

# CONTENTS

## Block Ciphers: Differential and Linear Cryptanalysis

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| The first experimental cryptanalysis of the Data Encryption Standard . . . . . | 1  |
| <i>Mitsuru Matsui</i>                                                          |    |
| Linear cryptanalysis of the Fast Data Encipherment Algorithm . . . . .         | 12 |
| <i>Kazuo Ohta and Kazumaro Aoki</i>                                            |    |
| Differential-linear cryptanalysis . . . . .                                    | 17 |
| <i>Susan K. Langford and Martin E. Hellman</i>                                 |    |
| Linear cryptanalysis using multiple approximations . . . . .                   | 26 |
| <i>Burton S. Kaliski Jr. and M. J. B. Robshaw</i>                              |    |

## Schemes Based on New Problems

|                                                                                                                |    |
|----------------------------------------------------------------------------------------------------------------|----|
| Hashing with $SL_2$ . . . . .                                                                                  | 40 |
| <i>Jean-Pierre Tillich and Gilles Zémor</i>                                                                    |    |
| Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks . . . . . | 50 |
| <i>Jinhui Chao, Kazuo Tanada and Shigeo Tsujii</i>                                                             |    |
| Cryptographic protocols based on discrete logarithms in real-quadratic orders . . . . .                        | 56 |
| <i>Ingrid Biehl, Johannes Buchmann and Christoph Thiel</i>                                                     |    |

## Signatures I

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Designated confirmer signatures and public-key encryption are equivalent . . . . . | 61 |
| <i>Tatsuaki Okamoto</i>                                                            |    |
| Directed acyclic graphs, one-way functions and digital signatures . . . . .        | 75 |
| <i>Daniel Bleichenbacher and Ueli M. Maurer</i>                                    |    |
| An identity-based signature scheme with bounded life-span . . . . .                | 83 |
| <i>Olivier Delos and Jean-Jacques Quisquater</i>                                   |    |

## Implementation and Hardware Aspects

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| More flexible exponentiation with precomputation . . . . .            | 95  |
| <i>Chae Hoon Lim and Pil Joong Lee</i>                                |     |
| A parallel permutation multiplier for a PGM crypto-chip . . . . .     | 108 |
| <i>Tamás Horváth, Spyros S. Magliveras and Tran van Trung</i>         |     |
| Cryptographic randomness from air turbulence in disk drives . . . . . | 114 |
| <i>Don Davis, Ross Ihaka and Philip Fenstermacher</i>                 |     |

## Authentication and Secret Sharing

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| Cryptanalysis of the Gemmell and Naor multi-round authentication protocol . . . . .                   | 121 |
| <i>Christian Gehrman</i>                                                                              |     |
| LFSR-based hashing and authentication . . . . .                                                       | 129 |
| <i>Hugo Krawczyk</i>                                                                                  |     |
| New bound on authentication code with arbitration . . . . .                                           | 140 |
| <i>Kaoru Kurosawa</i>                                                                                 |     |
| Multi-secret sharing schemes . . . . .                                                                | 150 |
| <i>Carlo Blundo, Alfredo De Santis, Giovanni Di Crescenzo, Antonio Giorgio Gaggia and Ugo Vaccaro</i> |     |

## Zero-Knowledge

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Designing identification schemes with keys of short size . . . . .                      | 164 |
| <i>Jacques Stern</i>                                                                    |     |
| Proofs of partial knowledge and simplified design of witness hiding protocols . . . . . | 174 |
| <i>Ronald Cramer, Ivan Damgård and Berry Schoenmakers</i>                               |     |
| Language dependent secure bit commitment . . . . .                                      | 188 |
| <i>Toshiya Itoh, Yuji Ohta and Hiroki Shizuya</i>                                       |     |
| On the length of cryptographic hash-values used in identification schemes . . . . .     | 202 |
| <i>Marc Girault and Jacques Stern</i>                                                   |     |

## Signatures II

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| Incremental cryptography: the case of hashing and signing . . . . .                       | 216 |
| <i>Mihir Bellare, Oded Goldreich and Shafi Goldwasser</i>                                 |     |
| An efficient existentially unforgeable signature scheme and<br>its applications . . . . . | 234 |
| <i>Cynthia Dwork and Moni Naor</i>                                                        |     |

## Combinatorics and its Applications

|                                                                |     |
|----------------------------------------------------------------|-----|
| Bounds for resilient functions and orthogonal arrays . . . . . | 247 |
| <i>Jürgen Bierbrauer, K. Gopalakrishnan and D. R. Stinson</i>  |     |
| Tracing traitors . . . . .                                     | 257 |
| <i>Benny Chor, Amos Fiat and Moni Naor</i>                     |     |

## Number Theory

|                                                                                                                |     |
|----------------------------------------------------------------------------------------------------------------|-----|
| Towards the equivalence of breaking the Diffie-Hellman protocol and<br>computing discrete logarithms . . . . . | 271 |
| <i>Ueli M. Maurer</i>                                                                                          |     |
| Fast generation of provable primes using search in arithmetic<br>progressions . . . . .                        | 282 |
| <i>Preda Mihailescu</i>                                                                                        |     |

## Cryptanalysis and Protocol Failures

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| Attack on the cryptographic scheme NIKS-TAS . . . . .                    | 294 |
| <i>Don Coppersmith</i>                                                   |     |
| On the risk of opening distributed keys . . . . .                        | 308 |
| <i>Mike Burmester</i>                                                    |     |
| Cryptanalysis of cryptosystems based on remote chaos replication . . . . | 318 |
| <i>Th. Beth, D. E. Lazic and A. Mathias</i>                              |     |

## Pseudo-Random Generation

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| A Fourier transform approach to the linear complexity of nonlinearly filtered sequences . . . . . | 332 |
| <i>James L. Massey and Shirlei Serconek</i>                                                       |     |

## Block Ciphers: Design and Cryptanalysis

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| The security of cipher block chaining . . . . .                                       | 341 |
| <i>Mihir Bellare, Joe Kilian and Phillip Rogaway</i>                                  |     |
| A chosen plaintext attack of the 16-round Khufu cryptosystem . . . . .                | 359 |
| <i>Henri Gilbert and Pascal Chauvaud</i>                                              |     |
| Ciphertext only attack for one-way function of the MAP using one ciphertext . . . . . | 369 |
| <i>Yukiyasu Tsunoo, Eiji Okamoto and Tomohiko Uyematsu</i>                            |     |
| Pitfalls in designing substitution boxes . . . . .                                    | 383 |
| <i>Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng</i>                              |     |

## Secure Computations and Protocols

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| A randomness-rounds tradeoff in private computation . . . . .      | 397 |
| <i>Eyal Kushilevitz and Adi Rosén</i>                              |     |
| Secure voting using partially compatible homomorphisms . . . . .   | 411 |
| <i>Kazuo Sako and Joe Kilian</i>                                   |     |
| Maintaining security in the presence of transient faults . . . . . | 425 |
| <i>Ran Canetti and Amir Herzberg</i>                               |     |

|                        |     |
|------------------------|-----|
| Author Index . . . . . | 439 |
|------------------------|-----|