UNIVERSITI PUTRA MALAYSIA

ENHANCED TIGHT FINITE KEY SCHEME FOR QUANTUM KEY DISTRIBUTION PROTOCOL TO AUTHENTICATE MULTI-PARTY SYSTEMS IN CLOUD INFRASTRUCTURE

ROSZELINDA BINTI KHALDI

FSKTM 2018 87

ENHANCED TIGHT FINITE KEY SCHEME FOR QUANTUM KEY DISTRIBUTION PROTOCOL TO AUTHENTICATE MULTI-PARTY SYSTEMS IN CLOUD INFRASTRUCTURE

By

ROSZELINDA BINTI KHALID

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

July 2018

COPYRIGHT

DEDICATION

Dedicated to the human beings

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

ENHANCED TIGHT FINITE KEY SCHEME FOR QUANTUM KEY DISTRIBUTION PROTOCOL TO AUTHENTICATE MULTI-PARTY SYSTEMS IN CLOUD INFRASTRUCTURE

By

ROSZELINDA BINTI KHALID

July 2018

Chairman : Prof. Zuriati Ahmad Zukarnain, PhD
Faculty : Computer Science and Information Technology

The aim of this study was to propose a unique communication protocol for authentication scheme for cloud infrastructure in replacing the key distribution technique based on public key infrastructure to achieve unconditional security in cloud with enhanced tight finite key. Currently, there are certain issues pertaining to confidentiality, integrity and authenticity in cloud systems. In our research we propose the use of quantum theory to transfer the authentication key via quantum channel. Referring to quantum theory, every key that we transform into bits cannot be cloned. This QKD protocol is believed to be able to detect any eavesdropping activities and provide an effective security. The Quantum Key Distribution (QKD) protocol used the concept of Multiparty QKD (MQKD) which allows the same key to be distributed to different parties based on quantum mechanism. A quantum key server generates a secret key that may strengthen the security aspects. A quantum key distribution key scheme is imposed in the cloud network to secure the top-secret message or information and capture the eavesdropper. The existence of quantum key storage between the cloud provider and cloud client may guarantee the integrity of communication process that ensures the party is authenticated and the communication cannot be intercepted. We propose the enhanced tight finite key scheme for quantum key distribution (QKD) protocol to authenticate multi-party system in cloud infrastructure. The main attraction is to provide a secure channel between a cloud client to establish a connection among them by applying the theories from Von Neumann and Shannon entropies and also Shor's algorithm. By generalizing these theories we will produce enhanced tight finite key scheme for quantum key distribution (QKD) protocol to authenticate multi-party system in cloud infrastructure. Hence we are using quantum channel and also quantum key distribution (QKD) together with BB84 protocol replacing common channel to distribute the key.

The result shows that our proposed method could improve the error rate. This is due to any noise, interference, distortion or bit synchronization during the transmission of the initial key that error rate can be slightly reduced the error rate by implementing our new scheme. In other words it can push aside any interference during the key transmission. Our result shows the authentication level is increased to 30% compared to existing methods proposed by other researchers. In general, the current authentication scheme being used is still relatively backward methods especially in cloud environment. Many of the key aspects of authentication cannot guarantee effective control, especially in data transmission via a public channel. From the result we can see there is a significant result on reducing the error rate, enhanced the authentication level and reduce the possibility of any kind of threat. The simulation results show that our proposed scheme provides a strong authentication mechanism. It shows by the low amount of error rate while the key is distributes among others. In addition, our results show that the proposed scheme could reduce amount of information leak.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENIGKATAN SKIM KERETAIAN KUNCI UNTUK PROTOKOL KUNCI KUANTUM TERAGIH BAGI PENGESAHAN SISTEM MULTI PENGGUNA DALAM INFRASTRUKTUR AWAN

Oleh

ROSZELINDA BINTI KHALID

Julai 2018

Pengerusi : Prof. Zuriati Ahmad Zukarnain, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Tujuan kajian ini adalah untuk menghasilkan satu protokol pengesahan komunikasi yang unik khusus untuk infrastuktur awan dengan menggunakan peningkatan skim keretaian kunci. Buat masa ini terdapat tiga perkara utama yang menjadi isu dalam aspek keselamatan adalah kerahsian, integriti dan kesahihan maklumat didalam sistem awan. Di dalam kajian ini kami mencadangkan menggunakan teori kuantum yang mana kunci pengesahan di hantar melalui saluran kuantum. Merujuk kepada teori kuantum bahawa setiap kunci yang dihantar mewakili bits tidak boleh ditiru atau dibuat salinan. Protokol Agihan Kunci Kuantum dipercayai boleh mengenalpasti kehadiran penceroboh dan memberikan kawalan keselamatan yang efektif. Protokol Kunci Kuantum menggunakan konsep multi pengguna yang membenarkan kunci yang sama diagihkan kepada pengguna yang berbeza merujuk kepada mekanisma kuantum. Server kuantum akan menjana kunci rahsia bagi memperkukuhkan dari aspek keselamatan. Agihan kunci kuantum ini akan digunakan didalam rangkaian awan untuk memastikan tahap keselamatan terhadapa maklumat rahsia tertinggi atau maklumat sulit diceroboh oleh penceroboh. Dengan wujudnya pangkalan data kunci kuantum diantara pembekal awan dan pelanggan awan ianya dapat menjamin integriti proses komunikasi tersebut daripada dipintas. Kami mencadangkan peningkatan skim keretaian kunci untuk protocol kunci kuantum teragih bagi pengesahan sistem multi pengguna dalam struktur awan. Perkara yang menjadi tarikan utama adalah ianya menyediakan saluran yang selamat diantara pelanggan awan to menghasilkan sambungan antara mereka dengan mengguna teori daripada Von Neumann, Shannon entropi dan juga algoritma Shor. Dengan menggunakan teori ini kami menghasilkan peningkatan skim keretaian kunci untuk protocol kunci kuantum teragih bagi pengesahan sistem multi pengguna dalam struktur awan. Disamping itu juga, kami menggunakan

saluran kuantum dan kunci kuantum teragih dengan protocol BB84 bagi menggantikan saluran yang biasa untuk agihan kunci.

Keputusan menunjukkan skim yang diperkenal ini dapat menambah baik dari segi kadar ralat. Oleh kerana gangguan luar semasa proses penghantaran kunci utama yang mana boleh dikurangkan dengan menggunakan skim yang dicadangkan. Keputusan kami menunjukkan paras kesahihan yang diperolehi adalah meningkat kepada 30% berbanding dengan kaedah yang diperkenal oleh penyelidik terdahulu. Secara keseluruhan kaedah pengesahan sedia ada masih menggunakan kaedah lama terutamanya dalam persekitaran awan. Kebanyakkan perkara utama dalam pengesahan tidak dapat memastikan kawalan yang efektif terutama semasa trasmisi data melalui saluran awam. Daripada keputusan kami dapati terdapat keputusan yang berkesan dalam mengurangkan kadar ralat, peningkatan dalan paras pengesahan dan mengurangkan kebarangkalian pencerobohan. Melalui keputusan simulasi, skim yang kami cadangkan menghasilkan mekanisma pengesahan yang kukuh. Ianya menunjukkan jumlah kadar ralat yang berkurang semasa kunci diagihkan diantara mereka. Sebagai tambahan, keputusan yang kami perolehi juga dapat mengurangkan ketirisan maklumat.

ACKNOWLEDGEMENTS

This thesis appears in its current form due to the assistance and guidance of several people. I would, therefore, like to offer my sincere thanks to all of them. First of all, I would like to express my profound appreciation toward my advisor Prof. Dr Zuriati Ahmad Zukarnain, who encouraged and helped me throughout the process of research and writing of this dissertation.

It gives me great pleasure to acknowledge the support of my committee members, Assoc. Prof. Dr Zurina and Dr Affendi, for their valuable comments and suggestions.

I would like to thank all my friends at Universiti Putra Malaysia for surrounding me with their kindness and support. Public Service Department for the schorlarship.

This research is supported in part by the Ministry of High Education (Fundamental Research Grant).

This dissertation is dedicated to my beloved family: my father Encik Khalid Bin Mohd Nor, mother Puan Sharifah Fatimah Helen Been Binti Syed Abd Aziz, sister Khalifatul Azura, brothers Mohd Firdaus, Mohd Redzuan , Hazman and my late grandmother Almarhumah Hajjah Sharifah Azizah Binti Syed Abd Rahman I cannot find words to express my appreciation to them for their unceasing encouragement and love.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Zuriati Ahmad Zukarnain, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zurina Mohd Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohamad Affendi Mohamed, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: _____ Date: _____

Name and Matric No: Roszelinda Binti Khalid, GS33594

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Prof. Zuriati Ahmad Zulkarnain

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Zurina Mohd Hanapi

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Mohamad Affendi Mohamed

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
AP	Access Point
CA	Certification Authority
DVS	Designated Verifier Signature
DV	Discrete Variable
EC	Error Correction
EF-CMA	Adaptive Chosen-Message Attacks
ECC	Error Correction Code
GOTP	Graphical One-Time Pad
GTK	Group Transient Key
IT	Information Technology
IBER	Initial Bit Error Rate
IaaS	Infrastructure-as-a-Service
IR	Intercept-Resend
KDC	Key Distribution Centre
KCK	Key Confirmation Key
KEK	Key Encryption Key
MIM	Man-In-Middle
MASP	Managed Authentication Service Provider
MQKD	Multiparty Quantum Key Distribution
MIC	Message Integrity Code
MSK	Master Session Key
OTP	One-Time Pad
OSI	Open System Interconnection
PKI	Public Key Infrastructure
PUF	Physical Unclonable Function
PaaS	Platform-as-a-Service
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
PMK	Pairwise Master Key

PBS	Polarizing Beam Splitters
PNS	Photon Number Splitting
QC	Quantum Cryptography
QIS	Quantum Information Science
QKD	Quantum key distribution
QBER	Quantum Bit Error Rate
QDC	Quantum Direct Communication
QCSC	Quantum Cloud Service Center
QSS	Quantum Secret Sharing
RA	Registration Authority
SaaS	Software-as-a-Service
XOR	Exclusive OR

CHAPTER 1

INTRODUCTION

This section is designed to explain the importance of information security in the cloud. Secure communication is the most prominent aspect in digital communication. Massive amounts of information are transferred over a digital channel every bits and continuously that includes the top profile information. The government is aiming for Malaysia to be a data center hub by the year 2017. Therefore a secured communication channel became a major concern by the Malaysian government recently. Besides the secured communication channel the world is moving to cloud computing. Cloud computing requires a secure communication channel as a medium for transferring the information among the clouds. Cloud computing technology is a new computing trend in which people only need to pay for the services without any cost to buy physical hardware. Cloud computing also defined as Internet-based computing, where people are able to share resources, software, and information provided by vendors on demand. Organizations as Cloud Service Provider gain benefits from cloud computing technology, including low service cost, scalable and flexible network model, and easy maintenance. Cloud computing model is to allow the service accessible from anywhere, and the accessibility relies on user demand.

In the era of cyber-attacks and global electronic surveillance, ordinary users, researchers and security expert are considering any possibilities to secure their communications. The most demand technique use to secure their communication is cryptography via the use of an encryption key. Cryptography is working with an encryption algorithm. The encryption algorithm is where the message needs to be encrypted and decrypt before the recipient can read the message. Cryptography as well can be applied to the authentication scheme.

Thus the authentication scheme for a multiparty system is the primary concern for secure communication in the cloud infrastructure. There are lots of challenges to secure the interaction among the multiparty system, and one of them is how to ensure the communication only happens between legitimate users in cloud infrastructure.

1.1 Background

Apparently, cloud computing are using a cryptography model to ensure their security level. The used of cryptography model based on complexity assumption. Also, the user of cloud computing is looking for a storage infrastructure to store a massive amount of data securely. Cryptography is a method that provides users with the four top factors of security, which are confidentiality, authenticity,

integrity, and non-repudiation. Depending on the applications, there is a decision between the elements. The critical aspect and challenge of cryptography is the secure communication channel to transfer the information.

The secure transmission is begun in 1917 when Vernam (Vernam, 1926) proposed a One-Time Pad (OTP). With a one-time pad (OTP) the sender and receiver use the same symmetric secret key to exchange the information. In principle, the key should not be the same to prevent from being a break. In conjunction with that, Claude Shannon introduced a new concept of perfect secrecy (C E Shannon, 1948).

According to Shannon the OTP can achieve to ideal secrecy if it satisfies the dictate requirements. However, to obtain the ideal secrecy is not practical due to generate the perfect random OTP. In theory, the total secrecy could be possible because it is more or less deal with the complexity of the calculation. As for now, researchers are still cannot prove any cryptosystem that can offer perfect secrecy in real implementation.

Evolving of technology with quantum technology, the barriers and possibility to achieve the absolute secrecy is possible. As yet, quantum-based cryptography has obtained the random generation and secure key distribution. Thus, perfect secrecy will be no more fiction in the future. Despite its promises, Quantum Cryptography (QC) is still in the early stage of the development phase from the emerging field of Quantum Information Science (QIS). To achieve the conventional cryptography or digital cryptography of success, QC needs to endure various challenges and tasks. This thesis focuses mainly on authenticated secret key distribution for cloud network using quantum protocol and digital cryptography techniques. Then, the contributions meant for an efficient scheme that combines the quantum theory and digital cryptography techniques. Every session in quantum theory will create some photons that represent keys. Only the selected number of photons becomes bits for cryptography key. The sender and receiver will use this cryptography key.

The main issue in cloud network is when transferring the information via a classical channel. There is 80% possibility of the information can be intercepted. Quantum key distribution has come as an innovation to secure key distribution process. The second issues that we are tackling are the exchange key generation rates is still unstable. Therefore, besides having a complexity cryptography algorithm, we are applying quantum theory to the quantum protocol in cloud authentication.

1.2 Limitation of Authentication in Cloud Infrastructure

In cloud infrastructure there are several authentication schemes to ensure the security of the information is in hand. The widely used is Public Key Infrastructure (PKI) which implement the asymmetric cryptograph. In general PKI is including

the security policies and encryption mechanism. The concept of identifying dedicated user with public and private makes user gain trust to use it. Basically the architecture may involve the action of generate, store and manage the keys for communication purposes. This will produce a key and digital certificate. Mainly in PKI there are role in order to produce a digital certificate. There will be a Certification Authority (CA) who may generate the key, Registration Authority (RA) who may register the legitimate user base on the generate key and Validation Authority (VA) who may validate the registration. PKI is actually a mechanism for public key cryptography to publish the public key. It describes the various policies, their standards, and the necessary software that are used to regulate X.509 based certificates, public & private keys (Arifeen et al, 2015). In Ziyad & Rehman (2014) they performed a critical review on providing an authentication mechanism for cloud infrastructure. They categorized in different needs in specified cloud infrastructure. Table 1.1 summarizes the literature on digital authentication on the classical approach to cloud infrastructure. In the context of digital authentication, most of the literature in the table is using multi-factor authentication to harden the security. However, we found that there is a threshold where the concept of One-Time Pad (OTP) as a digital authentication is still being implemented. There is a possibility the information is breakable. As we have described in the previous section, OTP is using the same key between the sender and receiver that are prone to man-in-middle attack.

With this classical approach, each of the information is represented in bits when it can be transferred via a communication channel. The major limitation in classical digital cryptography is the bit can be duplicated without any notification.

Table 1.1 : Literature on Cloud Infrastructure Authentication

Method/ Scheme	Advantages	Disadvantages	Future Direction
Authentication in the Clouds: A Framework and its Application to Mobile User (Chow et al., 2010)	The authentication is executed on the client's behaviour.	The authentication validation was identified against a defined threshold. However, the best result relies on the application.	A strong technique dedicated for clouds. The combination of infrastructure and authentication method.
Two Factor Authentication (Shen et al., 2010)	The method is strong and difficult to be hacked and able to protect against phishing and reply attacks.	The method are not cover on mobile application and prone to security breach.	Need to design a system that will authenticate the user with the feature other than possession of the Mobile phone.
A Strong User Authentication Framework for Cloud Computing (Choudhury et al., 2011)	Proposed a mutual agreement phase in for cloud computing.	The local system does password and smart card verification.	The framework needs to provide formal security proof.
Two-Factor Authentication System Based on Extended OTP Mechanism (Ku et al., 2013)	The mechanism introduces Graphical One-Time Pad (GOTP) authentication which can protect password stealing by a man-in-the- middle attack	GOTP technique is not that much sophisticated because of the image stored in the server with plain text format, and the images will remain the same for all login sessions.	Using a separate channel apart from the application server to generate an OTP.
Multi-level authentication technique for accessing cloud services (Dinesha & Agrawal, 2012)	Central server supplies credential to the application server. Hence no multiple authentications for different applications.	The authentication server is centralised. However, there is a possibility of single point failure.	Detail study on central authentication need to be done.
Toward Secure Strong Designated Verifier Signature Scheme from Identity-Based System (Lin, 2014)	A Designated Verifier Signature (DVS) scheme gives priority to the sender and receiver recognised them self by signature. The signature based on identity. It is not allow to send any data to third party without verification.	Compared with related works, the proposed scheme also has lower computational costs.	Additionally, the security requirement of unforgeability against Existential Forgery on Adaptive Chosen-Message Attacks (EF-CMA) formally proven in the random oracle model.
Continuous and transparent	Using multimodal trusted authentication scheme	Issues on transparency universality,	A scheme more user-friendly and

Method/ Scheme	Advantages	Disadvantages	Future Direction
multimodal authentication: reviewing the state of the art (Al Abdulwahid et al., 2016)	with biometric authentication have an issues regarding the universality and circumvention.	interoperability, scalability, high performance, and real data.	flexible to apply on any kind of network architecture.

1.3 Classical Authentication Protocol in Classical Communication Protocol

The authentication of public messages is a fundamental problem nowadays in network communications (Assis et al, 2012). The scenario is when two parties going through a communication there a must be a message to send out. Let's say we have Alice and Bob as a playing actor in this scenario. Alice will send her message via a public channel. In order to ensure it authenticity, the message will send together with the identifier. Most of the mechanisms are using the tagging system as an identifier. With the tag, Bob could verify either the message is genuine or being tampered. Now, we put the situation whereby the communication process is prone to attack. Here Eve role as an intruder. She will try to intercept the message by sending the false tag. However, Bob will only transfer the message to Eve only when he believe the tag is true. We may see, in this situation even in secure communication where we provide the encryption mechanism of the message, the authentication tag may resolve the secrecy issue and authentication issue. The authentication is the critical components for any kind of digital system. Quantum key distribution (QKD) offers unconditionally secure message transfer by providing a dedicated channel. The idea behind QKD is to send an authentication using a key to ensure the message receive by the authenticate user. According to research perform by (Rass, 2007) there are no approach to secure the communication from the man-in-middle attack. The common mechanism that is being used is password authentication. In a huge communication network the authentication architecture has been move to the use of public key and private key concept. Public key and private key concept is implemented in Public Key Infrastructure. However, in public key infrastructure there are still prone to man-in-middle attack because the unauthorized user could mimic the legitimate user by copying the key. (Rass, 2007) has introduced the authentication method in quantum network by exchanging the secret keys using quantum cryptography. Some of the existing authentication schemes established on client-server architecture been reviewed. Authentication is a simple function where one party presents a set of credentials to a system. If the credentials have a match on the system, the system returns a value that represents authorization; otherwise, it does not. The purpose of authentication is to verify that the specific information presented represents a request to be authentic from a specified entity (Bresson & Chevassut, 2001; Cariolaro, 2015).

Currently, most of the web-based systems are using a simple ID/password mechanism for achieving the goals associated with the identification and authentication. One of the most popular and earliest remote user authentication schemes was suggested by Lamport (1981); the server kept the hashed value of a user's password. In Lamport's scheme, password table was used to verify the legitimacy of users, but if this password table is compromised, stolen, or modified by an adversary, then the system could be partially or completely compromised. Some more recent smart card based password authentication schemes have also been proposed (An, 2012; Huang, Liu, & Chen, 2013; Li, Niu, Khurram Khan, & Liao, 2013). Earlier age, Shoup-Rubin (Shoup & Rubin, 1996) proposed an extension of the Bellare-Rogaway (M.Bellare, 1995) model which based on three-part key distribution protocol. Smartcard is used to store the long-term secret key and assumed that the smart card is never be compromised. The scheme falls in the one-factor category as two-factor schemes can be broken by compromising both the factors only. Liao et al. (2006) and Ziyad & Rehman (2014) tried to consolidate some passwords and smartcard-based properties and proposed two-factor smart card and password authentication scheme, which is still vulnerable to many attacks. Cloud computing is a variant of client-server architecture, where, thousands of clients use the same infrastructure on a large scale.

Consequently, it needs stronger authentication than the conventional client-server internetworking system. Banyal et al (2013) have proposed public key and mobile out of band based authentication for cloud computing. Some systems use more complicated authentication using the smartcard system Pippal et al (2012), where a user typically has an ID, a password, and also a time-generated passkey from the smart card which changes every 60 seconds. It represents the case possessing something physically. Other types of authentication that involve our body recognition is known as biometrics authentication. So, far these types of authentication consider the most secure authentication method because of the uniqueness of our body. Parts of the body usually use as the identifier are fingerprints and retina scan. The key of security is actually begin with the authentication. The security breach usually happened when there is unauthorized user trying to attempt the attack. If at the first layer we have strengthened it, there is no way the unauthorized user could intercept into our system. However, in current authentication there are security flaws that we can still mitigate. We frequently use the password, but we must aware that these types of authentication are prone to any kind of man-in-middle-attack (Banyal et al., 2013).

1.4 Key Distribution Scheme and Digital Cryptography

Cryptography is the problem solver involving two or more parties that may involve complexity to gain trust from one another. The issue happened when in digital communication they need to send a secret message. Supposedly two parties are required to communicate secretly. There are two types of cryptographic which are private key cryptosystem and public key cryptosystem.

With private key cryptosystem two parties will assign, the sender and receiver. The sender and receiver will communicate by sharing a private key. Sender need to confirm the form of the key to encrypt the message before send to receiver. The cryptography process will happen here, where the message will get encrypted and then decrypted. The message needs to decrypt using the shared key for the original message. The shared key must be a private key for the sender and receiver. Only sender and receiver who have the private key could have the original message. However, there are issues regarding private key cryptosystems. Most of the researchers are question on how to distribute the key. They found, the main issue is the communication that been used for a while. The communication channel allows the intruders to intercept the key exchange process that may lead to main-in-the-middle attack. Then the intruders can decrypt the message with the intercept key.

Quantum computation and quantum information researchers are fully utilize the quantum mechanics theory in their implementation. By the implementation of quantum mechanics in computation and information they believe the computer performance will be speed up compare to supercomputer. In line with that, the security aspects should be contemplated as well. The researchers have discovered that quantum mechanics could be imposed in the concept of key distribution. Thus, the security in the communication over the quantum channel cannot be compromised. With quantum mechanics, the information is transform into light photon. It is impossible for the light to be copied or mimic. Here the quantum key distribution has been introduced. The quantum key will be shared among the legitimate parties. When there is interference during the quantum key distribution, the legitimate parties will notice it, and the communication will be aborted immediately.

1.4.1 Thrust for Quantum Key Distribution

In order to gain customer trust, most of the organizations are focusing in the reliability and security aspects. The existing method as such, digital authentication has been used but the flaws is still exist. Looking into the solution, a method with quantum mechanics theory has come to save the world. It is quantum key distribution that people may see a great solution to secure the key distribution process. QKD has a big potential to take place in today's world. It may ensure the integrity of the top secret message whereby. The QKD implementers believe that the current digital technology does need this kind of new technology. Most of the cyber-attack towards the communication channel becomes ordinary. The fix must be at the communication channel, and for sure the technique should be aligned with it. We must say there are huge different between the classical approach and QKD.

Asymmetrical cryptography or known as public key cryptography have a debate among the security expert. The proof that shows that it cannot be broken is still unclear. The idea is to exchange the key without any disturbance from intruders and to ensure there are no leaking key. It needs to implement neither in

conventional computing nor quantum computers. Even in QKD the concept of asymmetrical cryptography are been used. There will be an exchange the secret key between the legitimate parties. Theoretically QKD has a proof that it going to be secure in terms of man-in-middle attack. This is because the use of photon in key distribution. In industrial field the integrity of the data is a must. Information leakage is a crucial issue for them to handle. When the data or information located in the cloud infrastructure many of the industrial players afraid that their top secret will be disclosed or steal by unauthorized user. QKD would replace the conventional cryptography to achieve the perfect secrecy of the information. Despite of this, QKD could be deployed in quantum networks, classical communication network and in cloud network. As for organization, it is surely the best mechanism for banks, ministries and any kind of related industries in order to secure the message delivery over the communication network.

1.4.2 Limitation of Key Distribution and Digital Cryptography

Küchlin (1987) proposed the public-key encryption with RSA. The message is transferred via public channel which is not secure. With the public-key encryption with RSA the can identify the unauthorized users who try to intercept the message. However, it been protected by the private key. Only the user who has the dedicated can read the message. Here the concept of encryption and decryption been used.

The proposed authentication scheme in this thesis is a quantum key distribution with enhanced tight finite scheme mechanism that can be imposed in cloud infrastructure. Table 1.2 summarized the digital authentication in Buhari et al (2012).

Table 1.2 : Literature on Digital Authentication

Protocol	Characteristics	Mechanism	Advantages	Limitation
Challenge-Handshake Authentication Protocol (CHAP)	Authenticates a user or network host to an authenticating entity.	Shared secret key, One-way hash function, three-way handshake	Protection against: Replay attack	The distribution of the secret key.
CRAM-MD5	SMTP mail agent authentication	A hash function, concatenation, Fresh random challenge	Resist to a Replay attack	Lack of Mutual Authentication, Storage of password, Vulnerable to dictionary attack
Kerberos	Network authentication protocol over an insecure channel	Issue tickets, Trusted the third party,	Mutual Authentication, Resist to Replay attack and eavesdropping	Single point of failure, Vulnerable to man-in-middle attack. Time constraints.
Otway–Rees protocol	Network authentication protocol over an insecure channel	Usage of the Nonce, session identifier, Server.	Resist to Replay attack and eavesdropping	Vulnerable to Intercept and resend attack
Needham–Schroeder protocol	Network authentication protocol over an insecure channel	The shared secret key, server	Establish session key and mutual authentication	Key distribution
Wide Mouth Frog protocol	Network authentication protocol over an insecure channel	Global clock, Server, shared a secret key, BAN logic	Resist replaying attack and eavesdropping. Detection of modification	Key distribution and required trusted server
CAPTCHA, reCAPTCHA	Network user identification non-cryptographic scheme	Images	Widely used in webmail	Availability.
Distance-bounding protocol	Cryptographic protocols that enable a verifier to establish an upper bound on the physical distance to a prover	Delay time, Radio frequency implementation	Widely use in identifying protocol	Availability
Physical Unclonable Function or PUF	PUF is a function that is embodied in a physical structure and is easy to evaluate but hard to predict.	Hardware implementation of the hash function,	Resist to spoofing attacks	Practical implementation and generality

Table 1.3 : Literature on Public Key Cryptography

Strengths	Weaknesses
The asymmetric in public-key cryptography allows it a sizable advantage over symmetric-key algorithms.	Asymmetric keys is longer than keys in secret-cryptography to have equivalent security. Keys in asymmetric cryptography are also vulnerable to brute force attacks than in secret-key cryptography.
The unique private and public keys provided to each user allowing them to conduct secure exchanges of information without first needing to devise some way to swap keys secretly.	Public-key cryptography also has vulnerabilities to attacks such as the man-in-the-middleattack. In this situation, a malicious third party intercepts a public key on its way to one of the parties involved. The third party can then instead pass along his or her public key with a message claiming to be from the original sender. An attacker can use this process at every step of exchange to successfully impersonate each member of the conversation without any other parties knowing this deception.

Key distribution is only a method on how to secure the key while it been exchanged. The key involved in this method are public key, private key and secret key. On the other hand, the process needs the digital signatures as a verifier to authenticate the message. The sender would send the private key while the message had been encrypted. Only recipient who have the authorized private key could decrypt the message. This is to ensure the integrity of the message and to identify the dedicated users.

1.5 Quantum Communication Protocol

Theoretically the quantum keys is impossible to prone even quantum computing. Throughout the previous research they believe this technology could overcome the issue in the classical form of encryption. However, in security there a no such things that it cannot be tampered. Apparently the quantum communication is still vulnerable to cyber-attacks and human failure. Thus, quantum encryption promises to provide the unbreakable mechanism to quantum secured communication system.

Initially the idea of Quantum key distribution (QKD) is to provide a platform to transfer a secret key is a secure manner. By applying the quantum mechanics, the form of key itself has been secure. The well-known QKD protocol is BB84 published by Bennett and Brassard in 1984. In terms of security aspect it still unambiguous. Most of it is the theoretical finding compare to experiment findings. To conduct an experiment it may cost a lot of money. Despite all this, there many researchers has coming out with their security proof of using the QKD. As for now, the most stable protocol for QKD is BB84.

1.6 Motivations

Securing the authentication process may attract our attention to introduce a new scheme for cloud infrastructure network. Referring to Gartner's prediction by the year 2016 (http://www.gartner.com/it/page.jsp?id=2060215) most of the organization may move their data to the cloud. The cloud services may be in demand and have many competitors. The only aspect that can gain trust from the user to use their services provides them with the highest security level in their services. The information that may place in the cloud server might be a very high profile document and confidential. They must ensure that the information could be access by only dedicated users. Recently the digital cryptography has been emerged and cultivated. Nevertheless, not all digital cryptography may suit will all the needs especially in digital transaction. It is prominent in all digital worlds especially when it relates with authentication and authorization. It is needs to include the elements of security, easy to handle, easy to maintain, and stable.

The main motivation of this thesis is to construct an authentication scheme with quantum key distribution protocol dedicated for multi-party system in cloud infrastructure. Since, the quantum authentication protocols are in its early development stage, designing a simple and effective scheme would be the first step towards the big goal. This scheme concept does not only to combine the quantum authentication and quantum communication but also to provide a systematic flow of information.

The highlight of this research is to combine quantum authentication scheme and cloud infrastructure that include multi-party quantum key distribution protocols. Hence, in every set of the transaction, quantum user authentication can be achieved.

1.7 Problem Statements

The authentication scheme for multi-party system in cloud infrastructure is still a major concern among the users and researchers. When the high confidential information has to be transfered among the cloud user the channel should be able to prevent from any interception from intruders that may lead to information leakage. In this situation the communication channel and the protocol must ensure the communication is only happened between the legitimate users in cloud infrastructure (Chang, Zhang, Yan, & Sheng, 2013). Other digital cryptography method or Public Key Infrastructure has been introduced but the percentage of information leakage is high. We found that the issue is pertaining to the security of the secret key that is going to be shared among in cloud infrastructure and the communication channel. Each of the cloud clients will be identified by their secret key.

Recently, the research on quantum communication channel is on demand. Researchers found that the quantum channel could replace the classical channel to distribute a secret key (Technology, 2012). The secret key transmission is through QKD. The basic property of QKD is able to detect eavesdropping. Through QKD the secret key is transformed into quantum bits. It is difference with the classical approach where the secret key is transformed into bits. In quantum bits, the information of the secret key is represented in photon. The information present in photon cannot be copied.

Despite the literature on the quantum key distribution that we are going to apply in the cloud infrastructure, there are gaps that we found out. The existing scheme for secret key which are tight finite key proposed by (Tomamichel, Lim, Gisin, & Renner, 2012) is exposed to the finite key distillation that may lead to key loss. The secret key rate is mainly affected by the detection. Hence, in Quantum Key Distribution the main issue is the number of signals exchanged between two parties. Number of signal may the reflect the security of the final key that will be distributed among the legitimate parties. (Matsumoto, 2007) has introduced the Multi-Party QKD to enable the secret key to be shared between two parties. However, the deficiency of efficient quantum user authentication from the previous research in terms of security compromise due to dishonest member becomes our main concern.

1.8 Research Objectives

The main objective of this entire research is to propose a secure authentication method for multi-party system in cloud infrastructure by using a Quantum Key Distribution (QKD) with enhanced tight finite key scheme. As such, there are three other specific objectives to achieve in this research.

The specific objectives are:

1. To enable the involved party to securely distribute a secret keys that can be used for securing further communication

2. To develop an enhanced tight finite key scheme for QKD protocol to authenticate multi-party system in cloud infrastructure

3. To develop a higher key rate for cloud multiparty quantum authentication protocol based on a modified, enhanced tight finite-key analysis and shared a secret key. The cluster of cloud client is called as cloudlets. Thus, in the proposed scheme there will be a cloudlet secret shared key. The higher key rate is measured by the conversion of the shared secret key among parties.

1.9 Research Scope

The scope of this research is to develop a secure authentication scheme with QKD for multi-party system in cloud infrastructure in which the following will be taken into consideration throughout the research. Cloud infrastructure is indicated for two types of cloud platform which are public and private. The comprehensive assumption is explained in each chapter:

a) Users in multi-party system established enhanced tight finite key between them using QKD mechanism.

b) Classical channel is authenticated. The message is sent in the form of encryption. Intruder may able to intercept the message.

c) The intruder can take over a quantum channel.

d) It is the noiseless quantum channel which means it is free from any kind of interference.

e) The calculation is only on single photon. The assumption is, each message and key are sent in the form or single photon.

f) Prerequisite for multi-party user in cloud infrastructure is three legitimate parties who are Alice, Bob and Charlie.

g) The transmission of shared secret keys between sender and receiver are on a secured channel.

The proposed authentication scheme will be implemented in cloud infrastructure. It may involve the quantum cryptography together with digital cryptography. The use of quantum cryptography is to provide a quantum channel and the use of single photon to transfer the message and exchange the key. On the other hand, we are still using the digital cryptography to authenticate the message. We are going through the Quantum Key Distribution process where we need to exchange the key. Exchanging the key will be happened in the quantum channel and transferring the message in via a public channel. In this thesis our focus is to provide a scheme for key distribution. Eventually, we will use the BB84 protocol to measure it effectiveness.

The experimental setup will be based on BB84 protocol. In the simulation model, there are all the phases involved including polarized based discrete variable QKD.

We mimic all the basic components that are required in quantum communication in the simulation.

1.10 Thesis Organization

This thesis is divided into seven chapters. The first chapter defines cloud infrastructure authentication and its various approaches, and the problem of current authentication analysis methodologies is presented. Chapter 2 discusses the current techniques used for cloud authentication, the problems associated with ad-hoc analysis, and several attempts at formal analysis methodologies. The third chapter presents the formalized methodology and techniques for a complete cloud authentication method with a quantum key distribution protocol; this chapter provides the bulk of the theoretical contributions of this thesis. The focuses are on the logical structure of the techniques and how they are applied. The fourth chapter is a collection of proposed method that is performed with this thesis' formalized analysis methodology; this chapter demonstrates the result analysis that is the contribution of the thesis. Chapter 5 describes the simulation process to prove the proposed method. Chapter 6 will describe the finding of implementing the quantum theory and digital authentication approach in cloud infrastructure. In the final chapter, Chapter 7 may conclude the whole thesis chapter and highlight the contribution of the thesis.

REFERENCES

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2016). Continuous and transparent multimodal authentication: reviewing the state of the art. *Cluster Computing*, *19*(1), 455–474. https://doi.org/10.1007/s10586-015-0510-4

Almulla, S. A., & Yeun, C. Y. (2010). Cloud computing security management. In *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on* (pp. 1–7). inproceedings.

Arifeen, F. U., Siddiqui, R. A., Ashraf, S., & Waheed, S. (2015). Inter-Cloud Authentication through X.509 for defense organization. In *Proceedings of 2015 12th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2015* (pp. 299–306). https://doi.org/10.1109/IBCAST.2015.7058520

Bacco, D., Canale, M., & Laurenti, N. (2013). Experimental quantum key distribution with finite-key security analysis for noisy channels. *Nature Communications*, *14*, 1–20. Retrieved from http://www.nature.com/ncomms/2013/130906/ncomms3363/full/ncomms3363.html?message-global=remove&WT.ec_id=NCOMMS-20130911

Badger, L., Patt-corner, R., & Voas, J. (2012). Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology. *National Institute of Standards And Technology*.

Bagan, E., Baig, M., & Muñoz-Tapia, R. (2004). Entanglement-assisted alignment of reference frames using a dense covariant coding. *Physical Review A*, *69*(5), 50303. article.

Barnett, S. M., & Phoenix, S. J. D. (2011). Securing a quantum key distribution relay network using secret sharing. *2011 IEEE GCC Conference and Exhibition (GCC)*, 143–145. https://doi.org/10.1109/IEEEGCC.2011.5752491

Bennett, C., Bessette, F., & Brassard, G. (1992). Experimental quantum cryptography. *Journal of ...*, (September). Retrieved from http://link.springer.com/article/10.1007/BF00191318

Bennett, C., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International ...*, *175*(150), 8. Retrieved from http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf

Bhargavan, K., & Corin, R. (2009). Cryptographic protocol synthesis and verification for multiparty sessions. In *22st IEEE Computer Security Foundations Symposium (CSF 2009)*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5230622

Bugiel, S., & Nürnberger, S. (2011). Twin clouds: An architecture for secure cloud computing. *... and Security in Clouds ...*, 1–11. Retrieved from http://www.zurich.ibm.com/~cca/csc2011/submissions/bugiel.pdf

Buhari, A., Zukarnain, Z. A., Subramaniam, S. K., Zainuddin, H., & Saharudin, S. (2012). A Quantum Based Challenge Response User Authentication Scheme Over Noiseless. *International Journal of Network Security & Its Applications (IJNSA)*, *4*(6), 67–79.

Cabello, A. (2000). Quantum key distribution in the Holevo limit. *Physical Review Letters*, *85*(26), 5635.

Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010). Security and cloud computing: intercloud identity management infrastructure. In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on* (pp. 263–265). inproceedings.

Chang, Y., Zhang, S.-B., Yan, L.-L., & Sheng, Z.-W. (2013). A Multiparty Controlled Bidirectional Quantum Secure Direct Communication and Authentication Protocol Based on EPR Pairs. *Chinese Physics Letters*, *30*(6), 060301. https://doi.org/10.1088/0256-307X/30/6/060301

Chen, R.-K., Zhang, Y.-Y., Shi, J.-H., & Li, F.-G. (2013). A multiparty error-correcting method for quantum secret sharing. *Quantum Information Processing*, *13*(1), 21–31. https://doi.org/10.1007/s11128-013-0716-4

Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011). A Strong User Authentication Framework for Cloud Computing. *2011 IEEE Asia-Pacific Services Computing Conference*, 110–115. https://doi.org/10.1109/APSCC.2011.14

Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E., & Song, Z. (2010). Authentication in the Clouds : A Framework and its Application to Mobile Users. *ACM Workshop on Cloud Computing Security*, 1–6. https://doi.org/10.1145/1866835.1866837

Chuang, M.-C., & Chen, M. C. (2014). An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Systems with Applications*, *41*(4), 1411–1418. https://doi.org/10.1016/j.eswa.2013.08.040

Computing, D. (2009). Cloud Computing: An Overview. *Distributed Computing*, *7*(5), 1–5. https://doi.org/10.1145/1538947.1554608

Dinesha, H., & Agrawal, V. (2012). Multi-level authentication technique for accessing cloud services. In *Computing, Communication and Applications (ICCCA), 2012 International Conference on* (pp. 1--4). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6179130

Fano, G., & Blinder, S. M. (2017). Mathematical Methods in Quantum Mechanics.

In *Twenty-First Century Quantum Mechanics: Hilbert Space to Quantum Computers* (pp. 43–84). Springer.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(January), 145–195. Retrieved from http://journals.aps.org/rmp/abstract/10.1103/RevModPhys.74.145

Gittsovich, O., Beaudry, N. J., Narasimhachar, V., Alvarez, R. R., & Moroder, T. (2013). Squashing model for detectors and applications to quantum key distribution protocols. *Physical Review A*, *89*(1), 1–29.

Gottesman, D., & Chuang, I. (2001). Quantum digital signatures. *ArXiv Preprint Quant-Ph/0105032*. article.

Guo, G.-P., & Guo, G.-C. (2003). Quantum secret sharing without entanglement. *Physics Letters A*, *310*(4), 247–251.

Gyongyosi, L., & Imre, S. (2012). Information geometric security analysis of differential phaseâ€• shift quantum key distribution protocol. *Security and Communication Networks*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/sec.542/full

Hillery, M., Bužek, V., & Berthiaume, A. (1999). Quantum secret sharing. *Physical Review A*, *59*(3), 1829–1834. https://doi.org/10.1103/PhysRevA.59.1829

Kak, S. (2006). A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, *19*(3), 293–296.

Khalid, Roszelinda and Zukarnain, Zuriati Ahmad and Hanapi, Zurina Mohd and Mohamed, M. A. (2015). Authentication Mechanism For Cloud Network And Its Fitness With Quantum Key Distribution Protocol : A Survey. *Journal of Theoretical and Applied Information Technology*, *81*(1), 51–64.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2013). Two-factor authentication system based on extended OTP mechanism. *International Journal of Computer Mathematics*, *90*(12), 2515–2529. https://doi.org/10.1080/00207160.2012.748901

Küchlin, W. (1987). Public key encryption. *ACM SIGSAM Bulletin*, *21*(3), 69–73. article.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11). Retrieved from http://dl.acm.org/citation.cfm?id=358797

Lee, S., Ong, I., Lim, H.-T., & Lee, H.-J. (2010). Two factor authentication for cloud computing. *Journal of Information and Communication Convergence Engineering*, *8*(4), 427–432. article.

Lian-Fang, H., & Yi-Min, L. (2007). Efficient multiparty-to-multiparty quantum

secret sharing via continuous variable operations. *Chinese Physics …*, *3312*. Retrieved from http://iopscience.iop.org/0256-307X/24/12/006

Lin, H. (2014). Toward Secure Strong Designated Verifier Signature Scheme from Identity-Based System. *The International Arab Journal Of Information Technology*, *11*(4), 315–321.

Liu, F., Qin, S.-J., & Wen, Q.-Y. (2014). A quantum secret-sharing protocol with fairness. *Physica Scripta*, *89*(7), 075104. https://doi.org/10.1088/0031-8949/89/7/075104

Liu, W., Chen, H., Li, Z., & Zhao, J. (2008). Efficient Many-to-One and One-to-Many Multiparty Quantum Secure Direct Dommunication with Authentication. *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, *2*(1), 1282–1285. https://doi.org/10.1109/IIH-MSP.2008.175

M.Bellare, P. R. (1995). Provably Secure Session Key Distribution — The Three Party Case. In *Proc.27th ACM Symp. Theory of Computing* (pp. 57–66).

Matsumoto, R. (2007). Quantum multiparty key distribution protocol without use of entanglement. *ArXiv Preprint ArXiv:0708.0902*, 1–8. Retrieved from http://arxiv.org/abs/0708.0902

Mink, A., Frankel, S., & Perlner, R. (2010). Quantum key distribution (QKD) and commodity security protocols: Introduction and integration. *ArXiv Preprint ArXiv:1004.0605*, *1*(2), 101–112. Retrieved from http://arxiv.org/abs/1004.0605

Mosca, M., Stebila, D., & Ustaoglu, B. (2013). Quantum Key Distribution in the Classical Authenticated Key Exchange Framework. In *Post-Quantum Cryptography* (pp. 136--154).

Nagamatsu, Y., Mizutani, A., Ikuta, R., Yamamoto, T., Imoto, N., & Tamaki, K. (2016). Security of quantum key distribution with non-I.I.D. light sources, 1–10. https://doi.org/10.1103/PhysRevA.93.042325

Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. *Privacy and Security for Cloud Computing*, 3–42. https://doi.org/10.1007/978-1-4471-4189-1

Rass, S. (2007). A method of Authentication for Quantum Networks. *International Journal of Information Technology*, *12*(March), 149–154. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=1305239X&AN=31704220&h=+7T8FWk9xtksC0NmKyXMINrSFFownm8KkODLmAZ7e0+WrX/3bpz9XCW6aFPLcDs0vW1NF1cK1CocWPeWRZcnEg==&crl=c

Scarani, V., & Bechmann-Pasquinucci, H. (2009). The security of practical quantum key distribution. *Reviews of Modern …*, 1–52. Retrieved from

http://rmp.aps.org/abstract/RMP/v81/i3/p1301_1

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, *27*(3), 379–423.

Shannon, C. E. (1948). Communication theory of secrecy systems. 1945. *M.D. Computing : Computers in Medical Practice*, *15*(1), 57–64. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/23484506

Shen, Z., Li, L., Yan, F., & Wu, X. (2010). Cloud Computing System Based on Trusted Computing Platform. *2010 International Conference on Intelligent Computation Technology and Automation*, 942–945. https://doi.org/10.1109/ICICTA.2010.724

Shoup, V., & Rubin, A. (1996). Session Key Distribution Using Smart Cards 1 Introduction. *Springer-Verlag*, 1–11.

Singh, H., Gupta, D. L., & Singh, a. . (2014). Quantum Key Distribution Protocols: A Review. *IOSR Journal of Computer Engineering*, *16*(2), 01–09. https://doi.org/10.9790/0661-162110109

Singh, Y., & Jena, S. K. (2011). Intrusion detection system for detecting malicious nodes in mobile ad hoc networks. In *Advances in Parallel Distributed Computing* (pp. 410–419). Springer.

Tancevski, L., Slutsky, B. A., Rao, R. R., & Fainman, Y. (1998). Evaluation of the cost of error-correction protocol in quantum cryptographic transmission. In *Voice, Video, and Data Communications* (pp. 322–331).

Technology, S. (2012). Quantum Key Distribution, *10*(6).

Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. *Nature Communications*, *3*(may 2011), 634. https://doi.org/10.1038/ncomms1631

Tsai, I-Ming and Yu, Chia-Mu and Tu, Wei-Ting and Kuo, S.-Y. (2005). A Secure Quantum Communication Protocol Using Insecure Public Channels. In *Security and Privacy in the Age of Ubiquitous Computing* (pp. 11–13). Springer.

Walenta, N., Burg, a, Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O., … Zbinden, H. (2014). A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics*, *16*(1), 013047. https://doi.org/10.1088/1367-2630/16/1/013047

Wegman, M. N., & Carter, J. L. (1981). New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, *22*(3), 265–279. https://doi.org/10.1016/0022-0000(81)90033-7

Wiles, J. (2005). QUANTUM BIT ERROR RATES IN QUANTUM KEY

DISTRIBUTION USING ENTANGLED PHOTONS. *US Patent 5,016,859*.

Xiao, Li and Long, Gui Lu and Deng, Fu-Guo and Pan, J.-W. (2003). Quantum secret sharing without entanglement. *Physical Review A*, *69*(5), 052307. Retrieved from http://www.sciencedirect.com/science/article/pii/S0375960103000744

Yan, F.-L., & Gao, T. (2005). Quantum secret sharing between multiparty and multiparty without entanglement. *Physical Review A*, *72*(1), 12304. article.

Yang, Y., & QiaoYan, W. (2008). Threshold quantum secure direct communication without entanglement. *Science in China Series G: Physics, Mechanics and Astronomy*, *51*(2), 176–183. article.

Zainuddin, H., & Saharudin, S. (2012). A S IMPLE P OST Q UANTUM S CHEME FOR H IGHER K EY R ATE M ULTIPARTY Q UANTUM K EY. *International Journal Of Network Security & Its Applications*, *4*(5), 1–14.

Zeng, G., & Keitel, C. H. (2002). Arbitrated quantum-signature scheme. *Physical Review A*, *65*(4), 42312. article.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

Ziyad, S., & Rehman, S. (2014). Critical Review of Authentication Mechanisms in Cloud Computing. *International Journal of Computer Science Issues (...*, *11*(3), 145–149. Retrieved from http://www.ijcsi.org/papers/IJCSI-11-3-1-145-149.pdf

BIODATA OF STUDENT

Roszelinda Binti Khalid is currently pursuing her PhD at the Faculty of Computer Science and Information Technology, UPM. She received a scholarship from Jabatan Perkhidmatan Awam Malaysia. She received a Bachelor Degree in Computer Science (2000) and Master in Software Engineering (2006) from the Universiti Putra Malaysia (UPM). Her professional working experience includes 1 years of service as software engineer 2 years of service as a security consultant, and 7 years as Information Technology Officer at Malaysia Government Sector that focusing in government ICT security. Being her research area is quantum authentication and quantum key distribution, she also has research interest quantum computing and cloud computing.

LIST OF PUBLICATIONS

Journal

Khalid, R., & Zulkarnain, Z. A. (2014). Enhanced Tight Finite Key Scheme for Quantum Key Distribution (QKD) Protocol to Authenticate Multi-Party System in Cloud Infrastructure. In *Applied Mechanics and Materials* (Vol. 481, pp. 220-224). Trans Tech Publications.

Khalid, R., Zukarnain, Z. A., Hanapi, Z. M., & Mohamed, M. A. (2015). Authentication Mechanism For Cloud Network And Its Fitness With Quantum Key Distribution Protocol: A Survey. *Journal of Theoretical and Applied Information Technology*, *81*(1), 51.

Book Chapter

Khalid, R., Zukarnain, Z. A., Hanapi, Z. M., & Mohamed, M. A. (2015). Multi-Party System Authentication for Cloud Infrastructure by Implementing QKD. In Computational Intelligence and Efficiency in Engineering Systems (pp. 195-207). Springer, Cham.

Conferences

Zukarnain, Z. A., & Khalid, R. (2014). Quantum key distribution approach for cloud authentication: Enhance tight finite key. In International Conference on Computer Science and Information Systems (ICSIS'2014) (pp. 28-33).

Khalid, R., Zukarnain, Z. A., Hanapi, Z. M., & Mohamed, M. A. (2015). Multi-Party System Authentication for Cloud Infrastructure by Implementing QKD. In Computational Intelligence and Efficiency in Engineering Systems (pp. 195-207). Springer International Publishing.

Khalid, R., & Zulkarnain, Z. A. Tight Finite Key Scheme For Quantum Key Distribution (Qkd) Protocol To Authenticate Multi-Party System In Cloud Infrastructure.

Khalid, R., & Zukarnain, Z. A. (2014, November). Effectiveness of enhanced tight finite scheme in quantum key distribution protocol for network communication. In Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian (pp. 141-145). IEEE.

Khalid, R., & Zukarnain, Z. A. (2015, December). Cloud Computing Security Threat with Quantum Key Distribution Defense Model. In The Third International Conference on Green Computing, Technology and Innovation (ICGCTI2015) (p. 49).

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : _____

TITLE OF THESIS / PROJECT REPORT :

ENHANCED TIGHT FINITE KEY SCHEME FOR QUANTUM KEY DISTRIBUTION PROTOCOL TO AUTHENTICATE MULTI-PARTY SYSTEMS IN CLOUD INFRASTRUCTURE

NAME OF STUDENT: ROSZELINDA BINTI KHALID

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☐	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐ **PATENT** Embargo from _____ (date) until _____ (date)

Approved by:

_____	_____
(Signature of Student)	(Signature of Chairman of Supervisory Committee)
New IC No/ Passport No.:	Name:
Date :	Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]