CONTENTS

Block Ciphers: Differential and Linear Cryptanalysis

Schemes Based on New Problems

Signatures I

Implementation and Hardware Aspects

Authentication and Secret Sharing

Zero-Knowledge

Signatures II

Combinatorics and its Applications

Number Theory

Cryptanalysis and Protocol Failures

Pseudo-Random Generation

Block Ciphers: Design and Cryptanalysis

Secure Computations and Protocols