

**UNIVERSITI TEKNOLOGI MARA**

**A NEW PROTOCOL OF DUAL  
DENIABILITY ENCRYPTION  
TECHNIQUES BASED ON  
ASYMMETRIC SECRET SHARING  
METHOD**

**MOHSEN BIN MOHAMAD HATA**

Thesis submitted in fulfillment  
of the requirements for the degree of  
**Doctor of Philosophy**  
**(Information Technology and Quantitative  
Sciences)**

**Faculty of Computer and Mathematical Sciences**


**May 2019**

## AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Mohsen Bin Mohamad Hata  
Student I.D. No. : 2010526887  
Programme : Doctor of Philosophy – CS990  
Faculty : Computer and Mathematical Sciences  
Thesis Title : A New Protocol of Dual Deniability Encryption  
Techniques Based on Asymmetric Secret Sharing  
Method

Signature of Student :   
Date : May 2019

## ABSTRACT

Computer networks are ever-changing technologies that embodied secure communication protocol offerings security towards the digital communications. Secure Communication most often uses cryptographic primitives as the methods or techniques to protect the confidentiality of data being communicated. The main components of cryptography are the algorithm and the key management. However, an adversary could use coercion method where both components can no longer be reliable. In a Public Key Infrastructure network, Deniable Encryption techniques have been introduced to achieve incoercible communication. This technique uses Fake Keys and/or Fake Messages to be presented for the Coercer in order to hide the Real Keys and/or Real Messages. For this technique to succeed, the Fake Keys must be indistinguishable from the Real Keys. Past works have proposed numerous techniques of Deniable Encryption in achieving incoercible communication. However they were often easily been compromise if the coercer already suspect Deniable Encryption is applied. For achieving plausible deniability this research proposed a new protocol that embeds two layers of techniques. This new approach of constructing two layers of deniability techniques is done in a manner of defining a protocol to embed and implementing them. The protocol defines the procedures which engage two layers of deniability techniques; namely Secret Sharing and Valid Fake Messages. Secret Sharing technique is used to generate Fake Asymmetric Keys by using LaGrange Polynomial Interpolation formula and RSA algorithm. Secured communication is achieved where the notion of plausible deniability is successfully implemented by fusing the processes of theorem's verification and data's validation in the protocol construction methodology.

## TABLE OF CONTENTS

	<b>Page</b>
<b>CONFIRMATION BY PANEL OF EXAMINERS</b>	<b>ii</b>
<b>AUTHOR'S DECLARATION</b>	<b>iii</b>
<b>ABSTRACT</b>	<b>iv</b>
<b>ACKNOWLEDGEMENT</b>	<b>iv</b>
<b>TABLE OF CONTENTS</b>	<b>vi</b>
<b>LIST OF TABLES</b>	<b>x</b>
<b>LIST OF FIGURES</b>	<b>xi</b>
<b>CHAPTER ONE: INTRODUCTION</b>	<b>1</b>
1.1 Introduction	1
1.2 Motivation	2
1.3 Problem Statement	2
1.4 Research Objectives	4
1.4.1 To Design and Develop a Dual Deniability Encryption Protocol	4
1.4.2 To Evaluate the Effectiveness of the Dual Deniability	5
1.5 Scopes and Limitations	5
1.6 Research Contributions	8
1.7 Significance of Study	8
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>10</b>
2.1 Introduction	10
2.2 Deniable Encryption Framework	11
2.2.1 Encryption Key	11
2.2.2 Coercion in Communication	12
2.2.3 DeniableEncryption Properties	13
2.3 Deniability Characteristics	14
2.3.1 Plausible (A.Y.Davydov, 2015)	14

2.3.2	Hidden (Skillen and Mannan, 2014)	15
2.3.3	A Non-Committing Encryption (Durmuth and Freeman,2011)	16
2.4	Public Key Infrastructure	16
2.5	Certificate Authority Processes	19
2.5.1	User's registration	19
2.5.2	Key Generation	19
2.5.3	Key Distribution	19
2.5.4	Encryption Algorithms Assignment	20
2.5.5	Issuing Digital Certificate	20
2.5.6	Key Revocation	20
2.5.7	Key Refresh	20
2.6	Multi-Party Computation	21
2.7	Secret Sharing Scheme	22
2.8	Related Researches	22
2.9	Techniques Comparison of Related Researches	31
<b>CHAPTER THREE: RESEARCH METHODOLOGY</b>		<b>35</b>
3.1	Introduction	35
3.2	Research Design Framework	35
3.3	Development Methodology	40
<b>CHAPTER FOUR: SYSTEM DESIGN</b>		<b>58</b>
4.1	Introduction	58
4.2	A Protocol of Dual Deniability Encryption Design Idea	58
4.3	Protocol Process Flow	62
4.4	Protocol Design	66
4.4.1	Development Layers	67
4.5	A lgorithm Design	75
4.5.1	Generating Fake Keys	75
4.5.2	Retrieving Secret/Real Key	78