

Advances in Cryptology - CRYPTO '98

Bearbeitet von
Hugo Krawczyk

1. Auflage 1998. Taschenbuch. xii, 524 S. Paperback

ISBN 978 3 540 64892 5

Format (B x L): 15,5 x 23,3 cm

Gewicht: 1660 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

Chosen-Ciphertext Security

Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1	1
<i>Daniel Bleichenbacher</i>	
A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack	13
<i>Ronald Cramer, Victor Shoup</i>	
Relations Among Notions of Security for Public-Key Encryption Schemes .	26
<i>Mihir Bellare, Anand Desai, David Pointcheval, Phillip Rogaway</i>	

Invited Lecture

Cryptography and the Internet	46
<i>Steven M. Bellovin</i>	

Cryptanalysis of Hash Functions and Block Ciphers

Differential Collisions in SHA-0	56
<i>Florent Chabaud, Antoine Joux</i>	
From Differential Cryptanalysis to Ciphertext-Only Attacks	72
<i>Alex Biryukov, Eyal Kushilevitz</i>	

Distributed Cryptography

A Simplified Approach to Threshold and Proactive RSA	89
<i>Tal Rabin</i>	
New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications	105
<i>Dario Catalano, Rosario Gennaro</i>	
Trading Correctness for Privacy in Unconditional Multi-party Computation	121
<i>Matthias Fitzi, Martin Hirt, Ueli Maurer</i>	

Identification and Certification

Fast Digital Identity Revocation	137
<i>William Aiello, Sachin Lodha, Rafail Ostrovsky</i>	

Self-Delegation with Controlled Propagation – or – What If You Lose Your Laptop	153
<i>Oded Goldreich, Birgit Pfitzmann, Ronald L. Rivest</i>	

Identity Escrow	169
<i>Joe Kilian, Erez Petrank</i>	

Block Cipher Design and Analysis

Generalized Birthday Attacks on Unbalanced Feistel Networks	186
<i>Charanjit S. Jutla</i>	

Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES	200
<i>Takeshi Shimoyama, Toshinobu Kaneko</i>	

Cryptanalysis of Block Ciphers with Probabilistic Non-linear Relations of Low Degree	212
<i>Thomas Jakobsen</i>	

Algebraic Cryptanalysis

Cryptanalysis of the Ajtai-Dwork Cryptosystem	223
<i>Phong Nguyen, Jacques Stern</i>	

Cryptanalysis of the Chor-Rivest Cryptosystem	243
<i>Serge Vaudenay</i>	

Cryptanalysis of the Oil & Vinegar Signature Scheme.....	257
<i>Aviad Kipnis, Adi Shamir</i>	

Relations Among Cryptographic Primitives

From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs	267
<i>Moni Naor, Omer Reingold</i>	

Many-to-One Trapdoor Functions and their Relation to Public-Key Cryptosystems.....	283
<i>Mihir Bellare, Shai Halevi, Amit Sahai, Salil Vadhan</i>	

IACR Distinguished Lecture

Authentication, Enhanced Security and Error Correcting Codes.....	299
<i>Yonatan Aumann, Michael O. Rabin</i>	

Algebraic Schemes

An Efficient Discrete Log Pseudo Random Generator	304
<i>Sarvar Patel, Ganapathy S. Sundaram</i>	

Fast RSA-type Cryptosystem Modulo $p^k q$	318
<i>Tsuyoshi Takagi</i>	

An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm.....	327
<i>Neal Koblitz</i>	

Quantum Cryptography

Quantum Bit Commitment from a Physical Assumption	338
<i>Louis Salvail</i>	

Signatures, Random Functions and Ideal Ciphers

On Concrete Security Treatment of Signatures Derived from Identification	354
<i>Kazuo Ohta, Tatsuaki Okamoto</i>	

Building PRFs from PRPs	370
<i>Chris Hall, David Wagner, John Kelsey, Bruce Schneier</i>	

Security Amplification by Composition: The Case of Doubly-Iterated, Ideal Ciphers	390
<i>William Aiello, Mihir Bellare, Giovanni Di Crescenzo, Ramarathnam Venkatesan</i>	

Zero-Knowledge

On the Existence of 3-Round Zero-Knowledge Protocols	408
<i>Satoshi Hada, Toshiaki Tanaka</i>	

Zero-Knowledge Proofs for Finite Field Arithmetic, or: Can Zero-Knowledge Be for Free?	424
<i>Ronald Cramer, Ivan Damgård</i>	

Concurrent Zero-Knowledge: Reducing the Need for Timing Constraints ..	442
<i>Cynthia Dwork, Amit Sahai</i>	

Implementation

The Solution of McCurley's Discrete Log Challenge	458
<i>Damian Weber, Thomas Denny</i>	

Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms ..	472
<i>Daniel V. Bailey, Christof Paar</i>	

Rights Protection

Time-Stamping with Binary Linking Schemes.....	486
<i>Ahto Buldas, Peeter Laud, Helger Lipmaa, Jan Villemson</i>	

Threshold Traitor Tracing..... 502
 Moni Naor, Benny Pinkas

Author Index 519