

*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

*University of California, Los Angeles, CA, 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*

Serge Vaudenay (Ed.)

# Advances in Cryptology – EUROCRYPT 2006

24th Annual International Conference on the Theory  
and Applications of Cryptographic Techniques  
St. Petersburg, Russia, May 28 – June 1, 2006  
Proceedings

Volume Editor

Serge Vaudenay  
EPFL, I&C, LASEC, Station 14  
INF Building, 1015 Lausanne, Switzerland  
E-mail: serge.vaudenay@epfl.ch

Library of Congress Control Number: 2006925895

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-34546-9 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-34546-6 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  
springer.com

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 11761679      06/3142      5 4 3 2 1 0

*The original version of the book was revised:  
The copyright line was incorrect. The Erratum  
to the book is available at  
DOI: [10.1007/978-3-540-34547-3\\_36](https://doi.org/10.1007/978-3-540-34547-3_36)*

# Preface

The 2006 edition of the Eurocrypt conference was held in St. Petersburg, Russia from May 28 to June 1, 2006. It was the 25th Eurocrypt conference. Eurocrypt is sponsored by the International Association for Cryptologic Research (IACR). Eurocrypt 2006 was chaired by Anatoly Lebedev, and I had the privilege to chair the Program Committee.

Eurocrypt collected 198 submissions on November 21, 2005. The Program Committee carried out a thorough review process. In total, 863 review reports were written by renowned experts, Program Committee members as well as external referees. Online discussions led to 1,114 additional discussion messages and about 1,000 emails. The review process was run using e-mail and the iChair software by Thomas Baignères and Matthieu Finiasz. Every submitted paper received at least three review reports. The Program Committee had a meeting in Lausanne on February 4, 2006. We selected 33 papers, notified acceptance or rejection to the authors, and had a cheese fondue. Authors were then invited to revise their submission. The present proceedings include all the revised papers. Due to time constraints the revised versions could not be reviewed again.

We delivered a “Eurocrypt Best Paper Award.” The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in the cryptographic research fields. Committee members were invited to nominate papers for this award. A poll then yielded a clear majority. This year, we were pleased to deliver the Eurocrypt Best Paper Award to Phong Q. Nguyen and Oded Regev for their brilliant paper “Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures.”

The Program Committee invited two speakers: David Naccache and Kevin McCurley. The current proceedings include papers about their presentation.

I would like to thank Anatoly Lebedev for organizing the conference. I would like to thank the IACR Board for honoring me by asking me to chair the Program Committee. The Program Committee and external reviewers worked extremely hard. I deeply thank them for this volunteer work. Acknowledgments also go to the authors of submitted papers, the speakers, and the invited speakers. I am grateful to Thomas Baignères and Matthieu Finiasz for their hard work developing the iChair software and constantly adding features. I also thank Shai Halevi and Amr Youssef, who participated in the software testing. Finally, I heartily thank Christine and Emilien, my family, for letting me spend some time on Eurocrypt.

This year, we celebrated the 30th anniversary of the publication of the Diffie-Hellman seminal paper “New Directions in Cryptography.” As cryptography was becoming a new academic research area, this pioneer paper invented public-key cryptography. My wish is that research in cryptography will lead us to 30 more years of fun.

March 2006

Serge Vaudenay  
Lausanne

# Eurocrypt 06

May 28–June 1, 2006, Saint Petersburg, Russia

## General Chair

Anatoly Lebedev, LAN Crypto  
Moscow, Russia

## Program Chair

Serge Vaudenay, EPFL  
Lausanne, Switzerland

## Program Committee

Feng Bao	Institute for Infocomm Research
Eli Biham	Technion
Alex Biryukov	Katholieke Universiteit Leuven
Alexandra Boldyreva	Georgia Institute of Technology
Colin Boyd	Queensland University of Technology
Jean-Sébastien Coron	University of Luxembourg
Yevgeniy Dodis	New York University
Matt Franklin	University of California Davis
Eiichiro Fujisaki	NTT Laboratories
Juan Garay	Bell Labs — Lucent Technologies
Martin Hirt	ETH Zurich
Tetsu Iwata	Ibaraki University
Pil Joong Lee	Pohang University of Science and Technology
Antoine Joux	DGA and University of Versailles
Jonathan Katz	University of Maryland
Arjen Lenstra	Bell Labs – Lucent Technologies and Technische Universiteit Eindhoven
Helger Lipmaa	Cybernetica AS and University of Tartu
Javier Lopez	University of Malaga
Stefan Lucks	University of Mannheim
Philip MacKenzie	DoCoMo USA Labs
Mitsuru Matsui	Mitsubishi Electric
Alexander May	University of Paderborn
Willi Meier	FH Aargau
Atsuko Miyaji	JAIST
Kaisa Nyberg	Helsinki University of Technology and Nokia
Kenny Paterson	Royal Holloway University of London
Greg Rose	Qualcomm
Berry Schoenmakers	Technische Universiteit Eindhoven
Serge Vaudenay (Chair)	EPFL
Michael Wiener	Cryptographic Clarity
Robert Zuccherato	Entrust, Inc.

## External Reviewers

Michel Abdalla	Nelly Fazio	Caroline Kudla
Masayuki Abe	Serge Fehr	Ulrich Kühn
Carlisle Adams	Matthieu Finiasz	Simon Künzli
Luis von Ahn	Marc Fischlin	Kaoru Kurosawa
Koichiro Akiyama	Matthias Fitzi	Tanja Lange
Elena Andreeva	Pierre-Alain Fouque	Joseph Lano
Kazumaro Aoki	Felix Freiling	Peeter Laud
Seigo Arita	Jun Furukawa	Sven Laur
Frederik Armknecht	Soichi Furuya	Jung Wook Lee
Tomoyuki Asano	Martin Gagne	Reynald Lercier
Gildas Avoine	Steven Galbraith	Christina Lindenberg
Thomas Baignères	David Galindo	Moses Liskov
Elad Barkan	Ran Gelles	Yi Lu
Don Beaver	Mark Gondree	Christoph Ludwig
Zuzana Beerliová	Daniel Gottesman	Anna Lysyanskaya
Mihir Bellare	Louis Goubin	Greg Maitland
Vicente Benjumea	Ignacio Gracia	John Malone-Lee
Dan Bernstein	Safuat Hamdy	Keith Martin
John Black	Goichiro Hanaoka	Sebastiá Martín
Daniel Bleichenbacher	Phil Hawkes	Natsume Matsuzaki
Johannes Blömer	Ryotaro Hayashi	Lorenz Minder
Jean Christian Boileau	Javier Herranz	Serge Mister
Xavier Boyen	Florian Hess	Payman Mohassel
Harry Buhrman	Shoichi Hirose	Jean Monnerat
Jan Camenisch	Dennis Hofheinz	Paz Morillo
Ran Canetti	Thomas Holenstein	Tim Moses
Juyoung Cha	Nick Howgrave-Graham	Siguna Mueller
Liquan Chen	Yong Ho Hwang	Frederic Muller
Rafi Chen	Yuval Ishai	Sean Murphy
Kookrae Cho	Stanislaw Jarecki	Toru Nakanishi
Sherman Chow	Jorge Jiménez	Deholo Nali
Carlos Cid	Ellen Jochemsz	Anderson Nascimento
Scott Contini	Pascal Junod	Gregory Neven
Yang Cui	Senny Kamara	Phong Nguyen
Reza Curtmola	Akinori Kawachi	Antonio Nicolosi
Ivan Damgård	John Kelsey	Jesper Nielsen
Vanessa Daza	Aggelos Kiayias	Wakaha Ogata
Alex Dent	Joe Killian	Kazuo Ohta
Claus Diem	Mehmet Kiraz	Koji Okada
Yan Zong Ding	Kazukuni Kobara	Takeshi Okamoto
Martin Döring	Vladimir Kolesnikov	Tatsuaki Okamoto
Orr Dunkelman	Chiu-Yuen Koo	Rafail Ostrovsky
Stefan Dziembowski	Matthias Krause	Raphael Overbeck
Daniela Engelbert	Volker Krummel	Michael Paddon

Carles Padro	Jong Hoon Shin	Frederik Vercauteren
Adriana Palacio	Tom Shrimpton	Jorge L. Villar
Saurabh Panjwani	Andrey Sidorenko	Ulrich Vollmer
Jung Hyung Park	Johan Sjödin	Martin Vuagnoux
Sylvain Pasini	Nigel Smart	Shabsi Walfish
Kun Peng	Adam Smith	Johan Wallén
Rene Peralta	Clayton Smith	Guilin Wang
Adrian Perrig	Miguel Soriano	Yongge Wang
Giuseppe Persiano	Masakazu Soshi	Bogdan Warinschi
Krzysztof Pietrzak	Martijn Stam	Benne de Weger
Benny Pinkas	Heiko Stamer	Ralf-Philipp Weinmann
Bart Preneel	Dirk Stegemann	William Whyte
Bartosz Przydatek	Ron Steinfeld	Christopher Wolf
Prashant Puniya	Daisuke Suzuki	Stefan Wolf
Carla Rafols	Koutarou Suzuki	Yongdong Wu
Dominik Raub	Mitsuru Tada	Jürg Wullschleger
Omer Reingold	Katsuyuki Takashima	Alex Yampolskiy
German Saez	Keisuke Tanaka	Ke Yang
Yasuyuki Sakai	Lauri Tarkkala	Yeon Hyeong Yang
Bagus Santoso	Tamir Tassa	Yiqun Lisa Yin
Hovav Schaham	Isamu Teranishi	Shoko Yonezawa
Daniel Schepers	Stefano Tessaro	Dae Hyun Yum
Katja Schmidt-Samoa	Toyohiro Tsurumaru	Yunlei Zhao
Jasper Scholten	Pim Tuyls	Huafei Zhu
Jae Woo Seo	Shigenori Uchiyama	
Ji Sun Shin	Maribel Vasco	



# Table of Contents

## Cryptanalysis

Security Analysis of the Strong Diffie-Hellman Problem <i>Jung Hee Cheon</i> .....	1
Cryptography in Theory and Practice: The Case of Encryption in IPsec <i>Kenneth G. Paterson, Arnold K.L. Yau</i> .....	12
Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects <i>Jean-Charles Faugère, Ludovic Perret</i> .....	30

## Invited Talk I

Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt <i>Vanessa Gratzner, David Naccache</i> .....	48
--	----

## Cryptography Meets Humans

Hiding Secret Points Amidst Chaff <i>Ye-Chien Chang, Qiming Li</i> .....	59
Parallel and Concurrent Security of the HB and HB <sup>+</sup> Protocols <i>Jonathan Katz, Ji Sun Shin</i> .....	73
Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol <i>Tal Moran, Moni Naor</i> .....	88

## Stream Ciphers

QUAD: A Practical Stream Cipher with Provable Security <i>Côme Berbain, Henri Gilbert, Jacques Patarin</i> .....	109
How to Strengthen Pseudo-random Generators by Using Compression <i>Aline Gouget, Hervé Sibert</i> .....	129

Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks <i>Frederik Armknecht, Claude Carlet, Philippe Gaborit, Simon Künzli, Willi Meier, Olivier Ruatta</i> .....	147
---	-----

## Hash Functions

VSH, an Efficient and Provable Collision-Resistant Hash Function <i>Scott Contini, Arjen K. Lenstra, Ron Steinfeld</i> .....	165
Herding Hash Functions and the Nostradamus Attack <i>John Kelsey, Tadayoshi Kohno</i> .....	183

## Oblivious Transfer

Optimal Reductions Between Oblivious Transfers Using Interactive Hashing <i>Claude Crépeau, George Savvides</i> .....	201
Oblivious Transfer Is Symmetric <i>Stefan Wolf, Jürg Wullschlegler</i> .....	222

## Numbers and Lattices

Symplectic Lattice Reduction and NTRU <i>Nicolas Gama, Nick Howgrave-Graham, Phong Q. Nguyen</i> .....	233
The Function Field Sieve in the Medium Prime Case <i>Antoine Joux, Reynald Lercier</i> .....	254
Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures <i>Phong Q. Nguyen, Oded Regev</i> .....	271

## Foundations

The Cramer-Shoup Encryption Scheme Is Plaintext Aware in the Standard Model <i>Alexander W. Dent</i> .....	289
Private Circuits II: Keeping Secrets in Tamperable Circuits <i>Yuval Ishai, Manoj Prabhakaran, Amit Sahai, David Wagner</i> .....	308

Composition Implies Adaptive Security in Minicrypt <i>Krzysztof Pietrzak</i> .....	328
---	-----

Perfect Non-interactive Zero Knowledge for NP <i>Jens Groth, Rafail Ostrovsky, Amit Sahai</i> .....	339
--	-----

## Invited Talk II

Language Modeling and Encryption on Packet Switched Networks <i>Kevin S. McCurley</i> .....	359
--	-----

## Block Ciphers

A Provable-Security Treatment of the Key-Wrap Problem <i>Phillip Rogaway, Thomas Shrimpton</i> .....	373
---	-----

Luby-Rackoff Ciphers from Weak Round Functions? <i>Ueli Maurer, Yvonne Anne Oswald, Krzysztof Pietrzak, Johan Sjödin</i> .....	391
---	-----

The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs <i>Mihir Bellare, Phillip Rogaway</i> .....	409
--	-----

## Cryptography Without Random Oracles

Compact Group Signatures Without Random Oracles <i>Xavier Boyen, Brent Waters</i> .....	427
--	-----

Practical Identity-Based Encryption Without Random Oracles <i>Craig Gentry</i> .....	445
---	-----

Sequential Aggregate Signatures and Multisignatures Without Random Oracles <i>Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, Brent Waters</i> .....	465
---	-----

## Multiparty Computation

Our Data, Ourselves: Privacy Via Distributed Noise Generation <i>Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, Moni Naor</i> .....	486
---	-----

On the (Im-)Possibility of Extending Coin Toss <i>Dennis Hofheinz, Jörn Müller-Quade, Dominique Unruh</i> . . . . .	504
Efficient Binary Conversion for Paillier Encrypted Values <i>Berry Schoenmakers, Pim Tuyls</i> . . . . .	522
Information-Theoretic Conditions for Two-Party Secure Function Evaluation <i>Claude Crépeau, George Savvides, Christian Schaffner, Jürg Wullschleger</i> . . . . .	538
<b>Cryptography for Groups</b>	
Unclonable Group Identification <i>Ivan Damgård, Kasper Dupont, Michael Østergaard Pedersen</i> . . . . .	555
Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys <i>Dan Boneh, Amit Sahai, Brent Waters</i> . . . . .	573
Simplified Threshold RSA with Adaptive and Proactive Security <i>Jesús F. Almansa, Ivan Damgård, Jesper Buus Nielsen</i> . . . . .	593
Erratum to: Advances in Cryptology – EUROCRYPT 2006 . . . . .	E1
<i>Serge Vaudenay</i>	
<b>Author Index</b> . . . . .	617