

CONTENTS

Agreement Page	
Originality Statements	
ABSTRACT	iv
PREFACE	v
UCAPAN TERIMA KASIH	vi
Contents	viii
List of Figures	x
List of Tables	xii
1 INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	3
1.3 Objective	3
1.4 Hypothesis	4
1.5 Research Method	4
2 LITERATURE REVIEW	6
2.1 Cryptography For Quantum Era	6
2.1.1 CRYSTALS-Kyber	9
2.1.2 CRYSTALS-Dilithium	11
2.1.3 Signcryption	11
2.2 Smart home	14
2.3 State of The Art	15
3 RESEARCH DESIGN AND METHODOLOGY	18
3.1 Research Methodology	18
3.2 System Design	19
3.2.1 Research Topology	19
3.2.2 Research Workflow	21

3.3	System Implementation	21
3.3.1	Experimental Setup	21
3.3.2	Smart Home Implementation	22
3.3.3	Kyber Implementation	22
3.3.4	Signcryption Implementation	27
3.4	Research Scenario	29
4	PERFORMANCE EVALUATION	30
4.1	Simulation Parameter	30
4.2	Signcryption Evaluation on IoT Node Gateway	31
4.2.1	Key Generation	31
4.2.2	Signcrypt	38
4.2.3	Unsigncrypt	46
4.3	Kyber-Dilithium Signcryption Simulation on Smart Home Environ- ment	55
4.4	Analysis and Discussion	59
5	Conclusion	61
5.1	Conclusion	61
5.2	Suggestion	62
	Bibliography	63