Lecture Notes in Computer Science 3376

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

Editorial Board

Alfred Menezes (Ed.)

Topics in Cryptology – CT-RSA 2005

The Cryptographers' Track at the RSA Conference 2005
San Francisco, CA, USA, February 14-18, 2005
Proceedings

Springer

Volume Editor

Alfred Menezes
University of Waterloo
Department of Combinatorics and Optimization
Waterloo, Ontario, N2L 3G1, Canada
E-mail: ajmeneze@uwaterloo.ca

Library of Congress Control Number: 2004117506

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4.4, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-24399-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11377726 06/3142 5 4 3 2 1 0

Preface

The RSA Conference is attended by over 10,000 security professionals each year. The Cryptographers' Track (CT-RSA), one of several parallel tracks at the conference, provides an excellent opportunity for cryptographers to showcase their research to a wide audience. CT-RSA 2005 was the fifth year of the Cryptographers' Track.

The selection process for the CT-RSA program is the same as for other cryptography research conferences. This year, the program committee selected 23 papers from 74 submissions (two of which were later withdrawn) that covered all aspects of cryptography. The program also included two invited talks by Cynthia Dwork and Moti Yung. These proceedings contain the revised versions of the selected papers. The revisions were not checked, and so the authors (and not the committee) bear full responsibility for the contents of their papers.

I am very grateful to the program committee for their very conscientious efforts to review each paper fairly and thoroughly. The initial review stage was followed by a tremendous amount of discussion which contributed to our high confidence in our judgements. Thanks also to the many external reviewers whose names are listed in the following pages. My apologies to those whose names were inadvertently omitted from this list.

Thanks to Eddie Ng for maintaining the submission server and the Web review system. The submission software was written by Chanathip Namprempre, and the Web review software by Wim Moreau and Joris Claessens. Thanks to Alfred Hofmann and his colleagues at Springer for the timely production of these proceedings. Finally, it is my pleasure to acknowledge Ari Juels and Mike Szydlo of RSA Laboratories for their assistance and cooperation during the past seven months.

October 2004 Alfred Menezes

RSA Cryptographers' Track 2005
February 14–18, 2005, San Francisco, CA, USA

The RSA Conference 2005 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track was organized by RSA Laboratories.

Program Chair

Alfred Menezes, University of Waterloo, Canada

Program Committee

Masayuki Abe ..... NTT Laboratories, Japan
Paulo Barreto ..... Scopus Tecnologia, Brazil
Alex Biryukov ..... K.U.Leuven, Belgium
John-Sebastien Coron ..... Gemplus, France
Steven Galbraith ..... Royal Holloway, University of London, UK
Amir Herzberg ..... Bar-Ilan University, Israel
Yuval Ishai ..... Technion, Israel
Stanislaw Jarecki ..... UC Irvine, USA
Lars Knudsen ..... Technical University of Denmark
Kaoru Kurosawa ..... Ibaraki University, Japan
Tanja Lange ..... Ruhr-Universität, Bochum, Germany
Helger Lipmaa ..... Helsinki University of Technology, Finland
Philip MacKenzie ..... DoCoMo, USA
Tal Malkin ..... Columbia University, USA
Wenbo Mao ..... HP Laboratories, UK
Ilya Mironov ..... Microsoft Research, USA
Josef Pieprzyk ..... Macquarie University, Australia
Palash Sarkar ..... Indian Statistical Institute, India
Jessica Staddon ..... Palo Alto Research Center, USA
Rene Struik ..... Certicom, Canada
Michael Szydlo ..... RSA Laboratories, USA
Tsuyoshi Takagi ..... TU Darmstadt, Germany

Steering Committee

Marc Joye ..... Gemplus, France
Tatsuaki Okamoto ..... NTT, Japan
Bart Preneel ..... K.U.Leuven, Belgium
Ron Rivest ..... MIT, USA
Moti Yung ..... Columbia University, USA

External Reviewers

Toru Akishita
Alexandr Andoni
Roberto Avanzi
Sara Bitan
Alexandra Boldyreva
Reinier Bröker
Daniel Brown
Bertrand Byramjee
Christophe De Canniere
Dario Catalano
Liqun Chen
Joe Cho
Carlos Cid
Mathieu Ciet
Scott Contini
Claus Diem
Yevgeniy Dodis
Eiichiro Fujisaki
Juan Garay
Craig Gentry
Philippe Golle
Shai Halevi
Darrel Hankerson
Heng Swee Huay
David Hwang
Kouichi Itoh
Tetsu Iwata
Antoine Joux
Masanobu Katagi
Jonathan Katz
Jeff King
Lea Kissner
Yuichi Komano
Hugo Krawczyk
Caroline Kudla
Joseph Lano
Kerstin Lemke
John Linn
Anna Lysyanskaya
Dahlia Malkhi
Daniele Micciancio
Anton Mityagin
Atsuko Miyaji
David Molnar
Michael Mueller
Jorge Nakahara
Wakaha Ogata
Kazuo Ohata
Yasuhiro Ohtaki
Akira Otsuka
Pascal Paillier
Zulfikar Ramzan
Leo Reyzin
Matt Robshaw
Markku-Juhani Saarinen
Taiichi Saito
Akashi Satoh
Kai Schramm
Daniel Schepers
Igor Shparlinski
Nigel Smart
Angelos Stavrou
Ron Steinfeld
Makoto Sugita
Matti Tommiska
Eran Tromer
Huaxiong Wang
Michael Wiener
Kai Wirt
Christopher Wolf
Shoko Yonezawa
Yunlei Zhao

Table of Contents

Design Principles

Password-Based Protocols

Pairings

Efficient and Secure Implementation