

CONTENTS

MAC and Hash

- MDx-MAC and Building Fast MACs from Hash Functions..... 1
Bart Preneel and Paul C. van Oorschot
- XOR MACs: New Methods for Message Authentication Using
Finite Pseudorandom Functions 15
Mihir Bellare, Roch Guérin and Phillip Rogaway
- Bucket Hashing and its Application to Fast Message Authentication..... 29
Phillip Rogaway

Number Theory I

- Fast Key Exchange with Elliptic Curve Systems 43
*Richard Schroepel, Hilarie Orman, Sean O'Malley and
Oliver Spatscheck*
- Fast Server-Aided RSA Signatures Secure Against Active Attacks..... 57
Philippe Béguin and Jean-Jacques Quisquater
- Security and Performance of Server-Aided RSA Computation Protocols..... 70
Chae Hoon Lim and Pil Joong Lee

Oblivious Transfer

- Efficient Commitment Schemes with Bounded Sender and
Unbounded Receiver..... 84
Shai Halevi
- Precomputing Oblivious Transfer..... 97
Donald Beaver
- Committed Oblivious Transfer and Private Multi-Party Computation 110
Claude Crépeau, Jeroen van de Graaf and Alain Tapp
- On the Security of the Quantum Oblivious Transfer and Key
Distribution Protocols..... 124
Dominic Mayers

Cryptanalysis I

How to Break Shamir's Asymmetric Basis	136
<i>Thorsten Theobald</i>	
On the Security of the Gollmann Cascades	148
<i>Sang-Joon Park, Sang-Jin Lee and Seung-Cheol Goh</i>	
Improving the Search Algorithm for the Best Linear Expression	157
<i>Kazuo Ohta, Shiho Moriai and Kazumaro Aoki</i>	
On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm	171
<i>Burton S. Kaliski Jr. and Yiqun Lisa Yin</i>	

Key Escrow

A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-like Key Escrow Systems	185
<i>Silvio Micali and Ray Sidney</i>	
A Key Escrow System with Warrant Bounds	197
<i>Arjen K. Lenstra, Peter Winkler and Yacov Yacobi</i>	
Fair Cryptosystems, Revisited	208
<i>Joe Kilian and Tom Leighton</i>	
Escrow Encryption Systems Visited: Attacks, Analysis and Designs	222
<i>Yair Frankel and Moti Yung</i>	

Protocols

Robustness Principles for Public Key Protocols.....	236
<i>Ross Anderson and Roger Needham</i>	

Cryptanalysis II

Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88.....	248
<i>Jacques Patarin</i>	
Cryptanalysis Based on 2-Adic Rational Approximation.....	262
<i>Andrew Klapper and Mark Goresky</i>	
A Key-schedule Weakness in SAFER K-64.....	274
<i>Lars R. Knudsen</i>	
Cryptanalysis of the Immunized LL Public Key Systems.....	287
<i>Yair Frankel and Moti Yung</i>	

Zero Knowledge, Interactive Protocols

Secure Signature Schemes based on Interactive Protocols.....	297
<i>Ronald Cramer and Ivan Damgård</i>	
Improved Efficient Arguments.....	311
<i>Joe Kilian</i>	
Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs.....	325
<i>Ivan Damgård, Oded Goldreich, Tatsuaki Okamoto and Avi Wigderson</i>	

Secret Sharing

Proactive Secret Sharing Or: How to Cope With Perpetual Leakage.....	339
<i>Amir Herzberg, Stanisław Jarecki, Hugo Krawczyk and Moti Yung</i>	
Secret Sharing with Public Reconstruction.....	353
<i>Amos Beimel and Benny Chor</i>	
On General Perfect Secret Sharing Schemes.....	367
<i>G. R. Blakley and G. A. Kabatianski</i>	

Number Theory II

NFS with Four Large Primes: An Explosive Experiment.....	372
<i>Bruce Dodson and Arjen K. Lenstra</i>	
Some Remarks on Lucas-Based Cryptosystems	386
<i>Daniel Bleichenbacher, Wieb Bosma and Arjen K. Lenstra</i>	

Secret Sharing II

Threshold DSS Signatures without a Trusted Party	397
<i>Susan K. Langford</i>	
t -Cheater Identifiable (k,n) Threshold Secret Sharing Schemes	410
<i>Kaoru Kurosawa, Satoshi Obana and Wakaha Ogata</i>	

Everything Else

Quantum Cryptanalysis of Hidden Linear Functions.....	424
<i>Dan Boneh and Richard J. Lipton</i>	
An Efficient Divisible Electronic Cash Scheme	438
<i>Tatsuaki Okamoto</i>	
Collusion-Secure Fingerprinting for Digital Data	452
<i>Dan Boneh and James Shaw</i>	

Author Index	467
---------------------------	-----



<http://www.springer.com/978-3-540-60221-7>

Advances in Cryptology — CRYPTO '95
15th Annual International Cryptology Conference, Santa
Barbara, California, USA, August 27–31, 1995.

Proceedings

Coppersmith, D. (Ed.)

1995, XII, 466 p., Softcover

ISBN: 978-3-540-60221-7