Contents

1 Introduction 1

2 Introduction to Block Ciphers 3

2.1 Secret-Key Block Ciphers 3

2.2 Security of Block Ciphers 5

2.2.1 Types of attacks 5

2.2.2 Unconditional and computational security 6

2.2.3 Data- and processing-complexity of a specified attack 10

2.2.4 Block cipher parameters 11

2.3 Design Principles for Block Ciphers 12

2.3.1 General design principles for security 12

2.3.2 Design principles for implementation 13

2.4 Iterated Ciphers 13

2.4.1 Iterated cipher and round function 13

2.4.2 Constructions of E/D similar iterated ciphers 14

3 The Block Cipher IDEA 21

3.1 Description of IDEA 21

3.1.1 The encryption process 21

3.1.2 The decryption process 23

3.1.3 The key schedule 23

3.2 Group Operations and their Interaction 25

3.2.1 The three operations as quasigroup operations 25

3.2.2 Polynomial expressions for multiplication and addition 27

3.3 Security Features of IDEA 30

3.3.1 Confusion 31

Bibliografische Informationen
http://d-nb.info/920912710

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3.3.2 Diffusion 32

3.3.3 Perfect secrecy for a "one-time" key 33

3.4 Implementations of the Cipher 34

3.4.1 Similarity of encryption and decryption 34

3.4.2 Low-High algorithm for multiplication 35

3.4.3 C-program of IDEA cipher and sample data 36

4 Markov Ciphers and Differential Cryptanalysis **41**

4.1 Markov Ciphers 41

4.2 Differential Cryptanalysis 46

4.2.1 The round differentials 46

4.2.2 Differential cryptanalysis attack 46

4.2.3 Hypothesis of stochastic equivalence 48

4.3 Complexity of Differential Cryptanalysis Attack 49

4.4 Security of Markov Ciphers 51

4.4.1 When is a Markov cipher secure? 51

4.4.2 The number of iterations 53

4.4.3 Non-symmetry of the transition matrix 54

5 Differential Cryptanalysis of the IDEA Cipher **57**

5.1 Transition Matrices of IDEA(m) 58

5.1.1 Experimental results for mini IDEA ciphers 61

5.2 High-Probability Differentials of IDEA 64

5.2.1 Transparencies of the MA-structure 66

5.2.2 Differentials based on the trivial transparency of the MA-structure 69

5.2.3 Differentials based on the non-trivial transparency of the MA-structure 72

5.2.4 Weak-key differentials 74

5.2.5 Differentials under the group operation XOR 77

5.3 Security of IDEA against Differential Cryptanalysis 78

6 Hash Functions Based on Block Ciphers **81**

6.1 Hash Functions 81

6.2 Iterated Hash Functions and Attacks 82

6.2.1 Security of an iterated hash function and strength of the hash round function 83

6.3 Hash Round Functions based on Block Ciphers 88

6.3.1 Constructions of m-bit hash round functions 88

6.4 Construction of $2m$-bit Hash Round Function 89

6.4.1 Quasigroup ciphers and one-way permutations 89

6.4.2 A principle for evaluating hash round functions and four attacks on three $2m$-bit hash round functions 91

6.4.3 Complexity of known attacks on some $2m$-bit hash functions . 97

6.4.4 Proposed schemes for block ciphers with $k = 2m$ 98

7 Concluding Remarks **101**

Bibliography **103**

Index **108**