

## Preface

The mathematical theory and practice of cryptography and coding underpins the provision of effective security and reliability for data communication, processing, and storage. Theoretical and implementational advances in the fields of cryptography and coding are therefore a key factor in facilitating the growth of data communications and data networks of various types. Thus, this Eight International Conference in an established and successful IMA series on the theme of “Cryptography and Coding” was both timely and relevant. The theme of this conference was the future of coding and cryptography, which was touched upon in presentations by a number of invited speakers and researchers.

The papers that appear in this book include recent research and development in error control coding and cryptography. These start with mathematical bounds, statistical decoding schemes for error correcting codes, and undetected error probabilities and continue with the theoretical aspects of error correction coding such as graph and trellis decoding, multifunctional and multiple access communication systems, low density parity check codes, and iterative decoding. These are followed by some papers on key recovery attack, authentication, stream cipher design, and analysis of ECIES algorithms, and lattice attacks on IP based protocols.

It is also my pleasant task to place on record my appreciation of the help and support of the members of the conference organizing committee, namely Mike Darnell, Paddy Farrell, Mick Ganley, John Gordon, Chris Mitchell, Fred Piper, and Mike Walker. I wish also to express my sincere thanks to Pamela Bye, Suzanne Coleman, and Terry Edwards of the IMA for their help with both the organization of the conference and the publication of this volume. Finally, my special thanks go to my colleague, Phillip Benachour, for his assistance in editing and preparing the camera-ready copies to a very tight schedule.

October 2001

Bahram Honary



<http://www.springer.com/978-3-540-43026-1>

Cryptography and Coding  
8th IMA International Conference Cirencester, UK,  
December 17-19, 2001 Proceedings  
Honary, B. (Ed.)  
2001, IX, 419 p., Softcover  
ISBN: 978-3-540-43026-1