Lecture Notes in Computer Science 6673

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

Serge Fehr (Ed.)

Information Theoretic Security

5th International Conference, ICITS 2011
Amsterdam, The Netherlands, May 21-24, 2011
Proceedings

Springer

Volume Editor

Serge Fehr
Centrum Wiskunde & Informatica (CWI)
Science Park 123, 1098 XG Amsterdam, The Netherlands
E-mail: serge.fehr@cwi.nl

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-20727-3 e-ISBN 978-3-642-20728-0
DOI 10.1007/978-3-642-20728-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011926693

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

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

ICITS 2011, the 5th International Conference on Information Theoretic Security, was held in the city of Amsterdam, The Netherlands, during May 21–24, 2011. The conference took place at CWI, the Dutch Center for Mathematics and Computer Science, and at the Trippenhuis, the headquarters of the Royal Dutch Academy of Arts and Sciences.

The goal of this conference series is to bring together the leading researchers in the field of information-theoretic cryptography. This area of cryptography aims at understanding the possibility and impossibility of cryptographic schemes that offer information-theoretic security. Such a strong level of security, sometimes also referred to as unconditional security, is very attractive as it does not rely on unproven computational hardness assumptions, and in particular also withstands attacks by quantum computers. The price for this level of security often comes in the form of less efficiency and/or some physical assumption. Understanding the minimal requirements for information-theoretic security is a central part of this line of research. Personally, what I find very attractive is the mathematical neatness of the field, and its rich connections to other areas of mathematics, such as probability and information theory, algebra, combinatorics, coding theory, and quantum information processing, just to mention the most prominent ones.

There were 27 submitted papers of which 10 were selected. Each contributed paper was reviewed by at least three members of the Program Committee. Submissions co-authored by Program Committee members were reviewed by at least five members. The Program Committee worked hard to review and discuss the submissions, and to finally select the best papers among them. It was a pleasure to work together with such a motivated and professional Program Committee. I would like to thank each member for his/her contribution. I also thank the external reviewers who assisted the Program Committee members during the reviewing process.

In addition to the accepted papers, the conference also featured nine invited speakers. Each invited speaker provided a summary of his presentation as a contribution to these proceedings. The invited speakers were: Benny Applebaum, Alexander Barg, Imre Csiszár, Ivan Damgård, Yuval Ishai, Renato Renner, Leonid Reyzin, Amin Shokrollahi, and Ronald de Wolf.

As a new component, ICITS 2011 featured a Rump Session: an informal afternoon program that gave all the attendees the possibility for a short presentation on a topic of their choosing. I hope that this turns into a tradition for future ICITS conferences.

I would like to thank the two General Chairs, Ronald Cramer and Krzysztof Pietrzak, for organizing the conference and for ensuring a smooth running of the event. I would also like to thank Niek Bouman for chairing the Rump Session, and Joachim Schipper for his work behind the scenes. Furthermore, my thanks

go to the local support staff at CWI, in particular to Susanne van Dam for her unwavering organizational assistances, and to Maarten Dijkema and Chris Wesseling for setting-up and maintaining the submission system. I used Shai Halevi's Web Submission And Review Software; this is a very handy system which was of great help to me to perform my work as Program Chair, and Shai was always very prompt in answering questions.

Last but not least, I would like to thank all the authors who submitted papers to the conference and all the attendees of the conference; you are the ones that make ICITS possible.

May 2011 Serge Fehr

ICITS 2011

The 5th International Conference on Information Theoretic Security
CWI Amsterdam, The Netherlands
May 21–24, 2011.

Supported by an NWO[1] VICI grant

General Chairs

Ronald Cramer	CWI Amsterdam, and Mathematical Institute Leiden University, The Netherlands
Krzysztof Pietrzak	CWI Amsterdam, The Netherlands

Program Chair

Serge Fehr	CWI Amsterdam, The Netherlands

Program Committee

Amos Beimel	Ben-Gurion University, Israel
Nishanth Chandran	UCLA, USA
Hao Chen	East China Normal University, China
Paolo D'Arco	University of Salerno, Italy
Stefan Dziembowski	La Sapienza, Italy
Serge Fehr, Chair	CWI, The Netherlands
Juan Garay	AT&T Labs – Research, USA
Vipul Goyal	Microsoft Research, India
Maria Isabel González Vasco	University Rey Juan Carlos, Spain
Kaoru Kurosava	Ibaraki University, Japan
Eyal Kushilevitz	Technion, Israel
Keith Martin	Royal Holloway, UK
Jesper Buus Nielsen	Aarhus University, Denmark
Carles Padró	Nanyang Technological University, Singapore
Reihaneh Safavi-Naini	University of Calgary, Canada
Louis Salvail	University of Montreal, Canada
Christian Schaffner	CWI, The Netherlands
Berry Schoenmakers	TU Eindhoven, The Netherlands
Adam Smith	Pennsylvania State University, USA
Tamir Tassa	The Open University, Israel
Dominique Unruh	Saarland University, Germany
Daniel Wichs	New York University, USA
Jürg Wullschleger	Université de Montréal and McGill, Canada

[1] Netherlands Organisation for Scientific Research.

Steering Committee

Carlo Blundo	University of Salerno, Italy
Gilles Brassard	University of Montreal, Canada
Ronald Cramer	CWI and Leiden University, The Netherlands
Yvo Desmedt, Chair	University College London, UK
Hideki Imai	AIST and Chuo University, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Ueli Maurer	ETH, Switzerland
C. Pandu Rangan	IIT, Madras and IIT, Hyderabad, India
Reihaneh Safavi-Naini	University of Calgary, Canada
Doug Stinson	University of Waterloo, Canada
Moti Yung	Google and Columbia University, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

External Referees

Hadi Ahmadi	Matthias Fitzi	Gil Segev
Mohsen Alimomeni	Goichiro Hanaoka	Ashraful Tuhin
Gilad Asharov	Michael Langberg	Severin Winkler
Seung Geol Choi	Steve Lu	He Xiang
Ashish Choudhury	Hemanta Maji	Vassilis Zikas
Stelvio Cimato	Ilan Orlov	
Frédéric Dupuis	Anat Paskin	
Sebastian Faust	Angel L. Perez del Pozo	

Table of Contents