

Table of Contents

Cryptanalysis I

Cryptanalysis of a Pseudorandom Generator Based on Braid Groups	1
<i>Rosario Gennaro, Daniele Micciancio</i>	
Potential Weaknesses of the Commutator Key Agreement Protocol Based on Braid Groups	14
<i>Sang Jin Lee, Eonkyung Lee</i>	
Extending the GHS Weil Descent Attack	29
<i>Steven D. Galbraith, Florian Hess, Nigel P. Smart</i>	

Public-Key Encryption

Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption	45
<i>Ronald Cramer, Victor Shoup</i>	
Key-Insulated Public Key Cryptosystems	65
<i>Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, Moti Yung</i>	
On the Security of Joint Signature and Encryption	83
<i>Jee Hea An, Yevgeniy Dodis, Tal Rabin</i>	

Invited Talk

AES and the Wide Trail Design Strategy	108
<i>Joan Daemen, Vincent Rijmen</i>	

Information Theory & New Models

Indistinguishability of Random Systems	110
<i>Ueli Maurer</i>	
How to Fool an Unbounded Adversary with a Short Key	133
<i>Alexander Russell, Hong Wang</i>	
Cryptography in an Unbounded Computational Model	149
<i>David P. Woodruff, Marten van Dijk</i>	

Implementational Analysis

Performance Analysis and Parallel Implementation of Dedicated Hash Functions	165
<i>Junko Nakajima, Mitsuru Matsui</i>	
Fault Injection and a Timing Channel on an Analysis Technique	181
<i>John A. Clark, Jeremy L. Jacob</i>	
Speeding Up Point Multiplication on Hyperelliptic Curves with Efficiently-Computable Endomorphisms	197
<i>Young-Ho Park, Sangtae Jeong, Jongin Lim</i>	

Stream Ciphers

Fast Correlation Attacks: An Algorithmic Point of View	209
<i>Philippe Chose, Antoine Joux, Michel Mitton</i>	
BDD-Based Cryptanalysis of Keystream Generators	222
<i>Matthias Krause</i>	
Linear Cryptanalysis of Bluetooth Stream Cipher	238
<i>Jovan Dj. Golić, Vittorio Bagini, Guglielmo Morgari</i>	

Digital Signatures I

Generic Lower Bounds for Root Extraction and Signature Schemes in General Groups	256
<i>Ivan Damgård, Maciej Koprowski</i>	
Optimal Security Proofs for PSS and Other Signature Schemes	272
<i>Jean-Sébastien Coron</i>	

Cryptanalysis II

Cryptanalysis of SFLASH	288
<i>Henri Gilbert, Marine Minier</i>	
Cryptanalysis of the Revised NTRU Signature Scheme	299
<i>Craig Gentry, Mike Szydło</i>	

Key Exchange

Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions	321
<i>Emmanuel Bresson, Olivier Chevassut, David Pointcheval</i>	
Universally Composable Notions of Key Exchange and Secure Channels . . .	337
<i>Ran Canetti, Hugo Krawczyk</i>	
On Deniability in Quantum Key Exchange	352
<i>Donald Beaver</i>	

Modes of Operation

A Practice-Oriented Treatment of Pseudorandom Number Generators . . .	368
<i>Anand Desai, Alejandro Hevia, Yiqun Lisa Yin</i>	
A Block-Cipher Mode of Operation for Parallelizable Message Authentication	384
<i>John Black, Phillip Rogaway</i>	

Invited Talk

Rethinking PKI: What's Trust Got to Do with It?	398
<i>Stephen Kent</i>	

Digital Signatures II

Efficient Generic Forward-Secure Signatures with an Unbounded Number of Time Periods	400
<i>Tal Malkin, Daniele Micciancio, Sara Miner</i>	
From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security	418
<i>Michel Abdalla, Jee Hea An, Mihir Bellare, Chanathip Namprempre</i>	
Security Notions for Unconditionally Secure Signature Schemes	434
<i>Junji Shikata, Goichiro Hanaoka, Yuliang Zheng, Hideki Imai</i>	

Traitor Tracking & Id-Based Encryption

Traitor Tracing with Constant Transmission Rate	450
<i>Aggelos Kiayias, Moti Yung</i>	

Toward Hierarchical Identity-Based Encryption 466
Jeremy Horwitz, Ben Lynn

Multiparty and Multicast

Unconditional Byzantine Agreement and Multi-party Computation
Secure against Dishonest Minorities from Scratch 482
Matthias Fitzi, Nicolas Gisin, Ueli Maurer, Oliver von Rotz

Perfectly Secure Message Transmission Revisited 502
Yvo Desmedt, Yongge Wang

Symmetric Cryptology

Degree of Composition of Highly Nonlinear Functions
and Applications to Higher Order Differential Cryptanalysis 518
Anne Canteaut, Marion Videau

Security Flaws Induced by CBC Padding –
Applications to SSL, IPSEC, WTLS 534
Serge Vaudenay

Author Index 547

Advances in Cryptology - EUROCRYPT 2002
International Conference on the Theory and
Applications of Cryptographic Techniques, Amsterdam,
The Netherlands, April 28 - May 2, 2002 Proceedings
Knudsen, L. (Ed.)
2002, XII, 552 p., Softcover
ISBN: 978-3-540-43553-2