Topics in Cryptology - CT-RSA 2001

The Cryptographer's Track at RSA Conference 2001 San Francisco, CA, USA, April 8-12, 2001
Proceedings

Bearbeitet von
David Naccache

1. Auflage 2001. Taschenbuch. XII, 480 S. Paperback
ISBN 978 3 540 41898 6
Format (B x L): 15,5 x 23,5 cm
Gewicht: 1510 g

Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit, Geschäftsoftware > Zeichen- und Zahlendarstellungen

Zu Leseprobe

schnell und portofrei erhältlich bei

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

## New Cryptosystems

Faster Generation of NICE-Schnorr-Type Signatures .......... 1  
*Detlef Hühnein (secunet Security Networks AG)*

New Key Agreement Protocols in Braid Group Cryptography .... 13  
*Iris Anshel (Arithmetica Inc.), Michael Anshel (City College of New York), Benji Fisher (Boston College), Dorian Goldfeld (Columbia University)*

## RSA

Improving SSL Handshake Performance via Batching ............. 28  
*Hovav Shacham (Stanford University), Dan Boneh (Stanford University)*

From Fixed-Length Messages to Arbitrary-Length Messages Practical RSA Signature Padding Schemes ......................... 44  
*Geneviève Arboit (McGill University), Jean-Marc Robert (Gemplus Card International)*

An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least Significant Bits ........................................... 52  
*Ron Steinfeld (Monash University), Yuliang Zheng (Monash University)*

## Symmetric Cryptography

On the Strength of Simply-Iterated Feistel Ciphers with Whitening Keys .......... 63  
*Paul Onions (Silicon Infusion Ltd.)*

Analysis of SHA-1 in Encryption Mode ............................. 70  
*Helena Handschuh (Gemplus Card International), Lars R. Knudsen (University of Bergen), Matthew J. Robshaw (ISG, Royal Holloway)*

Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays ........ 84  
*Kris Gaj (George Mason University), Paweł Chodowiec (George Mason University)*
Gambling and Lotteries

Fair e-Lotteries and e-Casinos ........................................ 100
Eyal Kushilevitz (Department of Computer Science, Technion),
Tal Rabin (IBM T.J. Watson Research Center)

Secure Mobile Gambling ............................................ 110
Markus Jakobsson (Bell Laboratories, Lucent Technologies),
David Pointcheval (ENS – CNRS), Adam Young (Lockheed Martin)

Reductions, Constructions and Security Proofs

Formal Security Proofs for a Signature Scheme with Partial Message
Recovery ................................................................. 126
Daniel R.L. Brown (Certicom Research), Don B. Johnson
(Certicom Research)

The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES ...... 143
Michel Abdalla (University of California, San Diego), Mihir Bellare
(University of California, San Diego), Phillip Rogaway (University of
California, Davis)

REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform . 159
Tatsuaki Okamoto (NTT Labs), David Pointcheval (ENS – CNRS)

Flaws and Attacks

Security Weaknesses in Bluetooth .................................... 176
Markus Jakobsson (Bell Laboratories, Lucent Technologies),
Susanne Wetzel (Bell Laboratories, Lucent Technologies)

Distinguishing Exponent Digits by Observing Modular Subtractions ...... 192
Colin D. Walter (Datacard platform\(^7\) seven, UMIST Manchester),
Susan Thompson (Datacard platform\(^7\) seven)

On the Power of Misbehaving Adversaries and Security Analysis of the
Original EPOC ......................................................... 208
Marc Joye (Gemplus Card International), Jean-Jacques Quisquater
(UCL Crypto Group), Moti Yung (CertCo)

Implementation

Modular Exponentiation on Fine-Grained FPGA ...................... 223
Alexander Tiountchik (National Academy of Sciences of Belarus),
Elena Trichina (PACT Informationstechnologie)
Scalable Algorithm for Montgomery Multiplication and Its Implementation on the Coarse-Grain Reconfigurable Chip .......................... 235
Elena Trichina (PACT Informationstechnologie), Alexander Tioumtchik (National Academy of Sciences of Belarus)

Software Implementation of the NIST Elliptic Curves Over Prime Fields .. 250
Michael Brown (University of Waterloo), Darrel Hankerson (Auburn University, Certicom Research), Julio López (University of Valle), Alfred Menezes (University of Waterloo, Certicom Research)

Multivariate Cryptography

The Security of Hidden Field Equations (HFE) ......................... 266
Nicolas T. Courtois (Université de Toulon et du Var)

QUARTZ, 128-Bit Long Digital Signatures ............................... 282
Jacques Patarin (Bull CP8), Nicolas Courtois (Bull CP8), Louis Goubin (Bull CP8)

FLASH, a Fast Multivariate Signature Algorithm ........................ 298
Jacques Patarin (Bull CP8), Nicolas Courtois (Bull CP8), Louis Goubin (Bull CP8)

Number Theoretic Problems

Analysis of the Weil Descent Attack of Gaudry, Hess and Smart .......... 308
Alfred Menezes (University of Waterloo, Certicom Research), Minghua Qu (Certicom Research)

Using Fewer Qubits in Shor’s Factorization Algorithm via Simultaneous Diophantine Approximation ................................. 319
Jean-Pierre Seifert (Infineon Technologies)

Passwords and Credentials

Relying Party Credentials Framework ...................................... 328
Amir Herzberg (NewGenPay Inc.), Yosi Mass (IBM Haifa Research Lab)

Password Authentication Using Multiple Servers .......................... 344
David P. Jablon (Integrity Sciences, Inc.)

More Efficient Password-Authenticated Key Exchange .................. 361
Philip MacKenzie (Bell Laboratories, Lucent Technologies)

Protocols I

Improved Boneh-Shaw Content Fingerprinting ............................ 378
Yacov Yacobi (Microsoft Research)
XII  Table of Contents

Efficient Asymmetric Public-Key Traitor Tracing without Trusted Agents . 392
  Yuji Watanabe (IIS, University of Tokyo), Goichiro Hanaoka
  (IIS, University of Tokyo), Hideki Imai (IIS, University of Tokyo)

Targeted Advertising ... And Privacy Too .................................. 408
  Ari Juels (RSA Laboratories)

Protocols II

Uncheatable Distributed Computations ................................. 425
  Philippe Golle (Stanford University), Ilya Mironov
  (Stanford University)

Forward-Secure Threshold Signature Schemes ..................... 441
  Michel Abdalla (University of California, San Diego), Sara Miner
  (University of California, San Diego), Chanathip Namprempre
  (University of California, San Diego)

A Cost-Effective Pay-Per-Multiplication Comparison Method for
Millionaires ............................................................... 457
  Marc Fischlin (Johann Wolfgang Goethe-Universität
  Frankfurt am Main)

Author Index ............................................................... 473