

Table of Contents

Public-Key Cryptanalysis I

On the Security of RSA Padding	1
<i>Jean-Sébastien Coron, David Naccache, Julien P. Stern</i>	
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization	19
<i>Aviad Kipnis, Adi Shamir</i>	
The Hardness of the Hidden Subset Sum Problem and Its Cryptographic Implications	31
<i>Phong Nguyen, Jacques Stern</i>	

Invited Lecture

Information-Theoretic Cryptography.....	47
<i>Ueli Maurer</i>	

Secure Communication and Computation

Information Theoretically Secure Communication in the Limited Storage Space Model	65
<i>Yonatan Aumann, Michael O. Rabin</i>	
The All-or-Nothing Nature of Two-Party Secure Computation	80
<i>Amos Beimel, Tal Malkin, Silvio Micali</i>	

Distributed Cryptography

Adaptive Security for Threshold Cryptosystems.....	98
<i>Ran Canetti, Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, Tal Rabin</i>	
Two Party RSA Key Generation	116
<i>Niv Gilboa</i>	
Robust Distributed Multiplication without Interaction	130
<i>Masayuki Abe</i>	

A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting 148
Berry Schoenmakers

Secret-Key Cryptography

Truncated Differentials and Skipjack 165
Lars R. Knudsen, M.J.B. Robshaw, David Wagner

Fast Correlation Attacks Based on Turbo Code Techniques 181
Thomas Johansson, Fredrik Jönsson

Highly Nonlinear Resilient Functions Optimizing Siegenthaler’s Inequality 198
Subhamoy Maitra, Palash Sarkar

Message Authentication Codes

UMAC: Fast and Secure Message Authentication 216
John Black, Shai Halevi, Hugo Krawczyk, Ted Krovetz, Phillip Rogaway

Square Hash: Fast Message Authentication via Optimized Universal Hash Functions 234
Mark Etzel, Sarvar Patel, Zufikar Ramzan

Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions..... 252
Jee Hea An, Mihir Bellare

Stateless Evaluation of Pseudorandom Functions: Security Beyond the Birthday Barrier..... 270
Mihir Bellare, Oded Goldreich, Hugo Krawczyk

Public-Key Cryptanalysis II

Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto ’97..... 288
Phong Nguyen

Weakness in Quaternion Signatures 305
Don Coppersmith

Cryptanalysis of “2R” Schemes..... 315
Ding-Feng Ye, Kwok-Yan Lam, Zong-Duo Dai

Factoring $N = p^r q$ for Large r	326
<i>Dan Boneh, Glenn Durfee, Nick Howgrave-Graham</i>	

Traitor Tracing

An Efficient Public Key Traitor Tracing Scheme.....	338
<i>Dan Boneh, Matthew Franklin</i>	
Dynamic Traitor Tracing	354
<i>Amos Fiat, Tamir Tassa</i>	
Efficient Methods for Integrating Traceability and Broadcast Encryption	372
<i>Eli Gafni, Jessica Staddon, Yiqun Lisa Yin</i>	

Differential Power Analysis

Differential Power Analysis	388
<i>Paul Kocher, Joshua Jaffe, Benjamin Jun</i>	
Towards Sound Approaches to Counteract Power-Analysis Attacks	398
<i>Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, Pankaj Rohatgi</i>	

Signature Schemes

Separability and Efficiency for Generic Group Signature Schemes	413
<i>Jan Camenisch, Markus Michels</i>	
A Forward-Secure Digital Signature Scheme	431
<i>Mihir Bellare, Sara K. Miner</i>	
Abuse-Free Optimistic Contract Signing	449
<i>Juan A. Garay, Markus Jakobsson, Philip MacKenzie</i>	

Zero Knowledge

Can Statistical Zero Knowledge Be Made Non-interactive? or On the Relationship of SZK and NISZK	467
<i>Oded Goldreich, Amit Sahai, Salil Vadhan</i>	
On Concurrent Zero-Knowledge with Pre-processing.....	485
<i>Giovanni Di Crescenzo, Rafail Ostrovsky</i>	

Asymmetric Encryption

On the Security Properties of OAEP as an All-or-Nothing Transform	503
<i>Victor Boyko</i>	
Non-malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization	519
<i>Mihir Bellare, Amit Sahai</i>	
Secure Integration of Asymmetric and Symmetric Encryption Schemes.....	537
<i>Eiichiro Fujisaki, Tatsuaki Okamoto</i>	

Electronic Cash

Auditable, Anonymous Electronic Cash	555
<i>Tomas Sander, Amnon Ta-Shma</i>	

Protocols and Broadcasting

Oblivious Transfer with Adaptive Queries	573
<i>Moni Naor, Benny Pinkas</i>	
Compressing Cryptographic Resources	591
<i>Niv Gilboa, Yuval Ishai</i>	
Coding Constructions for Blacklisting Problems without Computational Assumptions.....	609
<i>Ravi Kumar, Sridhar Rajagopalan, Amit Sahai</i>	
An Information Theoretic Analysis of Rooted-Tree Based Secure Multicast Key Distribution Schemes.....	624
<i>Radha Poovendran, John S. Baras</i>	

Author Index	639
---------------------------	-----



<http://www.springer.com/978-3-540-66347-8>

Advances in Cryptology - CRYPTO '99
19th Annual International Cryptology Conference, Santa
Barbara, California, USA, August 15-19, 1999
Proceedings
Wiener, M. (Ed.)
1999, XII, 648 p., Softcover
ISBN: 978-3-540-66347-8