Lecture Notes in Computer Science 4883

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

Yvo Desmedt (Ed.)

Information Theoretic Security

Second International Conference, ICITS 2007
Madrid, Spain, May 25-29, 2007
Revised Selected Papers

Springer

Volume Editor

Yvo Desmedt
Department of Computer Science
University College London
Gower Street, London WC1E 6BT, UK
E-mail: y.desmedt@cs.ucl.ac.uk

Library of Congress Control Number: 2009938103

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

ISSN 0302-9743
ISBN-10 3-642-10229-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-10229-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12787302 06/3180 5 4 3 2 1 0

Preface

ICITS 2007, the Second International Conference on Information Theoretic Security, was held in Madrid, Spain, May 25-29, 2007. The first one was held on Awaji Island, Japan, October 16-19, 2005, as the 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW 2005, Japan). The General Chair of ICITS 2007, Javier Lopez, and the Organizing Committee were responsible for local organization, registration, etc.

Modern unclassified research on cryptography started with Shannon's work on cryptography using information theory. Since then we have seen several research topics studied, requiring information theoretical security, also called unconditional security. Examples are anonymity, authenticity, reliable and private networks, secure multi-party computation, traitor tracing, etc. Moreover, we have also seen that coding as well as other aspects of information theory have been used in the design of cryptographic schemes.

In the last few years there have been plenty of conferences and workshops on specialized topics in cryptography. Examples are CHES, FSE, PKC and TCC. In view of the multitude of topics in cryptography requiring information theoretical security or using information theory, it is time to have a regular conference on this topic. This was first realized by Prof. Imai (then at University of Tokyo, Japan), who organized the first event in October 2005. The goal is to continue this event on a regular basis.

There were 26 papers submitted to ICITS 2007, of which one was withdrawn. Of the remaining ones, 13 were accepted. Ueli Maurer was the invited keynote speaker on "Random Systems: Theory and Applications." The other invited speakers were Amos Beimel, on "On Linear, Non-linear and Weakly-Private Secret Sharing Scheme," Iordanis Kerenidis on "An Introduction to Quantum Information Theory," Eyal Kushilevitz on "Zero-Knowledge from Secure Multiparty Computation," Renato Renner on "Can We Justify the i.i.d. Assumption?," Junji Shikata on "Construction Methodology of Unconditionally Secure Signature Schemes," Alain Tapp on "Anonymous Quantum Message Transmission," and Raymond Yeung on "Network Coding and Information Security."

The proceedings contain the slightly revised versions of the accepted papers and summaries of the keynote address and some invited papers. Each submitted paper was sent to at least three members of the Program Committee for comments. Revisions were not checked for correctness on their scientific aspects and the authors bear full responsibility for the contents of their papers. The invited talks were not refereed.

I am very grateful to the members of the Program Committee for their hard work and the difficult task of selecting roughly 1 out of 2 of the submitted papers. Submissions to ICITS 2007 were required to be anonymous. Papers submitted

by members of the Program Committee were sent to at least five referees (and, of course, no Program Committee member reviewed his or her own paper).

The following external referees helped the Program Committee in reaching their decisions: Masucci Barbara, Anne Broadbent, Ingemar Cox, José Manuel Fernandez, Robbert de Haan, Goichiro Hanaoka, Tetsu Iwata, Kazukuni Kobara, Hiroki Koga, Thomas Martin, David Mireles-Morales, Maura Paterson, Krzysztof Pietrzak, Dominik Raub, Junji Shikata, Kazuhiro Suzuki, Alain Tapp, Yongge Wang, Takashi Satoh, Alain Tapp, Juerg Wullschleger, Frédéric Dupuis. (I apologize for any possible omission.) The Program Committee appreciates their effort.

Thanks to the Organizing Committee, for maintaining the website of the conference, the registration, and the services corresponding to a conference. Neil Marjoram is thanked for setting up iChair and the e-mail address for submission-related issues for ICITS. Several people helped the General Chair with sending out the call for papers, registration, etc. I would also like to thank the General Chair for all his advice. Also, special thanks to Gilles Brassard for helping to format the preproceedings.

Finally, I would like to thank everyone who submitted to ICITS 2007.

September 2009 Yvo Desmedt

ICITS 2007

Second International Conference on Information Theoretic Security

Universidad Carlos III de Madrid, Spain
May 25-29, 2007

General Chair

Javier Lopez	University of Malaga, Spain

Conference Chair

Arturo Ribagorda Garnacho	Universidad Carlos III de Madrid, Spain

Local Co-chairs

Julio César Hernández Castro	Universidad Carlos III de Madrid, Spain
Maria Isabel González Vasco	Universidad Rey Juan Carlos, Spain

Program Chair

Yvo Desmedt	University College London, UK

Program Committee

Carlo Blundo	University of Salerno, Italy
Gilles Brassard	University of Montreal, Canada
Ronald Cramer	CWI, The Netherlands
Matthias Fitzi	Århus University, Denmark
Hideki Imai	National Institute of Advanced Industrial Science and Technology, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Keith Martin	Royal Holloway, UK
Rei Safavi-Naini	University of Calgary, Canada
Doug Stinson	University of Waterloo, Canada
Stefan Wolf	ETH, Switzerland
Moti Yung	RSA & Columbia University, USA
Yuliang Zheng	University of North Carolina, USA

Steering Committee

Carlo Blundo	University of Salerno, Italy
Gilles Brassard	University of Montreal, Canada
Ronald Cramer	CWI, The Netherlands
Yvo Desmedt, Chair	University College London, UK
Hideki Imai	National Institute of Advanced Industrial Science and Technology, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Ueli Maurer	ETH, Switzerland
Rei Safavi-Naini	University of Calgary, Canada
Doug Stinson	University of Waterloo, Canada
Moti Yung	RSA & Columbia University, USA
Yuliang Zheng	University of North Carolina, USA

Organizing Committee

Julio César Hernández Castro	Universidad Carlos III de Madrid, Spain
Maria Isabel González Vasco	Universidad Rey Juan Carlos, Spain
Ana Isabel González-Tablas	Universidad Carlos III de Madrid, Spain
Javier Lopez	University of Malaga, Spain
Arturo Ribagorda Garnacho	Universidad Carlos III de Madrid Spain

Table of Contents

Authentication II

Invited Talk

Secret Sharing

Invited Talk

Applications of Information Theory