Lecture Notes in Computer Science 4887

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

Steven D. Galbraith (Ed.)

Cryptography and Coding

11th IMA International Conference
Cirencester, UK, December 18-20, 2007
Proceedings

Volume Editor

Steven D. Galbraith
Royal Holloway University of London
Mathematics Department
Egham, Surrey, TW20 0EX, UK
E-mail: steven.galbraith@rhul.ac.uk

Library of Congress Control Number: 2007940956

CR Subject Classification (1998): E.3-4, G.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77271-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77271-2 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 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12203093 06/3180 5 4 3 2 1 0

Preface

The 11th IMA Conference on Cryptography and Coding was held at the Royal Agricultural College, Cirencester, UK during December 18–20, 2007. As usual, the venue provided a relaxed and convivial atmosphere for attendees to enjoy the conference programme and discuss current and future research ideas.

The programme comprised three invited talks and 22 contributed papers. The invited speakers were Jonathan Katz (University of Maryland, USA), Patrick Solé (Ecole Polytechnique de l'Université de Nice-Sophia Antipolis, France) and Whit Diffie (Sun Microsystems, USA). Special thanks are due to these speakers. Two of the invited speakers provided papers, included in this volume, which highlight the connections between cryptography, coding theory and discrete mathematics.

The contributed talks were selected from 48 submissions. The accepted papers cover a range of topics in mathematics and computer science, including symmetric and public key cryptography, Boolean functions, sequences, efficient implementation and side-channel analysis.

I would like to thank all the people who helped with the conference programme and organization. First, I thank the Steering Committee for their guidance on the general format of the conference and for suggestions of members of the Programme Committee. I also heartily thank the Programme Committee and the sub-reviewers listed on the following pages for their thoroughness during the review process. Each paper was reviewed by at least three people. There was significant online discussion about a number of papers.

The submission and review process was greatly simplified by the ichair software developed by Thomas Baignères and Matthieu Finiasz. Thanks also to Jon Hart for running the submissions Web server and Sriram Srinivasan for designing and maintaining the conference Web page.

Thanks go to the authors of all submitted papers. I also thank the authors of accepted papers for revising their papers according to referee suggestions and returning latex source files in good time. The revised versions were not checked by the Programme Committee so authors bear full responsibility for their contents. I thank the staff at Springer for their help with producing the proceedings.

I thank Hewlett-Packard and Vodafone for their sponsorship of this event.

Finally, I wish to thank the conference staff of the Institute for Mathematics and its Applications, especially Lucy Nye and Sammi Lauesen, for their help with running the conference and handling the finances.

October 2007 Steven Galbraith

Cryptography and Coding 2007

Royal Agricultural College, Cirencester, UK
December 18–20, 2007

Sponsored by
The Institute of Mathematics and its Applications

in cooperation with
Hewlett-Packard Laboratories and *Vodafone Ltd.*

Programme Chair

Steven Galbraith	Royal Holloway University of London

Steering Committee

Bahram Honary	Lancaster University
Chris Mitchell	Royal Holloway
Kenny Paterson	Royal Holloway
Fred Piper	Royal Holloway
Nigel Smart	University of Bristol
Mike Walker	Vodafone Ltd. and Royal Holloway

Programme Committee

Steve Babbage	Vodafone Group Services Ltd.
Nigel Boston	South Carolina/Wisconsin
Pascale Charpin	INRIA Rocquencourt
Liqun Chen	Hewlett-Packard
Carlos Cid	Royal Holloway
YoungJu Choie	Postech, Korea
Arjen Lenstra	EPFL, Lausanne
Alexander May	Ruhr Universität Bochum
Gary McGuire	University College Dublin
Alfred Menezes	University of Waterloo
David Naccache	Ecole Normale Supérieure
Matthew Parker	University of Bergen
Matt Robshaw	France Telecom
Ana Sălăgean	Loughborough University
Berry Schoenmakers	Technical University Eindhoven
Michael Scott	Dublin City University
Amin Shokrollahi	EPFL, Lausanne
Nigel Smart	University of Bristol
Frederik Vercauteren	K. U. Leuven
Gilles Zemor	Université Bordeaux

External Reviewers

Joppe Bos
Christophe De Cannière
Anne Canteaut
Claude Carlet
Mahdi Cheraghchi
Alex Dent
Fabien Galand
Philippe Guillot
Darrel Hankerson
Marcelo Kaihara
Cedric Lauradoux
Lorenz Minder
Marine Minier
Stephane Manuel
Ashley Montanaro
Sean Murphy
Dag Arne Osvik
Gregory Neven
Dan Page
Kenny Paterson
Benny Pinkas
Louis Salvail
Amin Shokrollahi
Andrey Sidorenko
Patrick Solé
Martijn Stam
Søren Steffen Thomsen
Eran Tromer
José Villegas

Table of Contents

Side Channels

Linear Complexity

Public Key Encryption

Curves

RSA Implementation

Signatures II