

Contents

Complexity Theory

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

Invited Lecture

- On the Foundations of Modern Cryptography 46
Oded Goldreich

Cryptographic Primitives

- Plug and Play Encryption 75
Donald Beaver
- Deniable Encryption 90
Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky

Lattice-Based Cryptography

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

Digital Signatures

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

Cryptanalysis of Public-Key Cryptosystems (I)

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

Cryptanalysis of Public-Key Cryptosystems (II)

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

Information Theory

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

Invited Lecture

- Quantum Information Processing: The Good, the Bad and the Ugly 337
Gilles Brassard

Elliptic Curve Implementation

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

Number-Theoretic Systems

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

Distributed Cryptography

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

Hash Functions

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

Cryptanalysis of Secret-Key Cryptosystems

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

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

Author Index **539**

Erratum **540**