Preface

The IMA conferences on Cryptography and Coding are not only a blend of these two aspects of information theory, but a blend of mathematics and engineering and of theoretical results and applications. The papers in this book show that the 1999 conference was no exception. Indeed, we again saw the mathematics underlying cryptography and error correcting coding being applied to other aspects of communications, and we also saw classical mathematical concepts finding new applications in communications theory.

As usual the conference was held at the Royal Agricultural College, Cirencester, shortly before Christmas - this time 20-22 December 1999. The papers appear in this book in the order in which they were presented, grouped into sessions, each session beginning with an invited paper. These invited papers were intended to reflect the invitees' views on the future of their subject - or more accurately where they intended to take it. Indeed the focus of the conference was the *future of cryptography and coding* as seen through the eyes of young researchers.

The first group of papers is concerned with mathematical bounds, concepts, and constructions that form a common thread running through error correcting coding theory, cryptography, and codes for multiple access schemes. This is followed by a group of papers from a conference session concerned with applications. The papers range over various topics from arithmetic coding for data compression and encryption, through image coding, biometrics for authentication, and access to broadcast channels, to photographic signatures for secure identification. The third set of papers deals with theoretical aspects of error correcting coding, including graph and trellis decoding, turbo codes, convolution codes and low complexity soft decision decoding of Reed Solomon codes. This is followed by a collection of papers concerned with some mathematical techniques in cryptography - elliptic curves, the theory of correlations of binary sequences, primality testing, and the complexity of finite field arithmetic. The final collection of papers is concerned primarily with protocols and schemes. There is a diversity of papers covering lattice based cryptosystems, protocols for sharing public key parameters and for delegating decryption, and arithmetic coding schemes.

It is my pleasure to record my appreciation to the members of the conference organising committee for their help in refereeing the papers that make up this volume. They were Michael Darnell, Paddy Farrell, Mick Ganley, John Gordon, Bahram Honary, Chris Mitchell, and Fred Piper. Sincere thanks also to Pamela Bye, Hilary Hill, Adrian Lepper, and Deborah Sullivan of the IMA for all their help with the organisation of the conference and with the publication of this collection of papers.

Finally, I hope that those of you who attended the conference found it rewarding and stimulating. For those of you who did not, I hope this book of papers will encourage you to participate in the next one.

December 1999 Mike Walker