

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

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

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Ronald Cramer (Ed.)

Advances in Cryptology – EUROCRYPT 2005

24th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Aarhus, Denmark, May 22-26, 2005
Proceedings



Springer

Volume Editor

Ronald Cramer
CWI, Amsterdam
and Mathematical Institute, Leiden University
Kruislaan 413, P.O. Box 94079
1090GB Amsterdam, The Netherlands
E-mail: cramer@cw.nl, cramer@math.leidenuniv.nl

Library of Congress Control Number: 2005926095

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-10 3-540-25910-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-25910-7 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© International Association for Cryptologic Research 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11426639 06/3142 5 4 3 2 1 0

Table of Contents

Cryptanalysis I

Cryptanalysis of the Hash Functions MD4 and RIPEMD <i>Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, Xiuquan Yu</i>	1
How to Break MD5 and Other Hash Functions <i>Xiaoyun Wang, Hongbo Yu</i>	19
Collisions of SHA-0 and Reduced SHA-1 <i>Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, William Jalby</i>	36

Theory I

Reducing Complexity Assumptions for Statistically-Hiding Commitment <i>Iftach Haitner, Omer Horvitz, Jonathan Katz, Chiu-Yuen Koo, Ruggero Morselli, Ronen Shaltiel</i>	58
Smooth Projective Hashing and Two-Message Oblivious Transfer <i>Yael Tauman Kalai</i>	78
On Robust Combiners for Oblivious Transfer and Other Primitives <i>Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, Alon Rosen</i>	96

Encryption I

Efficient Identity-Based Encryption Without Random Oracles <i>Brent Waters</i>	114
Tag-KEM/DEM: A New Framework for Hybrid Encryption and a New Analysis of Kurosawa-Desmedt KEM <i>Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, Victor Shoup</i>	128

Signatures and Authentication

Secure Remote Authentication Using Biometric Data <i>Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, Adam Smith</i>	147
Stronger Security Bounds for Wegman-Carter-Shoup Authenticators <i>Daniel J. Bernstein</i>	164
3-Move Undeniable Signature Scheme <i>Kaoru Kurosawa, Swee-Huay Heng</i>	181
Group Signatures with Efficient Concurrent Join <i>Aggelos Kiayias, Moti Yung</i>	198

Algebra and Number Theory I

Floating-Point LLL Revisited <i>Phong Q. Nguyen, Damien Stehlé</i>	215
Practical Cryptography in High Dimensional Tori <i>Marten van Dijk, Robert Granger, Dan Page, Karl Rubin, Alice Silverberg, Martijn Stam, David Woodruff</i>	234
A Tool Kit for Finding Small Roots of Bivariate Polynomials over the Integers <i>Johannes Blömer, Alexander May</i>	251

Quantum Cryptography

Computational Indistinguishability Between Quantum States and Its Cryptographic Application <i>Akinori Kawachi, Takeshi Koshihara, Harumichi Nishimura, Tomoyuki Yamakami</i>	268
Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes <i>Claude Crépeau, Daniel Gottesman, Adam Smith</i>	285

Secure Protocols

Compact E-Cash <i>Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya</i>	302
---	-----

Cryptographic Asynchronous Multi-party Computation with Optimal Resilience <i>Martin Hirt, Jesper Buus Nielsen, Bartosz Przydatek</i>	322
--	-----

Algebra and Number Theory II

Differential Cryptanalysis for Multivariate Schemes <i>Pierre-Alain Fouque, Louis Granboulan, Jacques Stern</i>	341
A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem <i>Ludovic Perret</i>	354
Partial Key Exposure Attacks on RSA up to Full Size Exponents <i>Matthias Ernst, Ellen Jochemsz, Alexander May, Benne de Weger</i>	371
The RSA Group is Pseudo-Free <i>Daniele Micciancio</i>	387

Theory II

Universally Composable Password-Based Key Exchange <i>Ran Canetti, Shai Halevi, Jonathan Katz, Yehuda Lindell, Phil MacKenzie</i>	404
Mercurial Commitments with Applications to Zero-Knowledge Sets <i>Melissa Chase, Alexander Healy, Anna Lysyanskaya, Tal Malkin, Leonid Reyzin</i>	422

Encryption II

Hierarchical Identity Based Encryption with Constant Size Ciphertext <i>Dan Boneh, Xavier Boyen, Eu-Jin Goh</i>	440
Fuzzy Identity-Based Encryption <i>Amit Sahai, Brent Waters</i>	457

Cryptanalysis II

Second Preimages on n -Bit Hash Functions for Much Less than 2^n Work <i>John Kelsey, Bruce Schneier</i>	474
Predicting and Distinguishing Attacks on RC4 Keystream Generator <i>Itzik Mantin</i>	491

Related-Key Boomerang and Rectangle Attacks <i>Eli Biham, Orr Dunkelman, Nathan Keller</i>	507
On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions <i>John Black, Martin Cochran, Thomas Shrimpton</i>	526
Broadcast Encryption and Traitor Tracing	
Public Traceability in Traitor Tracing Schemes <i>Hervé Chabanne, Duong Hieu Phan, David Pointcheval</i>	542
One-Way Chain Based Broadcast Encryption Schemes <i>Nam-Su Jho, Jung Yeon Hwang, Jung Hee Cheon, Myung-Hwan Kim, Dong Hoon Lee, Eun Sun Yoo</i>	559
Author Index	575

Preface

These are the proceedings of the 24th Annual IACR Eurocrypt Conference. The conference was sponsored by the International Association for Cryptologic Research (IACR; see www.iacr.org), this year in cooperation with the Computer Science Department of the University of Aarhus, Denmark. As General Chair, Ivan Damgård was responsible for local organization.

The Eurocrypt 2005 Program Committee (PC) consisted of 30 internationally renowned experts. Their names and affiliations are listed on pages VII and VIII of these proceedings. By the November 15, 2004 submission deadline the PC had received a total of 190 submissions via the IACR Electronic Submission Server. The subsequent selection process was divided into two phases, as usual. In the review phase each submission was carefully scrutinized by at least three independent reviewers, and the review reports, often extensive, were committed to the IACR Web Review System. These were taken as the starting point for the PC-wide Web-based discussion phase. During this phase, additional reports were provided as needed, and the PC eventually had some 700 reports at its disposal. In addition, the discussions generated more than 850 messages, all posted in the system. During the entire PC phase, which started in August 2003 with my earliest invitations to PC members and which continued until March 2005, more than 1000 email messages were communicated. Moreover, the PC received much appreciated assistance from a large body of external reviewers. Their names are listed on page VIII of these proceedings.

The selection process for Eurocrypt 2005 was finalized by the end of January 2005 with a one-day PC meeting held in Amsterdam, The Netherlands. This meeting was attended by most of the PC members. The PC ultimately selected 33 papers for publication in these proceedings and presentation at the conference. After notification of acceptance the authors were provided with the review comments and were granted one month to prepare the final versions, which were due by February 28, 2005. These final versions were not subjected to further scrutiny by the PC and their authors bear full responsibility.

It was a great pleasure to work with this PC, and I thank all members for contributing so much of their scientific expertise, advice, opinions, preferences and devotion, and for their very hard work in the relatively short time frame that a PC has to operate in.

The Eurocrypt 2005 “Best Paper Award” was shared by Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen and Xiuyuan Yu for their paper “Cryptanalysis of the Hash Functions MD4 and RIPEMD” and by Xiaoyun Wang and Hongbo Yu for their paper “How to Break MD5 and Other Hash Functions.”

Besides the above-mentioned 33 regular presentations, the Eurocrypt 2005 scientific program featured two invited speakers: *René Schoof* (University of Rome, Italy), with a survey talk on algebraic geometry algorithms in cryptology,

in particular on point counting algorithms for algebraic varieties over finite fields, and *Joe Kilian* (Yanilos Labs, Princeton, USA), with a talk on “Confusion, Quagmire and Irrelevancy: an Optimist’s View of the Future of Cryptographic Research.”

Many others have, in one way or another, helped the PC, contributed to these proceedings or the Eurocrypt conference as such, thereby also serving the international cryptology community as a whole, directly or indirectly.

The Eurocrypt conference continues to attract many very high-quality submissions from all over the world; so many in fact that not all good papers could be selected. All authors who submitted their work for consideration by the PC are hereby acknowledged for their contributions.

CWI¹ in Amsterdam and the Mathematical Institute at Leiden University, my employers, are gratefully acknowledged for their support.

Eurocrypt 2004 PC Co-chairs Christian Cachin and Jan Camenisch (IBM Research), as well as Crypto 2004 PC Chair Matt Franklin (UC Davis), gave useful advice on a number of occasions. Also many thanks to Springer for its collaboration. Peter Landrock (Cryptomathic) is kindly acknowledged for agreeing to organize and chair the Eurocrypt 2005 rump session, a traditional, entertaining Tuesday evening session with brief research announcements and “any other business.”

Hats off to John Tromp (Quantum Computing and Advanced Systems Research Group, CWI), who reallocated, from the summer of 2004 until February 2005, substantial amounts of his precious research time to expertly manage the technical infrastructure for electronic submissions and Web review. The software was run on the network of CWI’s INS Department. I hereby acknowledge the support of INS head Martin Kersten and his system manager Matthijs Mourits. Also many thanks to Harry Buhrman and Paul Vitányi! Thomas Herlea from KU Leuven’s IACR submission server and webreview system development team offered prompt technical assistance to John whenever needed. Michael Smeding (Computer Support Team, CWI) provided prompt service to me and my group.

Serge Fehr of my Cryptology and Information Security Research Group at CWI was in charge of “General Affairs.” In particular, he assisted me during the very busy week following the submission deadline, organized the PC meeting in collaboration with Wilmy van Ojik (Conference Organization, CWI), helped the PC by logging the entire decision process during the meeting, and provided instrumental assistance when I edited this volume. Serge, thanks a lot!

Finally, I thank Ivan Damgård, Eurocrypt 2005 General Chair, for our very pleasant collaboration during the organization of Eurocrypt 2005, a memorable addition to our many joint scientific endeavors (and friendship!)

March 2005

Ronald Cramer

¹ CWI is the National Research Institute for Mathematics and Computer Science in The Netherlands.

EUROCRYPT 2005

May 22–26, 2005, Aarhus, Denmark

Sponsored by the
International Association for Cryptologic Research (IACR)
in cooperation with the
*Computer Science Department, Faculty of Science,
University of Aarhus, Denmark*

General Chair

Ivan Damgård, Department of Computer Science,
University of Aarhus, Denmark

Program Chair

Ronald Cramer, CWI, Amsterdam & Mathematical Institute,
Leiden University, The Netherlands

Program Committee

Michael Backes IBM Zürich Research Laboratory, Switzerland
Daniel Bleichenbacher Lucent Bell Labs, USA
Don Beaver Syntechnica, LLC, USA
Don Coppersmith IBM T. J. Watson Research Center, USA
Hans Dobbertin University of Bochum, Germany
Yevgeniy Dodis New York University, USA
Marc Fischlin ETH Zürich, Switzerland
Steven Galbraith Royal Holloway, University of London, UK
Shafi Goldwasser MIT, USA & Weizmann Institute of Science, Israel
Shai Halevi IBM T. J. Watson Research Center, USA
Johan Håstad Royal Institute of Technology, UK
Marc Joye Gemplus, France
Aggelos Kiayias University of Connecticut, USA
Eyal Kushilevitz Technion, Israel
Arjen Lenstra Lucent Bell Labs, USA & TU Eindhoven, The Netherlands
Phong Q. Nguyễn CNRS & École Normale Supérieure, France
Kaisa Nyberg Nokia, Finland
Tatsuaki Okamoto NTT, Japan
Rafail Ostrovsky U.C.L.A., USA
Carles Padró Universitat Politècnica de Catalunya, Spain
Benny Pinkas Hewlett-Packard Labs, Israel
..... *(continued on the next page)*.....

Bart Preneel	Katholieke Universiteit Leuven, Belgium
Louis Salvail	University of Aarhus, Denmark
Palash Sarkar	Indian Statistical Institute, India
Berry Schoenmakers	TU Eindhoven, The Netherlands
Igor Shparlinski	Macquarie University, Australia
Douglas Stinson	University of Waterloo, Canada
Salil Vadhan	Harvard University, USA
Moti Yung	Columbia University, USA

External Referees

Michel Abdalla	Matt Franklin	Noboru Kunihiro
Masayuki Abe	Michael H. Freedman	Jeff Lagarias
Saurabh Aggarwal	Atsushi Fujioka	Tanja Lange
Roberto Avanzi	David Galindo	Joseph Lano
Joonsang Baek	Juan Garay	Kristin Lauter
Paulo Barreto	Rosario Gennaro	Yehuda Lindell
Amos Beimel	Guang Gong	Helger Lipmaa
Eli Biham	Maribel González Vasco	Moses Liskov
Alex Biryukov	Ignacio Gracia	Phil MacKenzie
Alexandra Boldyreva	Louis Granboulan	Subhamoy Maitra
Emmanuel Bresson	Stuart Haber	Tal Malkin
Éric Brier	Helena Handschuh	John Malone-Lee
Christian Cachin	Alex Healy	Stefan Mangard
Jan Camenisch	Javier Herranz	Keith Martin
Ran Canetti	Florian Hess	Alexander May
Christophe De Cannière	Jason Hinek	Mira Meyerovich
Dario Catalano	Martin Hirt	Silvio Micali
Debrup Chakraborty	Susan Hohenberger	Anton Mityagin
Yan-Cheng Chang	Thomas Holenstein	Paz Morillo
Denis Charles	Nick Howgrave-Graham	Siguna Mueller
Sanjit Chatterjee	Yuval Ishai	Sourav Mukhopadhyay
Benoît Chevallier-Mames	Markus Jakobsson	Enric Nart
Olivier Chevassut	Stanislaw Jarecki	Kenny Nguyen
Scott Contini	Antoine Joux	Minh-Huyen Nguyen
Giovanni Di Crescenzo	Ari Juels	Antonio Nicolosi
Ivan Damgård	Jonathan Katz	Jesper Nielsen
Drew Dean	Alexander Kholosha	Kobbi Nissim
Jean-François Dhem	Eike Kiltz	Satoshi Obana
Iwan Duursma	Tetsutaro Kobayashi	Miyako Ohkubo
Stefan Dziembowski	Tadayoshi Kohno	Kazuo Ohta
Kirsten Eisentraeger	Yuichi Komano	Elisabeth Oswald
Nelly Fazio	Hugo Krawczyk	Pascal Paillier
Matthias Fitzi	Gunnar Kreitz	Rafael Pass
Pierre-Alain Fouque	Caroline Kudla	Kenny Paterson

Maura Paterson	Werner Schindler	Shigenori Uchiyama
Souradyuti Paul	Mike Scott	Vinod Vaikuntanathan
Thomas Pedersen	Hovav Shacham	Ingrid Verbauwhede
Jan Pelzl	Ronen Shaltiel	Frederik Vercauteren
Giuseppe Persiano	Peter Shor	Eric Verheul
Erez Petrank	Victor Shoup	Jorge Luis Villar
Birgit Pfitzmann	Tom Shrimpton	Michael Waidner
Duong Hieu Phan	Alice Silverberg	Shabsi Walfish
Krzysztof Pietrzak	Nigel Smart	Huaxiong Wang
David Pointcheval	Martijn Stam	Xiaoyun Wang
Manoj Prabhakaran	François-Xavier Standaert	Mark Watkins
Bartosz Przydatek	Allan Steel	Benne de Weger
Jordi Pujolàs	Damien Stehlé	Steve Weis
Tal Rabin	Ron Steinfeld	Annegret Weng
Omer Reingold	Koutarou Suzuki	Mike Wiener
Rennato Renner	Mike Szydło	Douglas Wikström
Leonid Reyzin	Keisuke Tanaka	Christopher Wolf
Vincent Rijmen	Tamir Tassa	Stefan Wolf
Pankaj Rohatgi	Yael Tauman	Go Yamamoto
Alon Rosen	Isamu Teranishi	Aleksandr Yampolskiy
Germán Sáez	Edlyn Teske	Yuliang Zheng
Kazuo Sako	Mårten Trolin	Hong-Sheng Zhou
Takakazu Satoh	Yiannis Tsiounis	
Christian Schaffner	Pim Tuyls	