

Preface

The inaugural research program of the Institute for Mathematical Sciences at the National University of Singapore took place from July to December 2001 and was devoted to coding theory and cryptology. The program was split into three parts of about equal length: (i) mathematical foundations of coding theory and cryptology; (ii) coding and cryptography; (iii) applied cryptology.

As part of the program, tutorials for graduate students and junior researchers were given by leading experts. These tutorials covered fundamental aspects of coding theory and cryptology and were meant to prepare for original research in these areas. The present volume collects the expanded lecture notes of these tutorials. In the following, we give a brief indication of the range of topics that is represented in this volume. The 11 articles can roughly be classified into four groups, corresponding to mathematical foundations, coding theory, cryptology, and applied cryptology.

Coding theory and cryptology require several sophisticated mathematical tools which are covered in the articles by Lenstra, Niederreiter, and Shparlinski. The lecture notes of Lenstra present a detailed review of those parts of computational number theory that are relevant for the implementation and the analysis of public-key cryptosystems, such as fast arithmetic, prime generation, factoring, discrete logarithm algorithms, and algorithms for elliptic curves. It is important to note in this context that all public-key cryptosystems of current commercial interest rely on problems from computational number theory that are believed to be hard. The article by Niederreiter provides a quick introduction to the theory of algebraic function fields over finite fields. This theory is crucial for the construction of algebraic-geometry codes and has also found recent applications in cryptography. Exponential sums form another powerful number-theoretic tool in coding theory and they have recently come to the fore in cryptology as well. The lecture notes of Shparlinski offer an engaging introduction to the theory and the applications of exponential sums.

The articles by Barg, Feng, and Xing cover topics of great current interest in coding theory. Barg presents a selection of results on extremal problems of coding theory that are centered around the concept of a code as a packing of the underlying metric space. The results include combinatorial bounds on codes and their invariants, properties of linear codes, and applications of the polynomial method. The lecture notes of Feng describe the mathematical techniques in the rapidly developing subject of quantum error-correcting codes. The article contains also a useful review of classical error-correcting codes. The paper by Xing offers a brief introduction to algebraic-geometry codes and a description of some recent constructions of algebraic-geometry codes.

The articles by Dawson and Simpson, Matsumoto, and Pei deal with important mathematical aspects of cryptology. Dawson and Simpson provide a detailed account of current issues in the design and analysis of stream ciphers. The topics include Boolean functions, correlation attacks, the design of keystream generators, and implementation issues. The paper by Matsumoto is devoted to key management problems in group communication and describes recently developed key distribution schemes and protocols for such systems. The lecture notes of Pei present a detailed exposition of the author's recent work on optimal authentication schemes, both without and with arbitration. The essence of this work is to meet information-theoretic bounds by combinatorial constructions.

The lecture notes of Gollmann and Varadharajan treat topics in applied cryptology. Gollmann contributes to the intense debate on public-key infrastructures with an incisive examination of the security problems that public-key infrastructures claim to address. The article contains also a useful summary of current standards for public-key infrastructures. Varadharajan presents a detailed account of current principles for authorization policies and services in distributed systems. The article also outlines the constructs of a language that can be used to specify a range of commonly used access policies.

I want to take this opportunity to thank Professor Louis H.Y. Chen, the Director of the Institute for Mathematical Sciences, for his guidance and leadership of the IMS and for the invaluable advice he has so freely shared with the organizers of the research program. The expertise and the dedication of all the IMS staff were crucial for the success of the program. I am very grateful to my colleagues San Ling and Chaoping Xing of the Department of Mathematics at the National University of Singapore for the tremendous help they have given in running the program and

to the overseas advisers Eiji Okamoto (Toho University, Japan), Igor E. Shparlinski (Macquarie University, Australia), and Neil J.A. Sloane (AT&T Shannon Lab, USA) for their support and suggestions. The financial well-being of the research program was guaranteed by a generous grant from DSTA in Singapore, which is herewith acknowledged with gratitude. Finally, I would like to thank World Scientific Publishing, and especially Kim Tan and Ye Qiang, for the professionalism with which they have produced this volume.

Singapore, August 2002

Harald Niederreiter