

Table of Contents

XTR and NTRU

| | |
|---|----|
| The XTR Public Key System | 1 |
| <i>Arjen K. Lenstra, Eric R. Verheul</i> | |
| A Chosen-Ciphertext Attack against NTRU | 20 |
| <i>Éliane Jaulmes, Antoine Joux</i> | |

Privacy for Databases

| | |
|--|----|
| Privacy Preserving Data Mining | 36 |
| <i>Yehuda Lindell, Benny Pinkas</i> | |
| Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing | 55 |
| <i>Amos Beimel, Yuval Ishai, Tal Malkin</i> | |

Secure Distributed Computation and Applications

| | |
|--|-----|
| Parallel Reducibility for Information-Theoretically Secure Computation . . . | 74 |
| <i>Yevgeniy Dodis, Silvio Micali</i> | |
| Optimistic Fair Secure Computation | 93 |
| <i>Christian Cachin, Jan Camenisch</i> | |
| A Cryptographic Solution to a Game Theoretic Problem | 112 |
| <i>Yevgeniy Dodis, Shai Halevi, Tal Rabin</i> | |

Algebraic Cryptosystems

| | |
|---|-----|
| Differential Fault Attacks on Elliptic Curve Cryptosystems | 131 |
| <i>Ingrid Biehl, Bernd Meyer, Volker Müller</i> | |
| Quantum Public-Key Cryptosystems | 147 |
| <i>Tatsuaki Okamoto, Keisuke Tanaka, Shigenori Uchiyama</i> | |
| New Public-Key Cryptosystem Using Braid Groups | 166 |
| <i>Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park</i> | |

Message Authentication

| | |
|--|-----|
| Key Recovery and Forgery Attacks on the MacDES MAC Algorithm | 184 |
| <i>Don Coppersmith, Lars R. Knudsen, Chris J. Mitchell</i> | |

| | |
|---|-----|
| CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions | 197 |
| <i>John Black, Phillip Rogaway</i> | |

| | |
|---|-----|
| L-collision Attacks against Randomized MACs | 216 |
| <i>Michael Semanko</i> | |

Digital Signatures

| | |
|---|-----|
| On the Exact Security of Full Domain Hash | 229 |
| <i>Jean-Sébastien Coron</i> | |

| | |
|-----------------------------|-----|
| Timed Commitments | 236 |
| <i>Dan Boneh, Moni Naor</i> | |

| | |
|---|-----|
| A Practical and Provably Secure Coalition-Resistant Group Signature Scheme | 255 |
| <i>Giuseppe Ateniese, Jan Camenisch, Marc Joye, Gene Tsudik</i> | |

| | |
|--|-----|
| Provably Secure Partially Blind Signatures | 271 |
| <i>Masayuki Abe, Tatsuaki Okamoto</i> | |

Cryptanalysis

| | |
|--|-----|
| Weaknesses in the $SL_2(\mathbb{F}_{2^n})$ Hashing Scheme | 287 |
| <i>Rainer Steinwandt, Markus Grassl, Willi Geiselmann, Thomas Beth</i> | |

| | |
|---|-----|
| Fast Correlation Attacks through Reconstruction of Linear Polynomials | 300 |
| <i>Thomas Johansson, Fredrik Jönsson</i> | |

Traitor Tracing and Broadcast Encryption

| | |
|---|-----|
| Sequential Traitor Tracing | 316 |
| <i>Reihaneh Safavi-Naini, Yejing Wang</i> | |

| | |
|---|-----|
| Long-Lived Broadcast Encryption | 333 |
| <i>Juan A. Garay, Jessica Staddon, Avishai Wool</i> | |

Invited Talk

| | |
|----------------------|-----|
| Taming the Adversary | 353 |
| <i>Martín Abadi</i> | |

Symmetric Encryption

| | |
|--|-----|
| The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search | 359 |
| <i>Anand Desai</i> | |

| | |
|---|-----|
| On the Round Security of Symmetric-Key Cryptographic Primitives | 376 |
| <i>Zulfikar Ramzan, Leonid Reyzin</i> | |

| | |
|--|-----|
| New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack | 394 |
| <i>Anand Desai</i> | |

To Commit or Not to Commit

| | |
|--|-----|
| Efficient Non-malleable Commitment Schemes | 413 |
| <i>Marc Fischlin, Roger Fischlin</i> | |

| | |
|--|-----|
| Improved Non-committing Encryption Schemes Based on a General Complexity Assumption | 432 |
| <i>Ivan Damgård, Jesper Buus Nielsen</i> | |

Protocols

| | |
|---|-----|
| A Note on the Round-Complexity of Concurrent Zero-Knowledge | 451 |
| <i>Alon Rosen</i> | |
| An Improved Pseudo-random Generator Based on Discrete Log | 469 |
| <i>Rosario Gennaro</i> | |
| Linking Classical and Quantum Key Agreement: Is There “Bound Information”? | 482 |
| <i>Nicolas Gisin, Stefan Wolf</i> | |

Stream Ciphers and Boolean Functions

| | |
|--|-----|
| Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers . . . | 501 |
| <i>Muxiang Zhang, Agnes Chan</i> | |
| Nonlinearity Bounds and Constructions of Resilient Boolean Functions . . . | 515 |
| <i>Palash Sarkar, Subhamoy Maitra</i> | |
| Almost Independent and Weakly Biased Arrays: Efficient Constructions and Cryptologic Applications | 533 |
| <i>Jürgen Bierbrauer, Holger Schellwat</i> | |
| Author Index | 545 |

<http://www.springer.com/978-3-540-67907-3>

Advances in Cryptology - CRYPTO 2000

20th Annual International Cryptology Conference, Santa
Barbara, California, USA, August 20-24, 2000.

Proceedings

Bellare, M. (Ed.)

2000, XI, 543 p., Softcover

ISBN: 978-3-540-67907-3