Lecture Notes in Computer Science 5973

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

Kaoru Kurosawa (Ed.)

Information Theoretic Security

4th International Conference, ICITS 2009
Shizuoka, Japan, December 3-6, 2009
Revised Selected Papers

Springer

Volume Editor

Kaoru Kurosawa
Department of Computer
and Information Sciences
Ibaraki University
Hitachi, Ibaraki, Japan
E-mail: kurosawa@mx.ibaraki.ac.jp

Library of Congress Control Number: 2010932236

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 3-642-14495-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-14495-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

ICITS 2009 was held at the Shizuoka Convention and Arts Center "GRANSHIP" in Japan during December 3–6, 2009. This was the 4th International Conference on Information Theoretic Security.

Over the last few decades, we have seen several research topics studied requiring information theoretical security, also called unconditional security, where there is no unproven computational assumption on the adversary. (This is the framework proposed by Claude Shannon in his seminal paper.) Also, coding as well as other aspects of information theory have been used in the design of cryptographic schemes. Examples are authentication, secure communication, key exchange, multi-party computation and information hiding to name a few. A related area is quantum cryptography that predominantly uses information theory for modeling and evaluation of security. Needless to say, information theoretically secure cryptosystems are secure even if the factoring assumption or the discrete log assumption is broken. Seeing the multitude of topics in modern cryptography requiring information theoretical security or using information theory, it is time to have a regular conference on this topic. This was the fourth conference of this series, aiming to bring together the leading researchers in the area of information and/or quantum theoretic security.

There were 50 submissions of which 13 papers were accepted. Each paper was reviewed by at least three members of the Program Committee, while submissions co-authored by the Program Committee member were reviewed by at least five members. In addition to the accepted papers, the conference also included six invited speakers. These proceedings contain the accepted papers and the contribution by invited speakers. The invited speakers were: Yevgeniy Dodis "Leakage-Resilience and The Bounded Retrieval Model," Masato Koashi "Security of Key Distribution and Complementarity in Quantum Mechanics," Kazukuni Kobara "Code-Based Public-Key Cryptosystems and Their Applications," Prakash Narayan "Multiterminal Secrecy Generation and Tree Packing," Adi Shamir "Random Graphs in Security and Privacy" and Adam Smith "What Can Cryptography Do for Coding Theory?"

The conference received financial support from the Support Center for Advance Telecommunications Technology Research, Kayamori Foundation of Informational Science Advancement, and Research Center for Information Security (RCIS) of the National Institute of Advanced Industrial Science Technologies (AIST). We also received local support from the Shizuoka Convention and Visitors Bureau.

There are many people who contributed to the success of ICITS 2009. I would like to thank many authors from around the world for submitting their papers. I am deeply grateful to the Program Committee for their hard work to ensure that each paper received a thorough and fair review. I gratefully acknowledge

the external reviewers listed on the following pages. I would like to thank Shai Halevi for developing and maintaining his very nice Web Submission and Review System. Finally, I would like to thank the general chair, Akira Otsuka, and the local organizer, Yukiko Ito, for organizing the conference. In particular, the unrelenting effort of Yukiko ensured the smooth running of the conference.

January 2010 Kaoru Kurosawa

ICITS 2009

The 4th International Conference on Information Theoretic Security

December 3–6, 2009, Shizuoka, Japan

In cooperation with
International Association for Cryptologic Research (IACR) and
Technical Group on Information Security (ISEC) of IEICE, Japan

Technical Co-sponsor: *IEEE Information Theory Society*

General Chair

Akira Otsuka	National Institute of Advanced Industrial Science and Technology, Japan

Program Chair

Kaoru Kurosawa	Ibaraki University, Japan

Program Committee

Carlo Blundo	University of Salerno, Italy
Stefan Dziembowski	Universita La Sapienza, Italy
Paolo D'Arco	University of Salerno, Italy
Serge Fehr	CWI, The Netherlands
Juan Garay	AT&T Labs-Research, USA
Goichiro Hanaoka	National Institute of Advanced Industrial Science and Technology, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Hoi-Kwong Lo	University of Toronto, Canada
Keith Martin	Royal Holloway, University of London, UK
Ueli Maurer	ETH, Switzerland
Jesper Buus Nielsen	University of Aarhus, Denmark
Renato Renner	ETH, Switzerland
Rei Safavi-Naini	University of Calgary, Canada
Thomas Shrimpton	University of Lugano, Switzerland
Doug Stinson	University of Waterloo, Canada
Stefan Wolf	ETH, Switzerland
Moti Yung	Google and 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	Google and Columbia University, USA
Yuliang Zheng	University of North Carolina, USA

Local Organizer

Yukiko Ito	National Institute of Advanced Industrial Science and Technology, Japan

Advisor

Hideki Imai	National Institute of Advanced Industrial Science and Technology, Japan and Chuo University, Japan

External Reviewers

Johan Aaberg	Peter Gaži	Krzysztof Pietrzak
Hadi Ahmadi	Clint Givens	Angel Perez Del Pozo
Susan Barwick	Amin Aminzadeh Gohari	Dominik Raub
Zuzana Beerliova-Trubiniova	Yuval Ishai	Bagus Santoso
David Bernhard	Taichi Isogai	Hongsong Shi
Annalisa De Bonis	Yoshiyuki Kabashima	Thomas Sirvent
Niek Bouman	Hiroki Koga	Björn Tackmann
Cyril Branciard	Takeshi Koshiba	Stefano Tessaro
Ashish Choudhary	Kirill Morozov	Marco Tomamichel
Roger Colbeck	Yusuke Naito	Ivan Visconti
Yevgeniy Dodis	Siaw-Lynn Ng	Douglas Wikström
Matthias Fitzi	Koji Nuida	Hong-Sheng Zhou
Philip Fong	Miyako Ookubo	Vassilis Zikas
Clemente Galdi	Arpita Patra	
	Umberto Ferraro Petrillo	

Table of Contents

Leakage Resilient Cryptography

Quantum Cryptography and Indistinguishability

Connection to Computational Security

Secret Sharing

Key Agreement from Common Randomness

Random Graph and Group Testing

Reliable Data Transmision and Computation

Fingerprint and Watermarking