

Advances in Cryptology — ASIACRYPT 2001

7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001. Proceedings

Bearbeitet von
Colin Boyd

1. Auflage 2001. Taschenbuch. xi, 601 S. Paperback
ISBN 978 3 540 42987 6
Format (B x L): 15,5 x 23,5 cm
Gewicht: 960 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 varying sizes, arranged in a slight arc. 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

Lattice Based Cryptography

Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001	1
<i>Craig Gentry, Jakob Jonsson, Jacques Stern, Michael Szydlo</i>	
On the Insecurity of a Server-Aided RSA Protocol	21
<i>Phong Q. Nguyen, Igor E. Shparlinski</i>	
The Modular Inversion Hidden Number Problem	36
<i>Dan Boneh, Shai Halevi, Nick Howgrave-Graham</i>	

Human Identification

Secure Human Identification Protocols	52
<i>Nicholas J. Hopper, Manuel Blum</i>	

Invited Talk

Unbelievable Security (<i>Matching AES Security Using Public Key Systems</i>)	67
<i>Arjen K. Lenstra</i>	

Practical Public Key Cryptography

A Probable Prime Test with Very High Confidence for $n \equiv 1 \pmod{4}$	87
<i>Siguna Müller</i>	
Computation of Discrete Logarithms in $\mathbb{F}_{2^{607}}$	107
<i>Emmanuel Thomé</i>	
Speeding Up XTR	125
<i>Martijn Stam, Arjen K. Lenstra</i>	
An Efficient Implementation of Braid Groups	144
<i>Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, Jung Hee Cheon</i>	

Cryptography Based on Coding Theory

How to Achieve a McEliece-Based Digital Signature Scheme	157
<i>Nicolas T. Courtois, Matthieu Finiasz, Nicolas Sendrier</i>	
Efficient Traitor Tracing Algorithms Using List Decoding	175
<i>Alice Silverberg, Jessica Staddon, Judy L. Walker</i>	

Block Ciphers

- Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis 193
Makoto Sugita, Kazukuni Kobara, Hideki Imai
- Known-IV Attacks on Triple Modes of Operation of Block Ciphers 208
Deukjo Hong, Jaechul Sung, Seokhie Hong, Wonil Lee, Sangjin Lee, Jongin Lim, Okyeon Yi
- Generic Attacks on Feistel Schemes 222
Jacques Patarin
- A Compact Rijndael Hardware Architecture with S-Box Optimization 239
Akashi Satoh, Sumio Morioka, Kohji Takano, Seiji Munetoh

Provable Security

- Provable Security of KASUMI and 3GPP Encryption Mode f_8 255
Ju-Sung Kang, Sang-Uk Shin, Dowon Hong, Okyeon Yi
- Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices 272
Duncan S. Wong, Agnes H. Chan
- Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case 290
Emmanuel Bresson, Olivier Chevassut, David Pointcheval

Threshold Cryptography

- Fully Distributed Threshold RSA under Standard Assumptions 310
Pierre-Alain Fouque, Jacques Stern
- Adaptive Security in the Threshold Setting: From Cryptosystems to Signature Schemes 331
Anna Lysyanskaya, Chris Peikert
- Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks 351
Pierre-Alain Fouque, David Pointcheval

Two-Party Protocols

- Oblivious Polynomial Evaluation and Oblivious Neural Learning 369
Yan-Cheng Chang, Chi-Jen Lu
- Mutually Independent Commitments 385
Moses Liskov, Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Adam Smith

Zero Knowledge

Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank	402
<i>Nicolas T. Courtois</i>	
Responsive Round Complexity and Concurrent Zero-Knowledge	422
<i>Tzafir Cohen, Joe Kilian, Erez Petrank</i>	

Cryptographic Building Blocks

Practical Construction and Analysis of Pseudo-Randomness Primitives . . .	442
<i>Johan Håstad, Mats Näslund</i>	
Autocorrelation Coefficients and Correlation Immunity of Boolean Functions	460
<i>Yuriy Tarannikov, Peter Korolev, Anton Botev</i>	

Elliptic Curve Cryptography

An Extension of Kedlaya's Point-Counting Algorithm to Superelliptic Curves	480
<i>Pierrick Gaudry, Nicolas Gürel</i>	
Supersingular Curves in Cryptography	495
<i>Steven D. Galbraith</i>	
Short Signatures from the Weil Pairing	514
<i>Dan Boneh, Ben Lynn, Hovav Shacham</i>	
Self-Blindable Credential Certificates from the Weil Pairing	533
<i>Eric R. Verheul</i>	

Anonymity

How to Leak a Secret	552
<i>Ronald L. Rivest, Adi Shamir, Yael Tauman</i>	
Key-Privacy in Public-Key Encryption	566
<i>Mihir Bellare, Alexandra Boldyreva, Anand Desai, David Pointcheval</i>	
Provably Secure Fair Blind Signatures with Tight Revocation	583
<i>Masayuki Abe, Miyako Ohkubo</i>	
Author Index	603