

*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

*Massachusetts Institute of Technology, 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*

Reihaneh Safavi-Naini (Ed.)

# Information Theoretic Security

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

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

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 2008  
Printed in Germany

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<sup>1</sup>, University of Calgary, Canada

## Program Chair

Reihaneh Safavi-Naini              iCIS Lab<sup>2</sup>, University of Calgary, Canada

## Program Committee

Simon Blackburn	Royal Holloway University of London, UK
Carlo Blundo	University of Salerno, Italy
Stefan Dziembowski	Università 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 Netherlands
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

---

<sup>1</sup> Institute for Quantum Information Sciences.

<sup>2</sup> 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	Aggelos Kiayias
Kai Yuen Cheong	Varad kirtane
Ashish Choudary	Takeshi Koshihara
Yang Cui	Donggang Liu
Yvo Desmedt	Anderson C.A. Nascimento
Dejan Dukaric	Frederique Oggier
Nelly Fazio	Arpita Patra
Jun Furukawa	Krzysztof Pietrzak
Clemente Galdi	Hongsng Shi
Robbert de Haan	Takeshi Shimoyama
Manabu Hagiwara	SeongHan Shin
Martin Hirt	Hitoshi Tanuma
Shaoquan Jiang	Ashraful Tuhin
Masaru Kamada	Ivan Visconti

# Table of Contents

## Secure and Reliable Communication I

Partially Connected Networks: Information Theoretically Secure Protocols and Open Problems (Invited Talk) .....	1
<i>Juan A. Garay</i>	
Almost Secure 1-Round Message Transmission Scheme with Polynomial-Time Message Decryption .....	2
<i>Toshinori Araki</i>	

## Quantum Information and Communication

Interactive Hashing: An Information Theoretic Tool (Invited Talk) .....	14
<i>Claude Crépeau, Joe Kilian, and George Savvides</i>	
Distributed Relay Protocol for Probabilistic Information-Theoretic Security in a Randomly-Compromised Network .....	29
<i>Travis R. Beals and Barry C. Sanders</i>	

## Networks and Devices

Strong Secrecy for Wireless Channels (Invited Talk) .....	40
<i>João Barros and Matthieu Bloch</i>	
Efficient Key Predistribution for Grid-Based Wireless Sensor Networks .....	54
<i>Simon R. Blackburn, Tuvi Etzion, Keith M. Martin, and Maura B. Paterson</i>	
Does Physical Security of Cryptographic Devices Need a Formal Study? (Invited Talk) .....	70
<i>François-Xavier Standaert, Tal G. Malkin, and Moti Yung</i>	

## Multiparty Computation

A Single Initialization Server for Multi-party Cryptography .....	71
<i>Hugue Blier and Alain Tapp</i>	
Statistical Security Conditions for Two-Party Secure Function Evaluation .....	86
<i>Claude Crépeau and Jürg Wullschlegel</i>	



## Information Hiding and Tracing

Upper Bounds for Set Systems with the Identifiable Parent Property ...	100
<i>Michael J. Collins</i>	

## Coding Theory and Security

Oblivious Transfer Based on the McEliece Assumptions .....	107
<i>Rafael Dowsley, Jeroen van de Graaf, Jörn Müller-Quade, and Anderson C.A. Nascimento</i>	
List Error-Correction with Optimal Information Rate (Invited Talk) ....	118
<i>Venkatesan Guruswami</i>	

## Quantum Computation

Theory of Quantum Key Distribution: The Road Ahead (Invited Talk) .....	120
<i>Norbert Lütkenhaus</i>	
Susceptible Two-Party Quantum Computations .....	121
<i>Andreas Jakoby, Maciej Liškiewicz, and Aleksander Mądry</i>	

## Secure and Reliable Communication II

Perfectly Reliable and Secure Communication Tolerating Static and Mobile Mixed Adversary .....	137
<i>Ashish Choudhary, Arpita Patra, B.V. Ashwinkumar, K. Srinathan, and C. Pandu Rangan</i>	
Key Refreshing in Wireless Sensor Networks .....	156
<i>Simon R. Blackburn, Keith M. Martin, Maura B. Paterson, and Douglas R. Stinson</i>	
Efficient Traitor Tracing from Collusion Secure Codes .....	171
<i>Olivier Billet and Duong Hieu Phan</i>	

## Foundation

Revisiting the Karnin, Greene and Hellman Bounds .....	183
<i>Yvo Desmedt, Brian King, and Berry Schoenmakers</i>	
Simple Direct Reduction of String (1,2)-OT to Rabin's OT without Privacy Amplification .....	199
<i>Kaoru Kurosawa and Takeshi Koshihara</i>	
The Complexity of Distinguishing Distributions (Invited Talk) .....	210
<i>Thomas Baignères and Serge Vaudenay</i>	

## Encryption

Some Information Theoretic Arguments for Encryption: Non-malleability and Chosen-Ciphertext Security (Invited Talk) .....	223
<i>Goichiro Hanaoka</i>	
A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations .....	232
<i>Jacques Patarin</i>	
<b>Author Index</b> .....	249