

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

Alfred Kobsa

University of California, Irvine, CA, 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

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

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 I

Commitment and Authentication Systems	1
<i>Alexandre Pinto, André Souto, Armando Matos, and Luís Antunes</i>	
Unconditionally Secure Blind Signatures	23
<i>Yuki Hara, Takenobu Seito, Junji Shikata, and Tsutomu Matsumoto</i>	

Keynote Lecture

Random Systems: Theory and Applications	44
<i>Ueli Maurer</i>	

Group Cryptography

Optimising SD and LSD in Presence of Non-uniform Probabilities of Revocation	46
<i>Paolo D'Arco and Alfredo De Santis</i>	
Trade-Offs in Information-Theoretic Multi-party One-Way Key Agreement	65
<i>Renato Renner, Stefan Wolf, and Jürg Wullschleger</i>	
Improvement of Collusion Secure Convolutional Fingerprinting Information Codes	76
<i>Joan Tomàs-Buliart, Marcel Fernandez, and Miguel Soriano</i>	

Private and Reliable Message Transmission

On Exponential Lower Bound for Protocols for Reliable Communication in Networks	89
<i>K. Srinathan, C. Pandu Rangan, and R. Kumaresan</i>	
Almost Secure (1-Round, n -Channel) Message Transmission Scheme	99
<i>Kaoru Kurosawa and Kazuhiro Suzuki</i>	

Invited Talk

Construction Methodology of Unconditionally Secure Signature Schemes	113
<i>Junji Shikata</i>	

Authentication II

New Results on Unconditionally Secure Multi-receiver Manual Authentication	115
<i>Shuhong Wang and Reihaneh Safavi-Naini</i>	
Unconditionally Secure Chaffing-and-Winnowing for Multiple Use	133
<i>Wataru Kitada, Goichiro Hanaoka, Kanta Matsuura, and Hideki Imai</i>	

Invited Talk

Introduction to Quantum Information Theory	146
<i>Iordanis Kerenidis</i>	

Secret Sharing

Strongly Multiplicative Hierarchical Threshold Secret Sharing	148
<i>Emilia Käsper, Ventzislav Nikov, and Svetla Nikova</i>	
Secret Sharing Comparison by Transformation and Rotation.....	169
<i>Tord Ingolf Reistad and Tomas Toft</i>	

Invited Talk

Anonymous Quantum Communication (Extended Abstract)	181
<i>Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp</i>	

Applications of Information Theory

Efficient Oblivious Transfer Protocols Achieving a Non-zero Rate from Any Non-trivial Noisy Correlation.....	183
<i>Hideki Imai, Kirill Morozov, and Anderson C.A. Nascimento</i>	
Cryptographic Security of Individual Instances.....	195
<i>L. Antunes, S. Laplante, A. Pinto, and L. Salvador</i>	

Author Index	211
--------------------	-----