Contents

English Abstract ………………………………………………………… **i**

Chinese Abstract ……………………………………………...………… **ii**

Acknowledgements …………………………………………………… **iii**

Contents ……………………………………..……………………… **iv**

List of Figures ……………………………………………………… **vi**

List of Tables ……………………………………………………….. **vii**

Chapter 1 Introduction ………………………………………..…. **1**

Chapter 2 Background ……………………………………………….. **2**

2.1 Cryptography ………………………………………………...…...…… 2

2.2 Cryptographic Primitives ……………………………………..…….. 3

2.3 Ciphers ……………………………………………………………….... 3

2.3.1 Symmetric-Key and Public-Key Ciphers ……..……… 4

2.3.2 Block and Stream Ciphers …………………………… 4

2.4 Block Cipher Architectures ……..…………………………….... 5

2.4.1 Substitution-Permutation Networks ……..………….… 5

2.4.2 Feistel Networks ……………………………………… 6

2.4.3 Other Block Cipher Architectures ……...……………. 7

2.5 Block Cipher Standards …………………………………...... 8

2.5.1 Data Encryption Standard (DES) …………...……….... 9

2.5.2 Advanced Encryption Standard (AES) ……...……….. 9

2.6 Attacks on Block Ciphers ……………………………….…... 10

2.6.1 Exhaustive Key Search ……………………..…… 10

2.6.2 Linear Cryptanalysis ……………………………..… 11

2.6.3 Differential Cryptanalysis …………………………..… 11

Chapter 3 Linear Cryptanalysis on SPN …………………………. 12

3.1 Principle of Linear Attack …………………………………… 14

3.2 Linear Approximations of S-boxes …………………………... 15

3.3 Linear Characteristics ………………………………………... 17

3.4 Subkeys Attack ………………………………………………. 21

3.5 Techniques of Linear Cryptanalysis ………………………….. 22

3.5.1 Key Ranking ……………………………………………. 22

3.5.2 Multiple Linear Approximations ……………………… 22

Chapter 4 Attack Strategies on SPN …………………………….. 24

4.1 Trails-Finding ………………………………………………... 24

4.2 Minimum Number of test pairs ……………………………… 26

4.3 Attack Strategies ……………………………………………... 29

4.3.1 Basic Strategy ………………………………………….. 29

4.3.2 Using Multiple Linear Approximations …………….. 32

4.4 Backtracking …………………………………………………. 32

Chapter 5 Computer Experiments ……………………………….. 34

Chapter 6 Conclusion …………………………………………… 36

Bibliography …………………………………………………... 37

List of Figures

2.1 A taxonomy of cryptographic primitives (from [1, 2]) …………….. 3

2.2 Operation of a cipher ………………………………………………. 4

2.3 An SPN structure with N = 16, M = n = 4, R = 3 ………………….. 6

2.4 Basic Feistel network architecture …………………………………. 7

2.5 Encryption process of IDEA ……………………………………….. 8

2.6 One round of Rijndael (the AES) …………………………………... 9

3.1 Notations …………………………………………………………….. 13

3.2 Summary of linear cryptanalysis (Algorithm 2) ………………….. 16

3.3 A trail of a SPN with M = n = 4 (N = 16), R = 2, and the permutation of Kam and Davida [3] ……………………………….... 19

3.4 A trail for attack …………………………………………………….... 21

4.1 Flow chart of the attack ……………………………………………... 25

4.2 Two cases of distribution of $\mathrm{II}_{K'}$ with $\varepsilon > 0$……………………….. 27

4.3 Attack strategy: from K^1 to K^{R+1} (from [4]) ………………………. 30

4.4 Attack strategy: from K^{R+1} to K^1 (from [5]) ………………………. 31

4.5 Backtracking Scheme ……………………………………………….. 33

5.1 The SPN we will attack ……………………………………………... 34

List of Tables

2.1 The relation between key lengths and the numbers of rounds in AES …………………………………………………………………….. 10

3.1 Linear Approximation Table for Example 1 ………..……………. 18

4.1 The success rate of Matsui's Algorithm 2 ([6]) …………………... 29

5.1 S-box and permutation mappings ……………………………….... 35

5.2 Data complexity and time complexity ……………………………. 35

5.3 Success rate …………………………………………………….. 35