Lecture Notes in Computer Science 5155

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

Reihaneh Safavi-Naini (Ed.)

Information Theoretic Security

Third International Conference, ICITS 2008
Calgary, Canada, August 10-13, 2008
Proceedings

Springer

Volume Editor

Reihaneh Safavi-Naini
University of Calgary
Department of Computer Science
ICT Building, 2500 University Drive NW
Calgary, AB, T2N 1N4, Canada
E-mail: rei@cpsc.ucalgary.ca

Library of Congress Control Number: 2008931579

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 3-540-85092-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85092-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12444649 06/3180 5 4 3 2 1 0

Preface

ICITS 2008, the Third International Conference on Information Theoretic Security, was held in Calgary, Alberta, Canada, during August 10–13, 2008, at the University of Calgary. This series of conferences was started with the 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW 2005, Japan), held on Awaji Island, Japan, October 16–19, 2005.

The conference series aims at bringing focus to security research when there is no unproven computational assumption on the adversary. This is the framework proposed by Claude Shannon in his seminal paper formalizing modern unclassified research on cryptography. Over the last few decades, Shannon's approach to formalizing security has been used in various other areas including authentication, secure communication, key exchange, multiparty computation and information hiding to name a few. Coding theory has also proven to be a powerful tool in the construction of security systems with information theoretic security.

There were 43 submitted papers of which 14 were accepted. Each contributed paper was reviewed by three members of the Program Committee. In the case of co-authorship by a Program Committee member the paper was reviewed by five members of the committee (no committee member reviewed their own submission). In addition to the accepted papers, the conference also included nine invited speakers, whose contributions were not refereed. These proceedings contain the accepted papers with any revisions required by the Program Committee as well as the contributions by invited speakers.

The invited speakers were:

João Barros	Strong Secrecy for Wireless Channels
Claude Crèpeau	Interactive Hashing: An Information Theoretic Tool
Juan Garay	Partially Connected Networks: Information Theoretically Secure Protocols and Open Problems
Venkatesan Guruswami	List Error-Correction with Optimal Information Rate
Goichiro Hanaoka	Some Information-Theoretic Arguments for Encryption: Non-malleability and Chosen-Ciphertext Security
Norbert Lütkenhaus	Theory of Quantum Key Distribution: The Road Ahead
Pierre Moulin	Perfectly Secure Information Hiding
Serge Vaudenay	The Complexity of Distinguishing Distributions
Moti Yung	Does Physical Security of Cryptographic Devices Need a Formal Study?

Submissions to ICITS 2008 were required to be anonymous. The task of selecting 14 papers out of 43 submissions was challenging. Each paper was carefully discussed until a consensus was reached. It was a great pleasure to work with such a high-caliber and meticulous Program Committee. External referees helped the Program Committee in reaching their decisions, and I thank them for their effort. A list of all external referees appears later in these proceedings.

I would like to thank the General Chair of the conference, Barry Sanders, and the Organizing Committee (listed below), whose unrelenting effort ensured the smooth running of the conference. I would like to thank Michal Sramka and Karl-Peter Marzlin, in particular, for their continued effort in maintaining the conference website and submission system (iChair), and lending a hand whenever it was required.

The conference benefited enormously from the generous financial support of the University of Calgary, the Informatics Circle of Research Excellence in Alberta, the Pacific Institute of Mathematical Sciences, the Canadian Institute for Advanced Research and Quantum Works.

Finally, I would like to thank the authors of all submitted papers for their hard work and all attendees of the conference whose support ensured the success of the conference.

August 2008 Reihaneh Safavi-Naini

ICITS 2008

The Third International Conference on Information Theoretic Security
University of Calgary, Canada
August 10–13, 2008

General Chair

Barry Sanders	QIS[1],University of Calgary, Canada

Program Chair

Reihaneh Safavi-Naini	iCIS Lab[2], University of Calgary, Canada

Program Committee

Simon Blackurn	Royal Holloway University of London, UK
Carlo Blundo	University of Salerno, Italy
Stefan Dziembowski	Universitá La Sapienza, Italy
Cunsheng Ding	Hong Kong University of Science and Technology, Hong Kong
Yevgeniy Dodis	New York University, USA
Paolo D'Arco	University of Salerno, Italy
Serge Fehr	CWI, The Netherland
Matthias Fitzi	ETH, Switzerland
Hideki Imai	Chuo University, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Jörn Müller-Quade	Universität Karlsruhe, Germany
Dingyi Pei	Academia Sinica, P.R. China
C. Pandu Rangan	Indian Institute of Technology, India
Renato Renner	ETH, Switzerland
Alain Tapp	Université de Montréal, Canada
Huaxiong Wang	Nanyang Technological University, Singapore
Wolfgang Tittel	University of Calgary, Canada
Moti Yung	Google and Columbia University, USA
Yuliang Zheng	University of North Carolina, USA

[1] Institute for Quantum Information Sciences.
[2] iCORE Information Security Laboratory.

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
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, USA

Organizing Committee

Mina Askari	iCIS Lab, University of Calgary, Canada
Catherine Giacobbo	QIS, University of Calgary, Canada
Jeong San Kim	QIS, University of Calgary, Canada
Itzel Lucio Martinez	QIS, University of Calgary, Canada
Karl-Peter Marzlin	QIS, University of Calgary, Canada
Xiaofan Mo	QIS, University of Calgary, Canada
Michal Sramka	iCIS Lab, University of Calgary, Canada

External Referees

Nuttapong Attrapadung
Kai Yuen Cheong
Ashish Choudary
Yang Cui
Yvo Desmedt
Dejan Dukaric
Nelly Fazio
Jun Furukawa
Clemente Galdi
Robbert de Haan
Manabu Hagiwara
Martin Hirt
Shaoquan Jiang
Masaru Kamada
Aggelos Kiayias
Varad kirtane
Takeshi Koshiba
Donggang Liu
Anderson C.A. Nascimento
Frederique Oggier
Arpita Patra
Krzysztof Pietrzak
Hongsng Shi
Takeshi Shimoyama
SeongHan Shin
Hitoshi Tanuma
Ashraful Tuhin
Ivan Visconti

Table of Contents

Information Hiding and Tracing

Coding Theory and Security

Quantum Computation

Secure and Reliable Communication II

Foundation

Encryption