay attacks; however, this approach needs additional communication rounds. In traditional cryptography, authentication may be provided by using something called a digital signature. A digital signature is a digital code that is appended to a document before it is electronically sent so that the contents of the document may be verified. The provision of security may be achieved by the employment of simple mathematical procedures using quantum cryptography. Photons and polarisation are used in the process. Quantum cryptography provides a solution to a variety of assaults, including passive attacks, eavesdropping, and others. In the absence of adequate authentication, it is susceptible to attacks using a man in the middle. Quantum cryptography makes it harder to employ digital signatures, and it also demands additional communication rounds during the phase when the key is being exchanged. Therefore, the highest possible security and authentication may be achieved by combining conventional encryption with quantum techniques. We are able to include this level of protection into DigiLocker. Authentication methods such as digital signatures, implicit user authentication, and explicit mutual authentication may all be used here.

## 2. Literature survey

Classical cryptography and quantum cryptography are related in the article [1], where the authors claim that security in massive networks may be supplied based on quantum key distribution protocols by linking the two types of encryption. They discussed both implicit and explicit mutual authentication techniques that they devised in order to talk about their efforts. Eavesdropping and other forms of assault, such as securing replay, are among their specialties. Their suggested procedures have the potential to increase efficiency via the provision of the fewest possible rounds of quantum key distribution (QKD). A fresh approach to guaranteeing safety has been developed, and it makes use of the idea of the Unbiased Chosen Basis, or UCB. According to UCB, the no-cloning approach and quantum measurement that are used in QKD enable it to offer a secure key that is resistant to assaults from the other participants. The qubits are evaluated for measurement depending on the bias, which might be either a rectangle or a diagonal basis. According to the declaration of the no-cloning proposal, an unknown quantum state cannot be replicated, nor can an attacker copy the qubits in the system if the attacker is uninformed of the polarisation. These efforts that are being offered provide a novel approach to assessing QKDPs.

In quantum cryptography, the study of highly universal hash functions is done in [4] with the goal of better understanding authentication. The weaknesses that may be exploited by man-in-the-middle attacks are investigated. The estimated encrypted tags are determined with the help of the authentication lifespan. This proposes more basic precautions, such as utilising an auxiliary key for additional authentication, minimising the amount of information that is leaked, and often altering the secret hash function. Additional research concepts are presented in order to employ authentication methods that need fewer keys while maintaining a high level of security.

In [5,] the authors concentrate on constructing a safe model for massive networks, similar to what they did in [1, 2]. They integrate the physics of conventional encryption with those of quantum cryptography in this approach. This article discusses the QKD framework, together with the network architecture and services that make up the security it offers. UCB is used in order to provide a security proof for QKDP. It says that QKD offers increased safety thanks to the use of polarisation. It is necessary to utilise a session key in order to exchange the secret keys on several occasions over an extended period of time. This type is capable of efficiently fending off replay assaults as well as passive attacks.

In [6], just as in classical cryptography, the techniques that are presently being employed are unsafe and open to the possibility of passive attacks. Quantum cryptography offers a solution to these types of attacks, however. In order to ensure that the transmissions between the participants are kept safe, the combination of implicit and explicit QKDP has been presented as a solution. This has been accomplished by combining traditional encryption with quantum cryptography. This suggested method makes use of dynamic multicast systems that are built on bilinear maps, which might help address scaling concerns further. The use of Identity-tree is what enables authentication to take place. Within the confines of this plan, it is possible to maintain both forward and backward secrecy.

[7] introduces the idea of multi-server, which refers to an authentication system in which a person may simultaneously contact with many servers in order to verify their identity. This demonstrates a two-server setup that engages in direct communication with the user and is visible to the service server. Both the Classical Key Exchange (CKE) and the Quantum Key Distribution (QKD) models are used here. It suggests combining the two different theories into one coherent whole.

## 3. Proposed body of work

In this hybrid approach to classical and quantum cryptography, the participant and the TC reach an agreement on their polarisation by using a secret key that was previously exchanged between them. At the moment that the key is being distributed, these secret keys, together with the random string, may be used to generate another encryption key and encode the session key. Even if session keys that are very close to one another are communicated, the receiver will not be able to receive qubits with the same polarisation.

There are two types of user authentication presented here: implicit and explicit. The implicit user authentication guarantees that only approved users are able to access secret information, hence preventing unauthorised access. Explicit user authentication is available after a secure communication session that makes use of a session key. In addition, digital signatures should be added upon explicit authentication.

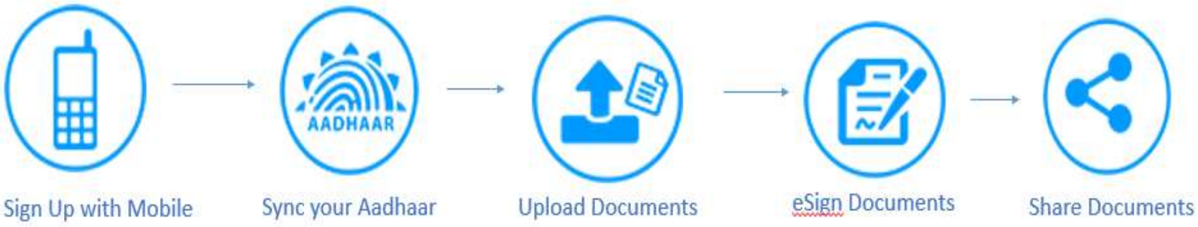

Fig1: Digi Locker Process

Fig shows the process to store the documents in DigiLocker. First we can sign up by using the mobile. Then synchronize the document and upload that document. After uploading we can provide security and authentication by using the hybrid classical and quantum cryptography in the background. Then this documents can be opened only by using security key.

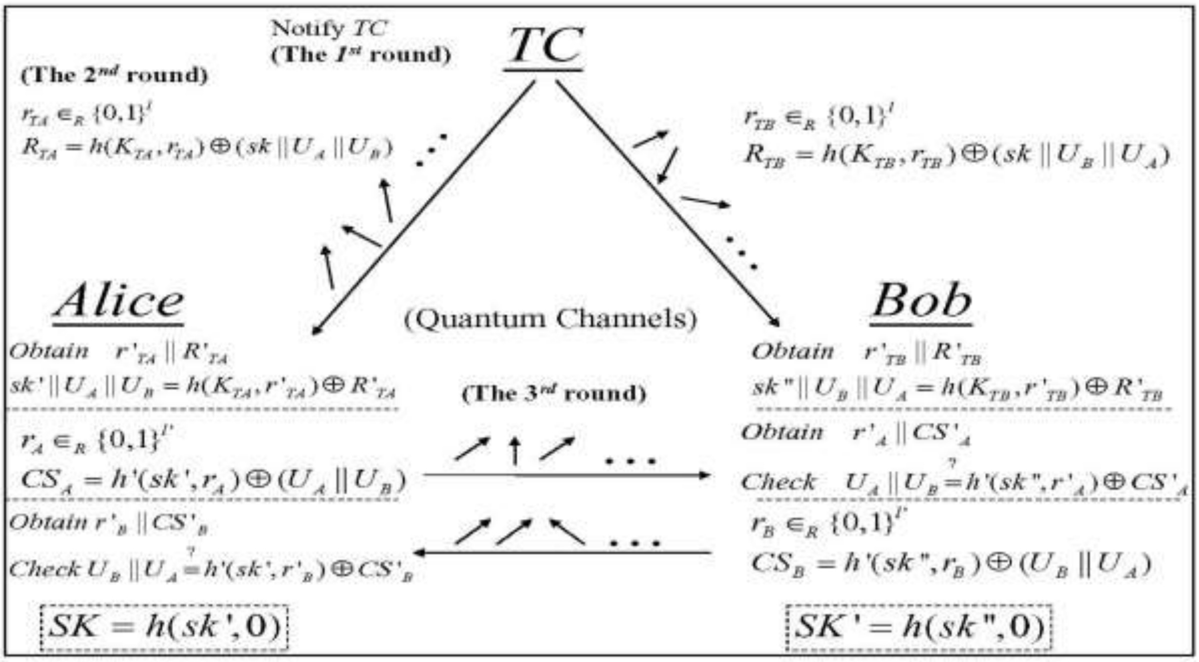
Notify $TC$
(The 1st round)
$TC$
(The 2nd round)
$r_{TA} \in_R \{0,1\}^l$
$R_{TA} = h(K_{TA}, r_{TA}) \oplus (sk \| U_A \| U_B)$
$r_{TB} \in_R \{0,1\}^l$
$R_{TB} = h(K_{TB}, r_{TB}) \oplus (sk \| U_B \| U_A)$
Alice
(Quantum Channels)
Bob
Obtain $r'_{TA} \| R'_{TA}$
$sk' \| U_A \| U_B = h(K_{TA}, r'_{TA}) \oplus R'_{TA}$
(The 3rd round)
Obtain $r'_{TB} \| R'_{TB}$
$sk'' \| U_B \| U_A = h(K_{TB}, r'_{TB}) \oplus R'_{TB}$
$r_A \in_R \{0,1\}^{l'}$
$CS_A = h'(sk', r_A) \oplus (U_A \| U_B)$
Obtain $r'_A \| CS'_A$
Check $U_A \| U_B \overset{?}{=} h'(sk'', r'_A) \oplus CS'_A$
Obtain $r'_B \| CS'_B$
Check $U_B \| U_A \overset{?}{=} h'(sk', r'_B) \oplus CS'_B$
$r_B \in_R \{0,1\}^{l'}$
$CS_B = h'(sk'', r_B) \oplus (U_B \| U_A)$
$SK = h(sk', 0)$
$SK' = h(sk'', 0)$

Fig a: Key distribution phase(Source:[1])

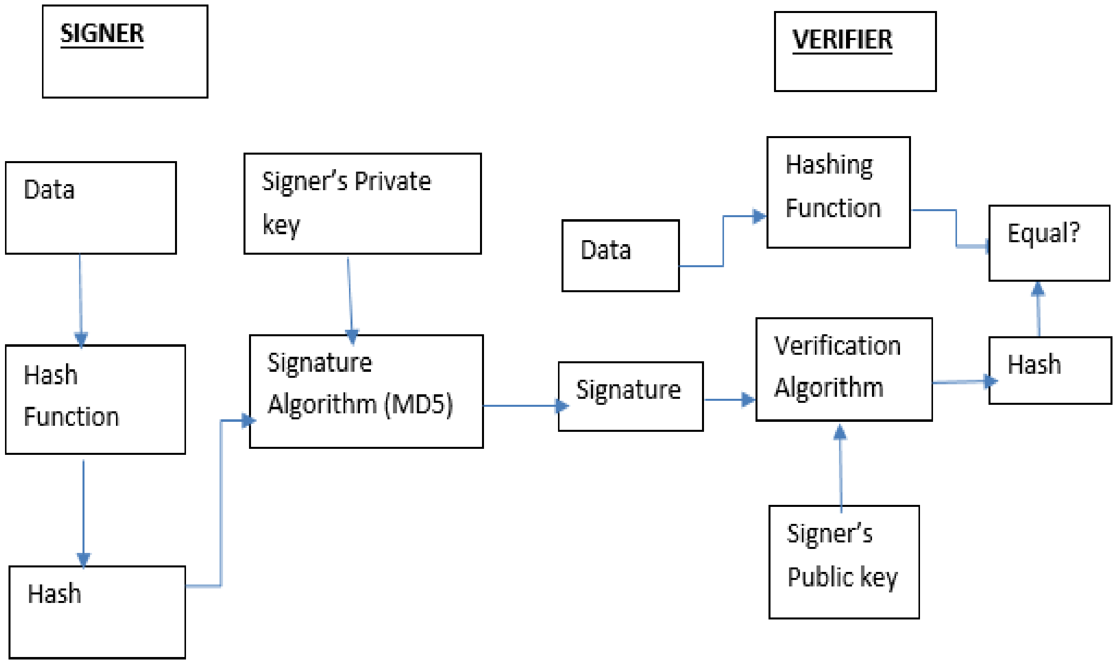

Fig b: Digital signatures

Fig2: Proposed integrated classical cryptography and quantum cryptography scheme

a) Key distribution phase
b) Adding digital signatures using session key

Below algorithm shows how to provide security by using hybrid classical and quantum cryptography.

## 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.ey

## Key Distribution Phase

1. First IMA 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/√2 (|0> +|1>)
- If $(r_{TA} || R_{TA})$i=1, $(K_{TA})$i=0,
  Then $(Q_{TA})$I is 1/√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'

$SK=h(sk',0)$

$SK'=h(sk'',0)$

**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
- 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.

**Security Proof**

UCB assumption in quantum cryptography can be done.

**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 so many number of participants can exist.

**Long-term secret key**

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

## 4. Efficiency of Proposed work compare to other protocols

**Table1: Comparison with other protocols**

| **Comparison** | **Proposed Quantum key and classical** | **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 | Yes | No | No |
| Digital Signatures | Yes | No | Yes |
| Vulnerable to | No | Yes | No |

| | | | |
|---|---|---|---|
| man-in –the middle attack | | | |

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.

## 5. Conclusion and Future Work

When we combine traditional cryptography with quantum cryptography, not only are we able to offer security and authentication, but we are also able to cut down on the number of communication rounds. We have the option of using implicit user authentication in addition to explicit mutual authentication and the addition of digital signatures. The DigiLocker programme is a good candidate for incorporating this security and authentication. Therefore, the suggested approach is superior to others in terms of its effectiveness when it comes to providing authentication and security. In the future, the price of qubits may be lowered. A trusted centre may be more successful at preventing replay attacks and providing secure session keys by making use of a secret key, a random number, and qubits. Combining several security methods with digital signatures allows for the protection of even the largest networks. The combination of conventional and quantum encryption offers the highest level of authenticity and protection. Therefore, we will be able to use this to any purpose going forward.

## 6. 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.