

Advances in Cryptology - CRYPTO 2002

22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002.
Proceedings

Bearbeitet von
Moti Young

1. Auflage 2002. Taschenbuch. xiv, 630 S. Paperback
ISBN 978 3 540 44050 5
Format (B x L): 15,5 x 23,3 cm
Gewicht: 1970 g

Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit,
Geschäftssoftware > Informations- und Kodierungstheorie

Zu Leseprobe

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text "beck-shop.de" in a bold, red, sans-serif font. Above the "i" in "shop" are three red dots of increasing size. Below the main text, the words "DIE FACHBUCHHANDLUNG" are written in a smaller, red, all-caps, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Table of Contents

Block Ciphers

Essential Algebraic Structure within the AES.....	1
<i>Sean Murphy and Matthew J.B. Robshaw</i>	
Blockwise-Adaptive Attackers: Revisiting the (In)Security of Some Provably Secure Encryption Modes: CBC, GEM, IACBC	17
<i>Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette</i>	
Tweakable Block Ciphers	31
<i>Moses Liskov, Ronald L. Rivest, and David Wagner</i>	

Multi-user Oriented Cryptosystems

The LSD Broadcast Encryption Scheme	47
<i>Dani Halevy and Adi Shamir</i>	
Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials	61
<i>Jan Camenisch and Anna Lysyanskaya</i>	

Foundations and Methodology

Provably Secure Steganography (Extended Abstract)	77
<i>Nicholas J. Hopper, John Langford, and Luis von Ahn</i>	
Flaws in Applying Proof Methodologies to Signature Schemes	93
<i>Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel P. Smart</i>	
Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case	111
<i>Jesper Buus Nielsen</i>	

Security of Practical Protocols

On the Security of RSA Encryption in TLS	127
<i>Jakob Jonsson and Burton S. Kaliski Jr.</i>	
Security Analysis of IKE's Signature-Based Key-Exchange Protocol	143
<i>Ran Canetti and Hugo Krawczyk</i>	
GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks	162
<i>Mihir Bellare and Adriana Palacio</i>	

Secure Multiparty Computation

On 2-Round Secure Multiparty Computation	178
<i>Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin</i>	

Private Computation – k -Connected versus 1-Connected Networks	194
<i>Markus Bläser, Andreas Jakob, Maciej Liśkiewicz, and Bodo Siebert</i>	

Public-Key Encryption

Analysis and Improvements of NTRU Encryption Paddings	210
<i>Phong Q. Nguyen and David Pointcheval</i>	

Universal Padding Schemes for RSA	226
<i>Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier</i>	

Cryptanalysis of Unbalanced RSA with Small CRT-Exponent	242
<i>Alexander May</i>	

Information Theory and Secret Sharing

Hyper-encryption against Space-Bounded Adversaries from On-Line Strong Extractors	257
<i>Chi-Jen Lu</i>	

Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups	272
<i>Ronald Cramer and Serge Fehr</i>	

Cipher Design and Analysis

A Generalized Birthday Problem (Extended Abstract)	288
<i>David Wagner</i>	

(Not So) Random Shuffles of RC4	304
<i>Ilya Mironov</i>	

Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV	320
<i>John Black, Phillip Rogaway, and Thomas Shrimpton</i>	

Elliptic Curves and Abelian Varieties

Supersingular Abelian Varieties in Cryptology	336
<i>Karl Rubin and Alice Silverberg</i>	

Efficient Algorithms for Pairing-Based Cryptosystems	354
<i>Paulo S.L.M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott</i>	

Computing Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2	369
<i>Frederik Vercauteren</i>	

Password-Based Authentication

Threshold Password-Authenticated Key Exchange (Extended Abstract) ...	385
<i>Philip MacKenzie, Thomas Shrimpton, and Markus Jakobsson</i>	

Distributed Cryptosystems

A Threshold Pseudorandom Function Construction and Its Applications ..	401
<i>Jesper Buus Nielsen</i>	
Efficient Computation Modulo a Shared Secret with Application to the Generation of Shared Safe-Prime Products	417
<i>Joy Algesheimer, Jan Camenisch, and Victor Shoup</i>	

Pseudorandomness and Applications

Hidden Number Problem with the Trace and Bit Security of XTR and LUC	433
<i>Wen-Ching W. Li, Mats Näslund, and Igor E. Shparlinski</i>	
Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security	449
<i>Ivan Damgård and Jesper Buus Nielsen</i>	

Variations on Signatures and Authentication

Threshold Ring Signatures and Applications to Ad-hoc Groups	465
<i>Emmanuel Bresson, Jacques Stern, and Michael Szydlo</i>	
Deniable Ring Authentication	481
<i>Moni Naor</i>	
SiBIR: Signer-Base Intrusion-Resilient Signatures	499
<i>Gene Itkis and Leonid Reyzin</i>	

Stream Ciphers and Boolean Functions

Cryptanalysis of Stream Ciphers with Linear Masking	515
<i>Don Coppersmith, Shai Halevi, and Charanjit Jutla</i>	
The Filter-Combiner Model for Memoryless Synchronous Stream Ciphers ..	533
<i>Palash Sarkar</i>	
A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction	549
<i>Claude Carlet</i>	

Commitment Schemes

Linear VSS and Distributed Commitments Based on Secret Sharing
and Pairwise Checks 565
Serge Fehr and Ueli Maurer

Perfect Hiding and Perfect Binding Universally Composable
Commitment Schemes with Constant Expansion Factor 581
Ivan Damgård and Jesper Buus Nielsen

Signature Schemes

Unique Signatures and Verifiable Random Functions
from the DH-DDH Separation 597
Anna Lysyanskaya

Security Proof for Partial-Domain Hash Signature Schemes 613
Jean-Sébastien Coron

Author Index 627