

Contents

Complexity Theory

The Complexity of Computing Hard Core Predicates	1
<i>Mikael Goldmann and Mats Näslund</i>	
Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations	16
<i>Eiichiro Fujisaki and Tatsuaki Okamoto</i>	
Keeping the SZK-Verifier Honest Unconditionally	31
<i>Giovanni Di Crescenzo, Tatsuaki Okamoto, and Moti Yung</i>	

Invited Lecture

On the Foundations of Modern Cryptography	46
<i>Oded Goldreich</i>	

Cryptographic Primitives

Plug and Play Encryption	75
<i>Donald Beaver</i>	
Deniable Encryption	90
<i>Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky</i>	

Lattice-Based Cryptography

Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem	105
<i>Oded Goldreich, Shafi Goldwasser, and Shai Halevi</i>	
Public-Key Cryptosystems from Lattice Reduction Problems	112
<i>Oded Goldreich, Shafi Goldwasser, and Shai Halevi</i>	

Digital Signatures

RSA-Based Undeniable Signatures	132
<i>Rosario Gennaro, Hugo Krawczyk, and Tal Rabin</i>	
Security of Blind Digital Signatures	150
<i>Ari Juels, Michael Luby, and Rafail Ostrovsky</i>	
Digital Signcryption or How to Achieve Cost (Signature & Encryption) \ll Cost (Signature) + Cost (Encryption)	165
<i>Yuliang Zheng</i>	
How to Sign Digital Streams	180
<i>Rosario Gennaro and Pankaj Rohatgi</i>	

Cryptanalysis of Public-Key Cryptosystems (I)

Merkle-Hellman Revisited: A Cryptanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorizations	198
<i>Phong Nguyen and Jacques Stern</i>	
Failure of the McEliece Public-Key Cryptosystem Under Message-Resend and Related-Message Attack	213
<i>Thomas A. Berson</i>	
A Multiplicative Attack Using LLL Algorithm on RSA Signatures with Redundancy	221
<i>Jean-François Misarsky</i>	

Cryptanalysis of Public-Key Cryptosystems (II)

On the Security of the KMOV Public Key Cryptosystem	235
<i>Daniel Bleichenbacher</i>	
A Key Recovery Attack on Discrete Log-Based Schemes Using a Prime Order Subgroup.....	249
<i>Chae Hoon Lim and Pil Joong Lee</i>	
The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems	264
<i>Adam Young and Moti Yung</i>	
“Pseudo-Random” Number Generation within Cryptographic Algorithms: The DSS Case	277
<i>Mihir Bellare, Shafi Goldwasser, and Daniele Micciancio</i>	

Information Theory

Unconditional Security Against Memory-Bounded Adversaries.....	292
<i>Christian Cachin and Ueli Maurer</i>	
Privacy Amplification Secure Against Active Adversaries	307
<i>Ueli Maurer and Stefan Wolf</i>	
Visual Authentication and Identification	322
<i>Moni Naor and Benny Pinkas</i>	

Invited Lecture

Quantum Information Processing: The Good, the Bad and the Ugly.....	337
<i>Gilles Brassard</i>	

Elliptic Curve Implementation

Efficient Algorithms for Elliptic Curve Cryptosystems	342
<i>Jorge Guajardo and Christof Paar</i>	
An Improved Algorithm for Arithmetic on a Family of Elliptic Curves	357
<i>Jerome A. Solinas</i>	

Number-Theoretic Systems

Fast RSA-Type Cryptosystems Using n -adic Expansion	372
<i>Tsuyoshi Takagi</i>	
A One Way Function Based on Ideal Arithmetic in Number Fields	385
<i>Johannes Buchmann and Sachar Paulus</i>	

Distributed Cryptography

Efficient Anonymous Multicast and Reception	395
<i>Shlomi Dolev and Rafail Ostrovsky</i>	
Efficient Group Signature Schemes for Large Groups	410
<i>Jan Camenisch and Markus Stadler</i>	
Efficient Generation of Shared RSA Keys	425
<i>Dan Boneh and Matthew Franklin</i>	
Proactive RSA	440
<i>Yair Frankel, Peter Gemmell, Philip D. MacKenzie, and Moti Yung</i>	

Hash Functions

Towards Realizing Random Oracles: Hash Functions that Hide All Partial Information	455
<i>Ran Canetti</i>	
Collision-Resistant Hashing: Towards Making UOWHFs Practical	470
<i>Mihir Bellare and Phillip Rogaway</i>	
Fast and Secure Hashing Based on Codes	485
<i>Lars Knudsen and Bart Preneel</i>	

Cryptanalysis of Secret-Key Cryptosystems

Edit Distance Correlation Attack on the Alternating Step Generator	499
<i>Jovan Dj. Golić and Renato Menicocci</i>	
Differential Fault Analysis of Secret Key Cryptosystems	513
<i>Eli Biham and Adi Shamir</i>	

Cryptanalysis of the Cellular Message Encryption Algorithm	526
<i>David Wagner, Bruce Schneier, and John Kelsey</i>	

Author Index.....	539
--------------------------	------------

Erratum.....	540
---------------------	------------

<http://www.springer.com/978-3-540-63384-6>

Advances in Cryptology - CRYPTO '97

17th Annual International Cryptology Conference, Santa
Barbara, California, USA, August 17-21, 1997,

Proceedings

Kaliski, B.S.J. (Ed.)

1997, 546 p., Softcover

ISBN: 978-3-540-63384-6