

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board:

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Oscar Nierstrasz

University of Berne, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

Dortmund University, Germany

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California at Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Christian Cachin Jan Camenisch (Eds.)

Advances in Cryptology - EUROCRYPT 2004

International Conference on the Theory
and Applications of Cryptographic Techniques
Interlaken, Switzerland, May 2-6, 2004
Proceedings



Springer

Volume Editors

Christian Cachin

Jan Camenisch

IBM Zurich Research Laboratory

Säumerstrasse 4, CH-8803 Rüschlikon, Switzerland

E-mail: {cca,jca}@zurich.ibm.com

Library of Congress Control Number: Applied for

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

ISSN 0302-9743

ISBN 3-540-21935-8 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 to prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign

Printed on acid-free paper SPIN: 10999516 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of Eurocrypt 2004, the 23rd Annual Eurocrypt Conference. The conference was organized by members of the IBM Zurich Research Laboratory in cooperation with IACR, the International Association for Cryptologic Research.

The conference received a record number of 206 submissions, out of which the program committee selected 36 for presentation at the conference (three papers were withdrawn by the authors shortly after submission). These proceedings contain revised versions of the accepted papers. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

The conference program also featured two invited talks. The first one was the 2004 IACR Distinguished Lecture given by Whitfield Diffie. The second invited talk was by Ivan Damgård who presented “Paradigms for Multiparty Computation.” The traditional rump session with short informal talks on recent results was chaired by Arjen Lenstra.

The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed independently by at least three members of the program committee, and papers co-authored by a member of the program committee were reviewed by at least six (other) members. The individual reviewing phase was followed by profound and sometimes lively discussions about the papers, which contributed a lot to the quality of the final selection. Extensive comments were sent to the authors in most cases. At the end, the comments and electronic discussion notes filled more than 32,000 lines of text! We would like to thank the members of the program committee for their hard work over the course of several months; it was a pleasure for us to work with them and to benefit from their knowledge and insight. We are also very grateful to the external reviewers who contributed with their expertise to the selection process. Their work is highly appreciated.

The submission of all papers was done using the electronic submission software written by Chanathip Namprempre with modifications by Andre Adelsbach. During the review process, the program committee was mainly communicating using the Web-based review software developed by Bart Preneel, Wim Moreau, and Joris Claessens. We would like to thank Roger Zimmermann for his help with installing and running the software locally, and for solving many other problems, not the least of which was the assembly of these proceedings. The final decisions were made at a meeting in Rüschlikon at the IBM Zurich Research Laboratory. Helga Steimann helped us with the organization and also made sure there was enough coffee and food available so that we could concentrate on the papers and were not distracted by empty stomachs. Thanks a lot!

We are grateful to Endre Bangerter, Martin Hirt, Reto Strobl, and Roger Zimmermann for their help with the local arrangements of the conference.

Eurocrypt 2004 was supported by the IBM Zurich Research Laboratory, Crypto AG, Omnisec, MediaCrypt, HP, Microsoft Research, and Swiss International Air Lines.

Our most important thanks go to our families for bearing with us through this busy period, for their support, and for their love.

Last but not least, we thank all the authors from all over the world who submitted papers. It is due to them and their work that the conference took place.

February 2004

Christian Cachin and Jan Camenisch

EUROCRYPT 2004

May 2–6, 2004, Interlaken, Switzerland

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with the
IBM Zurich Research Laboratory, Switzerland

Program and General Chairs

Christian Cachin and Jan Camenisch
IBM Zurich Research Laboratory, Switzerland

Program Committee

Alex Biryukov	Katholieke Universiteit Leuven, Belgium
John Black	University of Colorado at Boulder, USA
Christian Cachin	IBM Zurich Research Laboratory, Switzerland
Jan Camenisch	IBM Zurich Research Laboratory, Switzerland
Jean-Sébastien Coron	Gemplus Card International, France
Claude Crépeau	McGill University, Canada
Ivan Damgård	Aarhus University, Denmark
Juan Garay	Bell Labs - Lucent Technologies, USA
Rosario Gennaro	IBM T.J. Watson Research Center, USA
Alain Hiltgen	UBS, Switzerland
Thomas Johansson	Lund University, Sweden
Antoine Joux	DCSSI Crypto Lab, France
Joe Kilian	NEC Laboratories America, USA
Arjen Lenstra	Citibank, USA & TU Eindhoven, The Netherlands
Yehuda Lindell	IBM T.J. Watson Research Center, USA
Anna Lysyanskaya	Brown University, USA
Daniele Micciancio	UC San Diego, USA
Omer Reingold	Weizmann Institute of Science, Israel
Vincent Rijmen	Cryptomathic and IAIK, Belgium
Phillip Rogaway	UC Davis, USA & Chiang Mai University, Thailand
Igor Shparlinski	Macquarie University, Australia
Edlyn Teske	University of Waterloo, Canada
Rebecca Wright	Stevens Institute of Technology, USA

External Reviewers

Adi Akavia	Jonathan Herzog	Roberto Oliveira
Joy Algesheimer	Florian Hess	Pascal Paillier
Jee Hea An	Alejandro Hevia	Adriana Palacio
Siddhartha Annapureddy	Jason Hinek	Kenneth Paterson
Giuseppe Ateniese	Susan Hohenberger	Souradyuti Paul
Endre Bangerter	Nicholas Hopper	Thomas Pedersen
Lejla Batina	Nick Howgrave-Graham	Chris Peikert
Amos Beimel	Jim Hughes	Erez Petrank
Mihir Bellare	Yuval Ishai	Birgit Pfitzmann
Siddika Berna Ors	Markus Jakobsson	Benny Pinkas
Simon Blackburn	Stas Jarecki	David Pointcheval
Carlo Blundo	Eliane Jaulmes	Jonathan Poritz
Alexandra Boldyreva	Fredrik Jönsson	John Proos
Dan Boneh	Marc Joye	Michael Quisquater
Colin Boyd	Yael Tauman Kalai	Tal Rabin
Xavier Boyen	Aggelos Kiayias	Zulfikar Ramzan
An Braeken	Neal Koblitz	Leonid Reyzin
Thomas Brochman	David Kohel	Pierre-Michel Ricordel
Ran Canetti	Yoshi Kohno	Alon Rosen
Scott Contini	Hugo Krawczyk	Amit Sahai
Don Coppersmith	Ted Krovetz	Louis Salvail
Nora Dabbous	Sébastien Kunz-Jacques	Palash Sarkar
Christophe De Cannière	John Langford	Jasper Scholten
Alex Dent	Joseph Lano	Hovav Shacham
Giovanni Di Crescenzo	Moses Liskov	Taizo Shirai
Christophe Doche	Benjamin Lynn	Thomas Shrimpton
Yevgeniy Dodis	Philip MacKenzie	Alice Silverberg
Patrik Ekdahl	Chip Martel	Adam Smith
Nelly Fazio	Alex May	Patrick Solè
Serge Fehr	Dominic Mayers	Jessica Staddon
Marc Fischlin	Ralph C. Merkle	Markus Stadler
Matthias Fitzi	Sara Miner	Martijn Stam
Scott Fluhrer	Ilya Mironov	Andreas Stein
Matt Franklin	Siguna Müller	Ron Steinfeld
Martin Gagne	Frédéric Muller	Reto Strobl
Steven Galbraith	Sean Murphy	Frédéric Valette
M. I. Gonzáles Vasco	Chanathip Namprempre	Bart Van Rompay
Jens Groth	Moni Naor	Luis von Ahn
Jaime Gutierrez	Mats Näslund	Shabsi Walfish
Stuart Haber	Phong Nguyen	Huaxiong Wang
Shai Halevi	Antonio Nicolosi	Bogdan Warinschi
Helena Handschuh	Svetla Nikova	John Watrous
Darrel Hankerson	Kobbi Nissim	Christopher Wolf
Danny Harnik	Luke O'Connor	Ke Yang

Table of Contents

Private Computation

Efficient Private Matching and Set Intersection	1
<i>Michael J. Freedman, Kobbi Nissim, and Benny Pinkas</i>	
Positive Results and Techniques for Obfuscation	20
<i>Benjamin Lynn, Manoj Prabhakaran, and Amit Sahai</i>	
Secure Computation of the k^{th} -Ranked Element	40
<i>Gagan Aggarwal, Nina Mishra, and Benny Pinkas</i>	

Signatures I

Short Signatures Without Random Oracles	56
<i>Dan Boneh and Xavier Boyen</i>	
Sequential Aggregate Signatures from Trapdoor Permutations	74
<i>Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham</i>	

Unconditional Security

On the Key-Uncertainty of Quantum Ciphers and the Computational Security of One-Way Quantum Transmission	91
<i>Ivan Damgård, Thomas Pedersen, and Louis Salvail</i>	
The Exact Price for Unconditionally Secure Asymmetric Cryptography ..	109
<i>Renato Renner and Stefan Wolf</i>	
On Generating the Initial Key in the Bounded-Storage Model	126
<i>Stefan Dziembowski and Ueli Maurer</i>	

Distributed Cryptography

Practical Large-Scale Distributed Key Generation	138
<i>John Canny and Stephen Sorkin</i>	
Optimal Communication Complexity of Generic Multicast Key Distribution	153
<i>Daniele Micciancio and Saurabh Panjwani</i>	

Foundations I

An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem	171
<i>Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio</i>	
Black-Box Composition Does Not Imply Adaptive Security	189
<i>Steven Myers</i>	

Identity-Based Encryption

Chosen-Ciphertext Security from Identity-Based Encryption	207
<i>Ran Canetti, Shai Halevi, and Jonathan Katz</i>	
Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles	223
<i>Dan Boneh and Xavier Boyen</i>	

Elliptic Curves

Construction of Secure Random Curves of Genus 2 over Prime Fields	239
<i>Pierrick Gaudry and Éric Schost</i>	
Projective Coordinates Leak	257
<i>David Naccache, Nigel P. Smart, and Jacques Stern</i>	

Signatures II

Security Proofs for Identity-Based Identification and Signature Schemes ..	268
<i>Mihir Bellare, Chanathip Namprempre, and Gregory Neven</i>	
Concurrent Signatures	287
<i>Liqun Chen, Caroline Kudla, and Kenneth G. Paterson</i>	
The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures	306
<i>Tal Malkin, Satoshi Obana, and Moti Yung</i>	

Public-Key Cryptography

Public-Key Steganography	323
<i>Luis von Ahn and Nicholas J. Hopper</i>	
Immunizing Encryption Schemes from Decryption Errors	342
<i>Cynthia Dwork, Moni Naor, and Omer Reingold</i>	
Secure Hashed Diffie-Hellman over Non-DDH Groups	361
<i>Rosario Gennaro, Hugo Krawczyk, and Tal Rabin</i>	

Foundations II

On Simulation-Sound Trapdoor Commitments	382
<i>Philip MacKenzie and Ke Yang</i>	

Hash Function Balance and Its Impact on Birthday Attacks	401
<i>Mihir Bellare and Tadayoshi Kohno</i>	

Multiparty Computation

Multi-party Computation with Hybrid Security	419
<i>Matthias Fitzi, Thomas Holenstein, and Jürg Wullschleger</i>	

On the Hardness of Information-Theoretic Multiparty Computation	439
<i>Yuval Ishai and Eyal Kushilevitz</i>	

Dining Cryptographers Revisited	456
<i>Philippe Golle and Ari Juels</i>	

Cryptanalysis

Algebraic Attacks and Decomposition of Boolean Functions	474
<i>Willi Meier, Enes Pasalic, and Claude Carlet</i>	

Finding Small Roots of Bivariate Integer Polynomial Equations Revisited	492
<i>Jean-Sébastien Coron</i>	

New Applications

Public Key Encryption with Keyword Search	506
<i>Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano</i>	

Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data	523
<i>Yevgeniy Dodis, Leonid Reyzin, and Adam Smith</i>	

Algorithms and Implementation

Merkle Tree Traversal in Log Space and Time	541
<i>Michael Szydlo</i>	

Can We Trust Cryptographic Software? Cryptographic Flaws in GNU Privacy Guard v1.2.3	555
<i>Phong Q. Nguyen</i>	

Anonymity

Traceable Signatures 571
Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung

Handcuffing Big Brother: an Abuse-Resilient Transaction Escrow
Scheme 590
Stanislaw Jarecki and Vitaly Shmatikov

Anonymous Identification in *Ad Hoc* Groups 609
*Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and
Victor Shoup*

Author Index 627