

# Table of Contents

Analysis of Bernstein's Factorization Circuit . . . . .	1
<i>Arjen K. Lenstra, Adi Shamir, Jim Tomlinson, Eran Tromer</i>	
A Variant of the Cramer-Shoup Cryptosystem for Groups of Unknown Order . . . . .	27
<i>Stefan Lucks</i>	
Looking beyond XTR . . . . .	46
<i>Wieb Bosma, James Hutton, Eric R. Verheul</i>	
Bounds for Robust Metering Schemes and Their Relationship with $A^2$ -code . . . . .	64
<i>Wakaha Ogata, Kaoru Kurosawa</i>	
Unconditionally Secure Anonymous Encryption and Group Authentication . . . . .	81
<i>Goichiro Hanaoka, Junji Shikata, Yumiko Hanaoka, Hideki Imai</i>	
Adapting the Weaknesses of the Random Oracle Model to the Generic Group Model . . . . .	100
<i>Alexander W. Dent</i>	
On the Impossibilities of Basing One-Way Permutations on Central Cryptographic Primitives . . . . .	110
<i>Yan-Cheng Chang, Chun-Yun Hsiao, Chi-Jen Lu</i>	
A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order . . . . .	125
<i>Ivan Damgård, Eiichiro Fujisaki</i>	
Efficient Oblivious Transfer in the Bounded-Storage Model . . . . .	143
<i>Dowon Hong, Ku-Young Chang, Heuisu Ryu</i>	
In How Many Ways Can You Write Rijndael? . . . . .	160
<i>Elad Barkan, Eli Biham</i>	
On the Security of Rijndael-Like Structures against Differential and Linear Cryptanalysis . . . . .	176
<i>Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, Jongin Lim</i>	
Threshold Cryptosystems Based on Factoring . . . . .	192
<i>Jonathan Katz, Moti Yung</i>	

Non-interactive Distributed-Verifier Proofs and Proving Relations among Commitments . . . . .	206
<i>Masayuki Abe, Ronald Cramer, Serge Fehr</i>	
Asynchronous Secure Communication Tolerating Mixed Adversaries . . . . .	224
<i>K. Srinathan, M.V.N. Ashwin Kumar, C. Pandu Rangan</i>	
Amplified Boomerang Attack against Reduced-Round SHACAL . . . . .	243
<i>Jongsung Kim, Dukjae Moon, Wonil Lee, Seokhie Hong, Sangjin Lee, Seokwon Jung</i>	
Enhancing Differential-Linear Cryptanalysis . . . . .	254
<i>Eli Biham, Orr Dunkelman, Nathan Keller</i>	
Cryptanalysis of Block Ciphers with Overdefined Systems of Equations . . .	267
<i>Nicolas T. Courtois, Josef Pieprzyk</i>	
Analysis of Neural Cryptography . . . . .	288
<i>Alexander Klimov, Anton Mityagin, Adi Shamir</i>	
The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm . . . . .	299
<i>Dario Catalano, Phong Q. Nguyen, Jacques Stern</i>	
A Comparison and a Combination of SST and AGM Algorithms for Counting Points of Elliptic Curves in Characteristic 2 . . . . .	311
<i>Pierrick Gaudry</i>	
A General Formula of the $(t, n)$ -Threshold Visual Secret Sharing Scheme . .	328
<i>Hiroki Koga</i>	
On Unconditionally Secure Robust Distributed Key Distribution Centers . .	346
<i>Paolo D'Arco, Douglas R. Stinson</i>	
Short Signatures in the Random Oracle Model . . . . .	364
<i>Louis Granboulan</i>	
The Provable Security of Graph-Based One-Time Signatures and Extensions to Algebraic Signature Schemes . . . . .	379
<i>Alejandro Hevia, Daniele Micciancio</i>	
Transitive Signatures Based on Factoring and RSA . . . . .	397
<i>Mihir Bellare, Gregory Neven</i>	
1-out-of- $n$ Signatures from a Variety of Keys . . . . .	415
<i>Masayuki Abe, Miyako Ohkubo, Koutarou Suzuki</i>	
A Revocation Scheme with Minimal Storage at Receivers . . . . .	433
<i>Tomoyuki Asano</i>	

Optimistic Mixing for Exit-Polls .....	451
<i>Philippe Golle, Sheng Zhong, Dan Boneh, Markus Jakobsson, Ari Juels</i>	
Improved Construction of Nonlinear Resilient S-Boxes .....	466
<i>Kishan Chand Gupta, Palash Sarkar</i>	
An Upper Bound on the Number of $m$ -Resilient Boolean Functions.....	484
<i>Claude Carlet, Aline Gouget</i>	
Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks ..	497
<i>Emmanuel Bresson, Olivier Chevassut, David Pointcheval</i>	
Secure Channels Based on Authenticated Encryption Schemes:	
A Simple Characterization .....	515
<i>Chanathip Namprempre</i>	
ID-Based Blind Signature and Ring Signature from Pairings.....	533
<i>Fanguo Zhang, Kwangjo Kim</i>	
Hierarchical ID-Based Cryptography .....	548
<i>Craig Gentry, Alice Silverberg</i>	
Crypto-integrity .....	567
<i>Moti Yung</i>	
Gummy and Conductive Silicone Rubber Fingers .....	574
<i>Tsutomu Matsumoto</i>	
Author Index.....	577

<http://www.springer.com/978-3-540-00171-3>

Advances in Cryptology - ASIACRYPT 2002  
8th International Conference on the Theory and  
Application of Cryptology and Information Security,  
Queenstown, New Zealand, December 1-5, 2002,  
Proceedings  
Zheng, Y. (Ed.)  
2002, XIV, 582 p., Softcover  
ISBN: 978-3-540-00171-3