

CONTENTS

Distributed Cryptography and Applications I

- Securing threshold cryptosystems against chosen ciphertext attack 1
Victor Shoup and Rosario Gennaro
- Auto-recoverable auto-certifiable cryptosystems 17
Adam Young and Moti Yung
- A practical and provably secure scheme for publicly verifiable secret
sharing and its applications 32
Eiichiro Fujisaki and Tatsuaki Okamoto

Complexity Theory: Reductions and Lower Bounds

- Equivalence of counting the number of points on elliptic curve over the
ring \mathbb{Z}_n and factoring n 47
Noboru Kunihiro and Kenji Koyama
- Breaking RSA may not be equivalent to factoring 59
Dan Boneh and Ramarathnam Venkatesan
- Lower bounds on generic algorithms in groups 72
Ueli Maurer and Stefan Wolf

Cryptanalysis of Block Ciphers

- Improved cryptanalysis of RC5 85
Alex Biryukov and Eyal Kushilevitz
- Cryptanalysis of the ANSI X9.52 CBCM mode 100
Eli Biham and Lars R. Knudsen
- Differential-linear weak key classes of IDEA 112
Philip Hawkes

Distributed Cryptography and Applications II

- Divertible protocols and atomic proxy cryptography 127
Matt Blaze, Gerrit Bleumer, and Martin Strauss
- Optimum traitor tracing and asymmetric schemes 145
Kaoru Kurosawa and Yvo Desmedt

Computational Algorithms

On finding small solutions of modular multivariate polynomial equations	158
<i>Charanjit S. Jutla</i>	
Computing discrete logarithms with quadratic number rings	171
<i>Damian Weber</i>	
Improved algorithms for isomorphisms of polynomials	184
<i>Jacques Patarin, Louis Goubin and Nicolas Courtois</i>	

Improving Computational Efficiency

Visual cryptanalysis	201
<i>Adi Shamir</i>	
How to improve an exponentiation black-box	211
<i>G�rard Cohen, Antoine Lobstein, David Naccache, and Gilles Z�mor</i>	
Speeding up discrete log and factoring based schemes via precomputations	221
<i>Victor Boyko, Marcus Peinado, and Ramarathnam Venkatesan</i>	
Fast batch verification for modular exponentiation and digital signatures . .	236
<i>Mihir Bellare, Juan A. Garay, and Tal Rabin</i>	

Paradigms for Symmetric Systems

A formal treatment of remotely keyed encryption	251
<i>Matt Blaze, Joan Feigenbaum, and Moni Naor</i>	
Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible	266
<i>Mihir Bellare, Ted Krovetz, and Phillip Rogaway</i>	
The chain & sum primitive and its applications to MACs and stream ciphers	281
<i>Mariusz H. Jakubowski and Ramarathnam Venkatesan</i>	

Public Key Cryptosystems

A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption	294
<i>Detlef H�hnlein, Michael J. Jacobson, Sachar Paulus, and Tsuyoshi Takagi</i>	
A new public-key cryptosystem as secure as factoring	308
<i>Tatsuaki Okamoto and Shigenori Uchiyama</i>	

Complexity Theory: One-Way Functions

Towards a better understanding of one-wayness:

Facing linear permutations 319

Alain P. Hiltgen

Finding collisions on a one-way street:

Can secure hash functions be based on general assumptions? 334

Daniel R. Simon

Multi-party Computation

Secure communication in minimal connectivity models 346

Matthew Franklin and Rebecca N. Wright

On the foundations of oblivious transfer 361

Christian Cachin

Quorum-based secure multi-party computation 375

Donald Beaver and Avishai Wool

Digital Signatures

Strengthened security for blind signatures 391

David Pointcheval

Generic constructions for secure and efficient

confirmer signature schemes 406

Markus Michels and Markus Stadler

Security analysis of a practical “on the fly” authentication

and signature generation 422

Guillaume Poupard and Jacques Stern

Untraceability in Multi-party Schemes

Universally verifiable mix-net with verification work independent

of the number of mix-servers 437

Masayuki Abe

A practical mix 448

Markus Jakobsson

Boolean Functions

On the propagation criterion of degree ℓ and order k	462
<i>Claude Carlet</i>	

Highly nonlinear balanced Boolean functions with a good correlation-immunity	475
<i>Eric Filiol and Caroline Fontaine</i>	

Heuristic design of cryptographically strong balanced Boolean functions . . .	489
<i>William Millan, Andrew Clark, and Ed Dawson</i>	

Combinatorial Design and Analysis of Distributed Schemes

Secret sharing schemes with bipartite access structure	500
<i>Carles Padró and Germán Sáez</i>	

Combinatorial bounds for broadcast encryption	512
<i>Michael Luby and Jessica Staddon</i>	

New results on multi-receiver authentication codes	527
<i>Rei Safavi-Naini and Huaxiong Wang</i>	

Cryptanalysis of Elliptic Curve Systems

Specialized integer factorization	542
<i>Don Coppersmith</i>	

Security of an identity-based cryptosystem and the related reductions	546
<i>Tatsuaki Okamoto and Shigenori Uchiyama</i>	

Electronic Commerce and Payment

Easy come - easy go divisible cash	561
<i>Agnes Chan, Yair Frankel, and Yiannis Tsiounis</i>	

Secure and efficient metering	576
<i>Moni Naor and Benny Pinkas</i>	

Optimistic fair exchange of digital signatures	591
<i>N. Asokan, Victor Shoup, and Michael Waidner</i>	

Author Index	607
------------------------	-----

Advances in Cryptology - EUROCRYPT '98
International Conference on the Theory and Application
of Cryptographic Techniques, Espoo, Finland, May 31 -
June 4, 1998, Proceedings
Nyberg, K. (Ed.)
1998, XI, 613 p., Softcover
ISBN: 978-3-540-64518-4