

Contents

| | | | | | |
|----------|-----------------------------------------------------------|-----------|-----------|---------------------------------------------------------|-----------|
| 1 | Introduction | 3 | 8.6 | Partial Key Guessing Attacks | 46 |
| 2 | Twofish Design Goals | 3 | 8.7 | Related-key Cryptanalysis | 46 |
| 3 | Twofish Building Blocks | 4 | 8.8 | A Related-Key Attack on a Twofish Variant | 48 |
| 3.1 | Feistel Networks | 4 | 8.9 | Side-Channel Cryptanalysis and Fault Analysis | 50 |
| 3.2 | S-boxes | 5 | 8.10 | Attacking Simplified Twofish | 50 |
| 3.3 | MDS Matrices | 5 | 9 | Trap Doors in Twofish | 52 |
| 3.4 | Pseudo-Hadamard Transforms | 5 | 10 | When is a Cipher Insecure? | 53 |
| 3.5 | Whitening | 5 | 11 | Using Twofish | 53 |
| 3.6 | Key Schedule | 5 | 11.1 | Chaining Modes | 53 |
| 4 | Twofish | 5 | 11.2 | One-Way Hash Functions | 53 |
| 4.1 | The Function F | 7 | 11.3 | Message Authentication Codes | 53 |
| 4.2 | The Function g | 7 | 11.4 | Pseudo-Random Number Generators | 53 |
| 4.3 | The Key Schedule | 8 | 11.5 | Larger Keys | 54 |
| 4.4 | Round Function Overview | 12 | 11.6 | Additional Block Sizes | 54 |
| 5 | Performance of Twofish | 12 | 11.7 | More or Fewer Rounds | 54 |
| 5.1 | Performance on Large Microprocessors | 12 | 11.8 | Family Key Variant: Twofish-FK | 54 |
| 5.2 | Performance on Smart Cards | 15 | 12 | Historical Remarks | 56 |
| 5.3 | Performance on Future Microprocessors | 16 | 13 | Conclusions and Further Work | 57 |
| 5.4 | Hardware Performance | 17 | 14 | Acknowledgments | 58 |
| 6 | Twofish Design Philosophy | 18 | A | Twofish Test Vectors | 65 |
| 6.1 | Performance-Driven Design | 18 | A.1 | Intermediate Values | 65 |
| 6.2 | Conservative Design | 19 | A.2 | Full Encryptions | 67 |
| 6.3 | Simple Design | 20 | | | |
| 6.4 | S-boxes | 21 | | | |
| 6.5 | The Key Schedule | 22 | | | |
| 7 | The Design of Twofish | 23 | | | |
| 7.1 | The Round Structure | 23 | | | |
| 7.2 | The Key-dependent S-boxes | 24 | | | |
| 7.3 | MDS Matrix | 27 | | | |
| 7.4 | PHT | 29 | | | |
| 7.5 | Key Addition | 29 | | | |
| 7.6 | Feistel Combining Operation | 29 | | | |
| 7.7 | Use of Different Groups | 29 | | | |
| 7.8 | Diffusion in the Round Function | 29 | | | |
| 7.9 | One-bit Rotation | 30 | | | |
| 7.10 | The Number of Rounds | 31 | | | |
| 7.11 | The Key Schedule | 31 | | | |
| 7.12 | Reed-Solomon Code | 36 | | | |
| 8 | Cryptanalysis of Twofish | 36 | | | |
| 8.1 | Differential Cryptanalysis | 36 | | | |
| 8.2 | Extensions to Differential Cryptanalysis | 41 | | | |
| 8.3 | Search for the Best Differential Characteristic | 41 | | | |
| 8.4 | Linear Cryptanalysis | 44 | | | |
| 8.5 | Interpolation Attack | 45 | | | |