CONTENTS

ABSTRACT i

ABSTRAK ii

DEDICATION iii

ACKNOWLEDGEMENTS iv

CONTENTS v

LIST OF TABLES viii

LIST OF FIGURES ix

LIST OF ABBREVIATIONS x

LIST OF ALGORITHMS xi

CHAPTER 1: INTRODUCTION 1

1.1 Rationale 1

1.2 Theoretical Framework 2

1.3 Conceptual Framework 3

1.4 Statement of the Problem 3

1.5 Hypothesis 4

1.6 Assumption 4

1.7 Scope and Delimitation 4

1.8 Importance of the Study 5

CHAPTER 2: REVIEW OF LITERATURE AND STUDIES 6

2.1 Hash to Obtain Random Subset (HORS) with Tree 6

2.1.1 Key Generation In HORST 7

2.1.2 Signature Generation In HORST 8

2.1.3 Verification In HORST 10

2.1.4 Advantages and Disadvantages of HORST 11

2.2 Hash to Obtain Random Subset Integer Composision (HORSIC) 12

2.2.1 Key Generation in HORSIC 13

2.2.2 Signature generation in HORSIC 14

2.2.3 Verification in HORSIC 17

2.2.4 Advantages and Disadvantages of HORSIC 19

CHAPTER 3: RESEARCH METHODOLOGY 21

3.1 Seed Generation 22

3.1.1 Random Number Generator 22

3.2 Private Key Generation 25

3.2.1 Hash Message 25

3.2.2 Indexing Process 26

3.2.3 Generating Private Key 27

3.3 Signing Process in MHORST 29

3.4 Public Key Generation 37

3.5 Published Public Key Generation 38

3.6 Verification Process 40

3.6.1 Generating Seed 40

3.6.2 Obtaining Public Key from Published Public Key 40

3.6.3 Signature Verification 42

3.7 System Spesification 45

3.8 Experiment Design 45

CHAPTER 4: EXPERIMENT AND RESULT 46

4.1 Experiment Data 46

4.1.1 Key Generation 48

4.1.2 Signing 52

4.1.3 Verification 56

4.2 Analyse the Experiment Result 60

4.2.1 Time Consumption 61

4.2.1.1 Key Generation.. 61

4.2.1.2 Signing.. 64

4.2.1.3 Verification 66

4.2.2 Analyse Security Level... 69

4.2.2.1 Security Analysis of Private Key Penetration with Brute Force ... 69

4.2.2.2 Security Analysis Against Signature Forgery 71

CHAPTER 5: CONCLUSION AND RECOMMENDATION............................. 77

5.1 Conclusion 77

5.2 Recommendation 78

REFERENCES 79

APPENDIX 82