PREFACE

The first International Workshop on Coding and Cryptology was held in Wuyi Mountain, Fujian, China, June 11 - 15, 2007. The workshop was organised by Fujian Normal University, China and Nanyang Technological University, Singapore. We acknowledge with gratitude the financial support from the Key Laboratory of Network Security and Cryptology, Fujian Normal University.

The idea for this workshop grew out of the recognition of the recent development in various areas of coding theory and cryptology. Over the past years, we have seen the rapid growth of the Internet and World-Wide-Web, they have provided great opportunities for online commercial activities, business transactions and government services over open computer and communications networks. However, such developments are only possible if communications can be conducted in a secure and reliable way. The mathematical theory and practice of coding theory and cryptology underpin the provision of effective security and reliability for data communication, processing and storage. Theoretical and practical advances in the fields are therefore a key factor in facilitating the growth of data communications and data networks.

The aim of the workshop was to bring experts from coding theory, cryptology and their related areas for a fruitful exchange of ideas. We hoped (and achieved) the meeting would encourage and stimulate further research in telecommunications, information and computer security, the design and implementation of coding-related cryptosystems and other related areas. Another goal of the meeting was to stimulate collaboration and more active interaction between mathematicians, computer scientists, practical cryptographers and engineers.

This workshop post-proceedings consists of 20 papers submitted by the invited speakers of the workshop, each paper has been reviewed by at least two referees. They cover a wide range of topics in coding theory and cryptology such as theory, techniques, applications, practical experiences. They contain significant advances in the areas as well as very useful surveys.

We would like to express our thanks to World Scientific Publishing Co.

and in particular, E H Chionh for the advice and support. We thank Zhexian Wan for his encouragement and support, the staff and students from the Key Laboratory of Network Security and Cryptology, Fujian Normal University for their excellent organization of the event. Special thanks also go to Guo Jian for the LaTeX assistance.