

Topics in Cryptology - CT-RSA 2002

The Cryptographer's Track at the RSA Conference 2002, San Jose, CA, USA, February 18-22, 2002,
Proceedings

Bearbeitet von
Bart Preneel

1. Auflage 2002. Taschenbuch. X, 318 S. Paperback

ISBN 978 3 540 43224 1

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

Gewicht: 1020 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, 'DIE FACHBUCHHANDLUNG' is 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

Public Key Cryptography

On Hash Function Firewalls in Signature Schemes	1
<i>Burton S. Kaliski Jr.</i>	

Observability Analysis – Detecting When Improved Cryptosystems Fail . . .	17
<i>Marc Joye, Jean-Jacques Quisquater, Sung-Ming Yen, and Moti Yung</i>	

Efficient Hardware Implementations

Precise Bounds for Montgomery Modular Multiplication and Some Potentially Insecure RSA Moduli	30
<i>Colin D. Walter</i>	

Montgomery in Practice: How to Do It More Efficiently in Hardware	40
<i>Lejla Batina and Geeke Muurling</i>	

MIST: An Efficient, Randomized Exponentiation Algorithm for Resisting Power Analysis	53
<i>Colin D. Walter</i>	

An ASIC Implementation of the AES SBoxes	67
<i>Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger</i>	

Public Key Cryptography: Theory

On the Impossibility of Constructing Non-interactive Statistically-Secret Protocols from Any Trapdoor One-Way Function	79
<i>Marc Fischlin</i>	

The Representation Problem Based on Factoring	96
<i>Marc Fischlin and Roger Fischlin</i>	

Symmetric Ciphers

Ciphers with Arbitrary Finite Domains	114
<i>John Black and Phillip Rogaway</i>	

Known Plaintext Correlation Attack against RC5	131
<i>Atsuko Miyaji, Masao Nonaka, and Yoshinori Takii</i>	

E-Commerce and Applications

Micropayments Revisited	149
<i>Silvio Micali and Ronald L. Rivest</i>	

Proprietary Certificates	164
<i>Markus Jakobsson, Ari Juels, and Phong Q. Nguyen</i>	

Stateless-Recipient Certified E-Mail System Based on Verifiable Encryption	182
<i>Giuseppe Ateniese and Cristina Nita-Rotaru</i>	

Digital Signatures

RSA-Based Undeniable Signatures for General Moduli	200
<i>Steven D. Galbraith, Wenbo Mao, and Kenneth G. Paterson</i>	

Co-operatively Formed Group Signatures	218
<i>Greg Maitland and Colin Boyd</i>	

Transitive Signature Schemes	236
<i>Silvio Micali and Ronald L. Rivest</i>	

Homomorphic Signature Schemes	244
<i>Robert Johnson, David Molnar, Dawn Song, and David Wagner</i>	

Public Key Encryption

GEM: A <u>G</u> eneric Chosen-Ciphertext Secure <u>E</u> ncryption <u>M</u> ethod	263
<i>Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen</i>	

Securing “Encryption + Proof of Knowledge” in the Random Oracle Model	277
<i>Masayuki Abe</i>	

Discrete Logarithm

Nonuniform Polynomial Time Algorithm to Solve Decisional Diffie-Hellman Problem in Finite Fields under Conjecture	290
<i>Qi Cheng and Shigenori Uchiyama</i>	

Secure Key-Evolving Protocols for Discrete Logarithm Schemes	300
<i>Cheng-Fen Lu and Shiuh-Pyng Winston Shieh</i>	

Author Index	311
--------------------	-----