Lecture Notes in Computer Science 4004

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Springer

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

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

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

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

Table of Contents

Hash Functions

Oblivious Transfer

Numbers and Lattices

Foundations

Invited Talk II

Block Ciphers

Cryptography Without Random Oracles

Multiparty Computation

Cryptography for Groups