

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Birgit Pfitzmann (Ed.)

Advances in Cryptology – EUROCRYPT 2001

International Conference on the Theory
and Application of Cryptographic Techniques
Innsbruck, Austria, May 6-10, 2001
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Birgit Pfitzmann
Universität des Saarlandes, Fachrichtung Informatik
Postfach 15 11 50, 66041 Saarbrücken, Germany
E-mail: pfitzmann@cs.uni-sb.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6 - 10, 2001. Birgit Pfitzmann (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2045)
ISBN 3-540-42070-3

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743

ISBN 3-540-42070-3 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Steingraber Satztechnik GmbH, Heidelberg
Printed on acid-free paper SPIN: 10781446 06/3142 5 4 3 2 1 0

Preface

EUROCRYPT 2001, the 20th annual Eurocrypt conference, was sponsored by the IACR, the International Association for Cryptologic Research, see <http://www.iacr.org/>, this year in cooperation with the Austrian Computer Society (OCG). The General Chair, Reinhard Posch, was responsible for local organization, and registration was handled by the IACR Secretariat at the University of California, Santa Barbara.

In addition to the papers contained in these proceedings, we were pleased that the conference program also included a presentation by the 2001 IACR distinguished lecturer, Andrew Odlyzko, on “Economics and Cryptography” and an invited talk by Silvio Micali, “Zero Knowledge Has Come of Age.” Furthermore, there was the rump session for presentations of recent results and other (possibly satirical) topics of interest to the crypto community, which Jean-Jacques Quisquater kindly agreed to run.

The Program Committee received 155 submissions and selected 33 papers for presentation; one of them was withdrawn by the authors. The review process was therefore a delicate and challenging task for the committee members, and I wish to thank them for all the effort they spent on it. Each committee member was responsible for the review of at least 20 submissions, so each paper was carefully evaluated by at least three reviewers, and submissions with a program committee member as a (co-)author by at least six. Final decisions, after intensive web discussions, were taken at a one-day face-to-face program committee meeting. The selection was based on originality, quality, and relevance to cryptography. In most cases, the reviewers provided extensive comments to the authors. Subsequently, the authors made a substantial effort to take these comments into account. I was pleased to see that the field is continuing to flourish and believe that we were able to select a varied and high-quality program. I wish to thank all the authors who submitted papers, thus making such a choice possible, and those of accepted papers for their cooperation in the timely production of revised versions.

Many thanks also go to the additional colleagues who reviewed submissions in their area of expertise: Joy Algesheimer, Seigo Arita, Giuseppe Ateniese, Olivier Baudron, Charles Bennett, Dan Boneh, Annalisa De Bonis, Wieb Bosma, Marco Bucci, Ran Canetti, Anne Canteaut, Suresh Chari, Philippe Chose, Christophe Clavier, Scott Contini, Don Coppersmith, Jean-Sébastien Coron, Ronald Cramer, Nora Dabbous, Ivan Damgård, Giovanni Di Crescenzo, Markus Dichtl, Yevgeniy Dodis, Paul Dumais, Serge Fehr, Marc Fischlin, Roger Fischlin, Matthias Fitzi, Pierre-Alain Fouque, Jun Furukawa, Pierre Girard, Clemente Gladi, Daniel Gottesman, Clemens Holenstein, Rosario Gennaro, Nick Howgrave-Graham, James Hughes, Yuval Ishai, Markus Jakobsson, Eliane Jaulmes, Antoine Joux, Olaf Keller, Ki Hyoung Ko, Reto Kohlas, Takeshi Koshihara, Eyal Kushilevitz, Yehuda Lindell, Helger Lipmaa, Anna Lysyanskaya, Subhamoy

Maitra, Tal Malkin, Daniel Mall, Barbara Masucci, Dominic Mayers, Alfred Menezes, Renato Menicocci, Daniele Micciancio, Markus Michels, Miodrag Mihaljevic, Phong Nguyen, Svetla Nikova, Satoshi Obana, Kazuo Ohta, Pino Persiano, David Pointcheval, Bartosz Przydatek, Michael Quisquater, Omer Reingold, Leonid Reyzin, Jean-Marc Robert, Pankaj Rohatgi, Alon Rosen, Ludovic Rousseau, Daniel Simon, Nigel Smart, Adam Smith, Othmar Staffelbach, Martijn Stam, Michael Steiner, Katsuyuki Takashima, Alain Tapp, Christophe Tychmen, Shigenori Uchiyama, Frédéric Valette, Ramarathnam Venkatesan, Eric Verheul, Stefan Wolf, Akihiro Yamamura, Yuliang Zheng. I apologize for any inadvertent omissions.

The review process was greatly simplified by submission software written by Mihir Bellare and Chanathip Namprempré for Crypto 2000, and review software developed for EUROCRYPT 2000 by Bart Preneel, Wim Moreau, and Joris Claessens.

I am very grateful to André Adelsbach. Skillfully and patiently, he carried the main load of background work of the Program Chair, in particular in setting up the submission and review servers, providing technical help to the authors and committee members, and in the preparation of these proceedings. I would also like to thank Michael Steiner and Martin Wanke for technical support, Matthias Schunter for organizing the program committee meeting, and Mihir Bellare and Michael Waidner for advice.

March 2001

Birgit Pfitzmann

EUROCRYPT 2001

May 6 – 10, 2001, Innsbruck (Tyrol), Austria

Sponsored by the
International Association for Cryptologic Research (IACR)
in cooperation with the
Austrian Computer Society (OCG)

General Chair

Reinhard Posch, Institute for Applied Information Processing and
Communications (IAIK), Austria

Program Chair

Birgit Pfitzmann, Saarland University, Saarbrücken, Germany

Program Committee

Josh Benaloh	Microsoft Research, USA
Carlo Blundo	Università di Salerno, Italy
Jan Camenisch	IBM Zürich Research Laboratory, Switzerland
Matt Franklin	UC Davis, USA
Shai Halevi	IBM T. J. Watson Research Center, USA
Martin Hirt	ETH Zürich, Switzerland
Thomas Johansson	Lund University, Sweden
Neal Koblitz	Univ. of Washington, USA
Hugo Krawczyk	Technion, Israel
Kaoru Kurosawa	Tokyo Institute of Technology, Japan
Arjen Lenstra	Citicorp, USA
Willi Meier	Fachhochschule Aargau, Switzerland
David Naccache	Gemplus, France
Kaisa Nyberg	Nokia, Finland
Torben Pryds Pedersen	Cryptomathic, Denmark
Guillaume Poupard	DCSSI Crypto Lab, France
Tal Rabin	IBM T. J. Watson Research Center, USA
Vincent Rijmen	K. U. Leuven, Belgium
Amit Sahai	Princeton University, USA
Kazue Sako	NEC, Japan
Louis Salvail	BRICS, University of Århus, Denmark
Claus-Peter Schnorr	University of Frankfurt, Germany
David Wagner	UC Berkeley, USA
Michael Waidner	IBM Zürich Research Laboratory, Switzerland

Table of Contents

Elliptic Curves

A Memory Efficient Version of Satoh's Algorithm	1
<i>Frederik Vercauteren (K. U. Leuven, Belgium)</i>	
<i>Bart Preneel (K. U. Leuven, Belgium)</i>	
<i>Joos Vandewalle (K. U. Leuven, Belgium)</i>	
Finding Secure Curves with the Satoh-FGH Algorithm and an Early-Abort Strategy	14
<i>Mireille Fouquet (LIX, École polytechnique, France)</i>	
<i>Pierrick Gaudry (LIX, École polytechnique, France)</i>	
<i>Robert Harley (ArgoTech, France)</i>	
How Secure Are Elliptic Curves over Composite Extension Fields?	30
<i>Nigel P. Smart (University of Bristol, UK)</i>	

Commitments

Efficient and Non-interactive Non-malleable Commitment	40
<i>Giovanni Di Crescenzo (Telcordia Technologies Inc., USA)</i>	
<i>Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)</i>	
<i>Rafail Ostrovsky (Telcordia Technologies Inc., USA)</i>	
<i>Adam Smith (Massachusetts Institute of Technology, USA)</i>	
How to Convert the Flavor of a Quantum Bit Commitment	60
<i>Claude Crépeau (McGill University, Canada)</i>	
<i>Frédéric Légaré (Zero-Knowledge Systems Inc., Canada)</i>	
<i>Louis Salvail (BRICS, University of Århus, Denmark)</i>	

Anonymity

Cryptographic Counters and Applications to Electronic Voting	78
<i>Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)</i>	
<i>Steven Myers (University of Toronto, Canada)</i>	
<i>Rafail Ostrovsky (Telcordia Technologies Inc., USA)</i>	

An Efficient System for Non-transferable Anonymous Credentials
with Optional Anonymity Revocation 93
Jan Camenisch (IBM Zürich Research Laboratory, Switzerland)
Anna Lysyanskaya (Massachusetts Institute of Technology, USA)

Priced Oblivious Transfer: How to Sell Digital Goods 119
Bill Aiello (AT&T Labs – Research, USA)
Yuval Ishai (DIMACS and AT&T Labs – Research, USA)
Omer Reingold (AT&T Labs – Research, USA)

Signatures and Hash Functions

A Secure Three-Move Blind Signature Scheme
for Polynomially Many Signatures 136
Masayuki Abe (NTT Laboratories, Japan)

Practical Threshold RSA Signatures without a Trusted Dealer 152
Ivan Damgård (BRICS, University of Århus, Denmark)
Maciej Koprowski (BRICS, University of Århus, Denmark)

Hash Functions: From Merkle-Damgård to Shoup 166
Ilya Mironov (Stanford University, USA)

XTR and NTRU

Key Recovery and Message Attacks on NTRU-Composite 182
Craig Gentry (DoCoMo Communications Laboratories Inc., USA)

Evidence that XTR Is More Secure
than Supersingular Elliptic Curve Cryptosystems 195
Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)

NSS: An NTRU Lattice-Based Signature Scheme 211
Jeffrey Hoffstein (NTRU Cryptosystems Inc., USA)
Jill Pipher (NTRU Cryptosystems Inc., USA)
Joseph H. Silverman (NTRU Cryptosystems Inc., USA)

Assumptions

The Bit Security of Paillier’s Encryption Scheme and Its Applications 229
Dario Catalano (University of Catania, Italy)
Rosario Gennaro (IBM T. J. Watson Research Center, USA)
Nick Howgrave-Graham (IBM T. J. Watson Research Center, USA)

Assumptions Related to Discrete Logarithms:
Why Subtleties Make a Real Difference 244
Ahmad-Reza Sadeghi (Saarland University, Germany)
Michael Steiner (Saarland University, Germany)

Multiparty Protocols

On Adaptive vs. Non-adaptive Security of Multiparty Protocols	262
<i>Ran Canetti (IBM T. J. Watson Research Center, USA)</i>	
<i>Ivan Damgård (BRICS, University of Århus, Denmark)</i>	
<i>Stefan Dziembowski (BRICS, University of Århus, Denmark)</i>	
<i>Yuval Ishai (DIMACS and AT&T Labs – Research, USA)</i>	
<i>Tal Malkin (AT&T Labs – Research, USA)</i>	
Multiparty Computation from Threshold Homomorphic Encryption	280
<i>Ronald Cramer (BRICS, University of Århus, Denmark)</i>	
<i>Ivan Damgård (BRICS, University of Århus, Denmark)</i>	
<i>Jesper B. Nielsen (BRICS, University of Århus, Denmark)</i>	
On Perfect and Adaptive Security in Exposure-Resilient Cryptography	301
<i>Yevgeniy Dodis (University of New York, USA)</i>	
<i>Amit Sahai (Princeton University, USA)</i>	
<i>Adam Smith (Massachusetts Institute of Technology, USA)</i>	

Block Ciphers

Cryptanalysis of Reduced-Round MISTY	325
<i>Ulrich Kühn (Dresdner Bank AG, Germany)</i>	
The Rectangle Attack – Rectangling the Serpent	340
<i>Eli Biham (Technion, Israel)</i>	
<i>Orr Dunkelman (Technion, Israel)</i>	
<i>Nathan Keller (Technion, Israel)</i>	

Primitives

Efficient Amplification of the Security of Weak Pseudo-Random Function Generators	358
<i>Steven Myers (University of Toronto, Canada)</i>	
Min-round Resettable Zero-Knowledge in the Public-Key Model	373
<i>Silvio Micali (Massachusetts Institute of Technology, USA)</i>	
<i>Leonid Reyzin (Massachusetts Institute of Technology, USA)</i>	

Symmetric Ciphers

Structural Cryptanalysis of SASAS	394
<i>Alex Biryukov (The Weizmann Institute, Israel)</i>	
<i>Adi Shamir (The Weizmann Institute, Israel)</i>	
Hyper-bent Functions	406
<i>Amr M. Youssef (University of Waterloo, Canada)</i>	
<i>Guang Gong (University of Waterloo, Canada)</i>	

New Method for Upper Bounding
the Maximum Average Linear Hull Probability for SPNs 420
Liam Keliher (Queen's University at Kingston, Canada)
Henk Meijer (Queen's University at Kingston, Canada)
Stafford Tavares (Queen's University at Kingston, Canada)

Key Exchange and Multicast

Lower Bounds for Multicast Message Authentication 437
Dan Boneh (Stanford University, USA)
Glenn Durfee (Stanford University, USA)
Matt Franklin (University of California, USA)

Analysis of Key-Exchange Protocols
and Their Use for Building Secure Channels 453
Ran Canetti (IBM T. J. Watson Research Center, USA)
Hugo Krawczyk (Technion, Israel)

Efficient Password-Authenticated Key Exchange
Using Human-Memorable Passwords 475
Jonathan Katz (Telcordia Technologies Inc. and Columbia University, USA)
Rafail Ostrovsky (Telcordia Technologies Inc., USA)
Moti Yung (CertCo Inc., USA)

Authentication and Identification

Identification Protocols Secure against Reset Attacks 495
Mihir Bellare (University of California at San Diego, USA)
Marc Fischlin (University of Frankfurt, Germany)
Shafi Goldwasser (Massachusetts Institute of Technology, USA)
Silvio Micali (Massachusetts Institute of Technology, USA)

Does Encryption with Redundancy Provide Authenticity? 512
Jee Hea An (University of California at San Diego, USA)
Mihir Bellare (University of California at San Diego, USA)

Encryption Modes with Almost Free Message Integrity 529
Charanjit S. Jutla (IBM T. J. Watson Research Center, USA)

Author Index 545