Lecture Notes in Computer Science 5557

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

Yeow Meng Chee Chao Li San Ling
Huaxiong Wang Chaoping Xing (Eds.)

Coding and Cryptology

Second International Workshop, IWCC 2009
Zhangjiajie, China, June 1-5, 2009
Proceedings

Springer

Volume Editors

Yeow Meng Chee
San Ling
Huaxiong Wang
Chaoping Xing

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371

E-mail:{ymchee; lingsan; hxwang; xingcp}@ntu.edu.sg

Chao Li
National University of Defense Technology,
410073 Changsha Hunan, China

E-mail: lichao_nudt@sina.com

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3-4, G.2.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-01813-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-01813-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12674015 06/3180 5 4 3 2 1 0

Preface

The biennial International Workshop on Coding and Cryptology (IWCC) aims to bring together many of the world's greatest minds in coding and cryptology to share ideas and exchange knowledge related to advancements in coding and cryptology, amidst an informal setting conducive for interaction and collaboration.

It is well known that fascinating connections exist between coding and cryptology. Therefore this workshop series was organized to facilitate a fruitful interaction and stimulating discourse among experts from these two areas.

The inaugural IWCC was held at Wuyi Mountain, Fujian Province, China, during June 11-15, 2007 and attracted over 80 participants. Following this success, the second IWCC was held June 1-5, 2009 at Zhangjiajie, Hunan Province, China. Zhangjiajie is one of the most scenic areas in China.

The proceedings of this workshop consist of 21 technical papers, covering a wide range of topics in coding and cryptology, as well as related fields such as combinatorics. All papers, except one, are contributed by the invited speakers of the workshop and each paper has been carefully reviewed. We are grateful to the external reviewers for their help, which has greatly strengthened the quality of the proceedings.

IWCC 2009 was co-organized by the National University of Defense Technology (NUDT), China and Nanyang Technological University (NTU), Singapore. We acknowledge with gratitude the financial support from NUDT.

We would like to express our thanks to Springer for making it possible for the proceedings to be published in the *Lecture Notes in Computer Science series*. We also thank Zhe-xian Wan for his great encouragement and constant support for this workshop series. We are also grateful to the staff and students from both NUDT and NTU for the administrative and technical support they have rendered to the conference and the proceedings. Special thanks go to Longjiang Qu for taking care of the website of the workshop, and Yang Ding for assistance on matters related to LaTeX.

Yeow Meng Chee
Chao Li
San Ling
Huaxiong Wang
Chaoping Xing

Organization

Chair of Organizing Committee

Zhe-xian Wan	Academy of Mathematics and System Sciences, CAS, China

Organizing Committee

Yeow Meng Chee	Nanyang Technological University, Singapore
Chao Li	National University of Defense Technology, China
San Ling	Nanyang Technological University, Singapore
Huaxiong Wang	Nanyang Technological University, Singapore
Zhengming Wang	National University of Defense Technology, China
Chaoping Xing	Nanyang Technological University, Singapore
Jianming Zhu	National University of Defense Technology, China

Table of Contents