

Contents

Hashing and Authentication I

Keying Hash Functions for Message Authentication	1
<i>Mihir Bellare, Ran Canetti, Hugo Krawczyk</i>	
Universal Hashing and Multiple Authentication	16
<i>M. Atici, Douglas R. Stinson</i>	
Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings	31
<i>Tor Helleseth, Thomas Johansson</i>	

New Systems

Asymmetric Cryptography with a Hidden Monomial	45
<i>Jacques Patarin</i>	
Anonymous Communication and Anonymous Cash	61
<i>Daniel R. Simon</i>	

Cryptanalysis I: Asymmetric Systems

Weaknesses in Some Threshold Cryptosystems	74
<i>Susan K. Langford</i>	
Hidden Collisions on DSS	83
<i>Serge Vaudenay</i>	
The Dark Side of 'Black-Box' Cryptography, or: Should We Trust Capstone?	89
<i>Adam Young, Moti Yung</i>	
Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems	104
<i>Paul C. Kocher</i>	

Hard Bits

All Bits in $ax + b \bmod p$ are Hard	114
<i>Mats Näslund</i>	
Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes	129
<i>Dan Boneh, Ramarathnam Venkatesan</i>	

Signatures

Security of 2^t -Root Identification and Signatures	143
<i>Claus P. Schnorr</i>	
Robust and Efficient Sharing of RSA Functions	157
<i>Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, Tal Rabin</i>	
New Generation of Secure and Practical RSA-Based Signatures	173
<i>Ronald Cramer, Ivan Damgård</i>	

Zero Knowledge

Proving Without Knowing: On Oblivious, Agnostic and Blindfolded Provers	186
<i>Markus Jakobsson, Moti Yung</i>	
Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing	201
<i>Shai Halevi, Silvio Micali</i>	

Cryptanalysis II: Symmetric Systems

Improved Differential Attacks on RC5	216
<i>Lars R. Knudsen, Willi Meier</i>	
Improving Implementable Meet-in-the-Middle Attacks by Orders of Magnitude	229
<i>Paul C. van Oorschot, Michael J. Wiener</i>	

More on Symmetric Systems

Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES	237
<i>John Kelsey, Bruce Schneier, David Wagner</i>	
How to Protect DES Against Exhaustive Key Search	252
<i>Joe Kilian, Phillip Rogaway</i>	

Diffie-Hellman Oracle

Diffie-Hellman Oracles	268
<i>Ueli M. Maurer, Stefan Wolf</i>	
Algorithms for Black-Box Fields and Their Application to Cryptography	283
<i>Dan Boneh, Richard J. Lipton</i>	

Hashing and Authentication II

Fast Hashing on the Pentium	298
<i>Antoon Bosselaers, René Govaerts, Joos Vandewalle</i>	
On Fast and Provably Secure Message Authentication Based on Universal Hashing	313
<i>Victor Shoup</i>	

Quantum Crypto

Quantum Cryptography over Underground Optical Fibers	329
<i>R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, C. Simmons</i>	
Quantum Key Distribution and String Oblivious Transfer in Noisy Channels	343
<i>Dominic Mayers</i>	

Stream Ciphers

Linear Complexity of Periodic Sequences: A General Theory	358
<i>James L. Massey, Shirlei Serconek</i>	
Generalization of Siegenthaler Inequality and Schnorr-Vaudenay Multipermutations	372
<i>Paul Camion, Anne Canteaut</i>	

Secret Sharing

Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution	387
<i>Carlo Blundo, Luiz A. Frota Mattos, Douglas R. Stinson</i>	
New Results on Visual Cryptography	401
<i>Stefan Droste</i>	
Author Index	417

<http://www.springer.com/978-3-540-61512-5>

Advances in Cryptology — CRYPTO '96
16th Annual International Cryptology Conference, Santa
Barbara, California, USA, August 18–22, 1996,
Proceedings
Koblitz, N. (Ed.)
1996, XII, 415 p., Softcover
ISBN: 978-3-540-61512-5