

# Table of Contents

## Cryptanalysis I

Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers . . . . .	1
<i>Alex Biryukov, Adi Shamir</i>	
Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99 . . . . .	14
<i>Glenn Durfee, Phong Q. Nguyen</i>	
Why Textbook ElGamal and RSA Encryption Are Insecure . . . . .	30
<i>Dan Boneh, Antoine Joux, Phong Q. Nguyen</i>	
Cryptanalysis of the TTM Cryptosystem . . . . .	44
<i>Louis Goubin, Nicolas T. Courtois</i>	
Attacking and Repairing Batch Verification Schemes . . . . .	58
<i>Colin Boyd, Chris Pavlovski</i>	

## IACR Distinguished Lecture

Cryptography Everywhere . . . . .	72
<i>Thomas A. Berson</i>	

## Digital Signatures

Security of Signed ElGamal Encryption . . . . .	73
<i>Claus P. Schnorr, Markus Jakobsson</i>	
From Fixed-Length to Arbitrary-Length RSA Padding Schemes . . . . .	90
<i>Jean-Sébastien Coron, Francois Koeune, David Naccache</i>	
Towards Signature-Only Signature Schemes . . . . .	97
<i>Adam Young, Moti Yung</i>	
A New Forward-Secure Digital Signature Scheme . . . . .	116
<i>Michel Abdalla, Leonid Reyzin</i>	
Unconditionally Secure Digital Signature Schemes Admitting Transferability . . . . .	130
<i>Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, Hideki Imai</i>	

## Protocols I

Efficient Secure Multi-party Computation . . . . .	143
<i>Martin Hirt, Ueli Maurer, Bartosz Przydatek</i>	

Mix and Match: Secure Function Evaluation via Ciphertexts .....	162
<i>Markus Jakobsson, Ari Juels</i>	
A Length-Invariant Hybrid Mix .....	178
<i>Miyako Ohkubo, Masayuki Abe</i>	
Attack for Flash MIX .....	192
<i>Masashi Mitomo, Kaoru Kurosawa</i>	
Distributed Oblivious Transfer .....	205
<i>Moni Naor, Benny Pinkas</i>	

## Number Theoretic Algorithms

Key Improvements to XTR.....	220
<i>Arjen K. Lenstra, Eric R. Verheul</i>	
Security of Cryptosystems Based on Class Groups of Imaginary Quadratic Orders .....	234
<i>Safuat Hamdy, Bodo Möller</i>	
Weil Descent of Elliptic Curves over Finite Fields of Characteristic Three .....	248
<i>Seigo Arita</i>	
Construction of Hyperelliptic Curves with CM and Its Application to Cryptosystems .....	259
<i>Jinhui Chao, Kazuto Matsuo, Hiroto Kawashiro, Shigeo Tsujii</i>	

## Symmetric-Key Schemes I

Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis .....	274
<i>Jaechul Sung, Sangjin Lee, Jongin Lim, Seokhie Hong, Sangjoon Park</i>	
On the Pseudorandomness of Top-Level Schemes of Block Ciphers .....	289
<i>Shiho Moriai, Serge Vaudenay</i>	
Exploiting Multiples of the Connection Polynomial in Word-Oriented Stream Ciphers .....	303
<i>Philip Hawkes, Gregory G. Rose</i>	
Encode-Then-Encipher Encryption: How to Exploit Nonces or Redundancy in Plaintexts for Efficient Cryptography .....	317
<i>Mihir Bellare, Phillip Rogaway</i>	

## Protocols II

Verifiable Encryption, Group Encryption, and Their Applications to Separable Group Signatures and Signature Sharing Schemes . . . . .	331
<i>Jan Camenisch, Ivan Damgård</i>	
Addition of ElGamal Plaintexts . . . . .	346
<i>Markus Jakobsson, Ari Juels</i>	
Improved Methods to Perform Threshold RSA . . . . .	359
<i>Brian King</i>	
Comital Deniable Proofs and Electronic Campaign Finance . . . . .	373
<i>Matt Franklin, Tomas Sander</i>	
Provably Secure Metering Scheme . . . . .	388
<i>Wakaha Ogata, Kaoru Kurosawa</i>	

## Invited Lecture

CRYPTREC Project - Cryptographic Evaluation Project for the Japanese Electronic Government - . . . . .	399
<i>Hideki Imai, Atsuhiko Yamagishi</i>	

## Fingerprinting

Anonymous Fingerprinting with Direct Non-repudiation . . . . .	401
<i>Birgit Pfitzmann, Ahmad-Reza Sadeghi</i>	
Efficient Anonymous Fingerprinting with Group Signatures . . . . .	415
<i>Jan Camenisch</i>	

## Zero-Knowledge and Provable Security

Increasing the Power of the Dealer in Non-interactive Zero-Knowledge Proof Systems . . . . .	429
<i>Danny Gutfreund, Michael Ben-Or</i>	
Zero-Knowledge and Code Obfuscation . . . . .	443
<i>Satoshi Hada</i>	
A Note on Security Proofs in the Generic Model . . . . .	458
<i>Marc Fischlin</i>	

## Boolean Functions

On Relationships among Avalanche, Nonlinearity, and Correlation Immunity . . . . .	470
<i>Yuliang Zheng, Xian-Mo Zhang</i>	

## Cryptanalysis II

Cryptanalysis of the Yi-Lam Hash .....	483
<i>David Wagner</i>	

Power Analysis, What Is Now Possible.....	489
<i>Mehdi-Laurent Akkar, Régis Bevan, Paul Dischamp, Didier Moyart</i>	

## Pseudorandomness

Concrete Security Characterizations of PRFs and PRPs: Reductions and Applications .....	503
<i>Anand Desai, Sara Miner</i>	

## Symmetric-Key Schemes II

The Security of Chaffing and Winnowing.....	517
<i>Mihir Bellare, Alexandra Boldyreva</i>	

Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm.....	531
<i>Mihir Bellare, Chanathip Namprempre</i>	

Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques.....	546
<i>Michel Abdalla, Mihir Bellare</i>	

Proofs of Security for the Unix Password Hashing Algorithm .....	560
<i>David Wagner, Ian Goldberg</i>	

## Public-Key Encryption and Key Distribution

Trapdooring Discrete Logarithms on Elliptic Curves over Rings .....	573
<i>Pascal Paillier</i>	

Strengthening McEliece Cryptosystem .....	585
<i>Pierre Loidreau</i>	

Password-Authenticated Key Exchange Based on RSA.....	599
<i>Philip MacKenzie, Sarvar Patel, Ram Swaminathan</i>	

Round-Efficient Conference Key Agreement Protocols with Provable Security .....	614
<i>Wen-Guey Tzeng, Zhi-Jia Tzeng</i>	

Author Index .....	629
--------------------	-----

Advances in Cryptology - ASIACRYPT 2000  
6th International Conference on the Theory and  
Application of Cryptology and Information Security,  
Kyoto, Japan, December 3-7, 2000 Proceedings  
Okamoto, T. (Ed.)  
2000, XII, 636 p., Softcover  
ISBN: 978-3-540-41404-9