

Contents

List of Figures	xi
List of Tables	xiii
Preface	xvii
1. INTRODUCTION	1
1.1 Challenges of Broadcast Communication	3
1.2 Why is Security for Broadcasts Hard?	5
1.2.1 Broadcast Authentication	5
1.2.2 Broadcast Signature	8
1.2.3 Broadcast Data Integrity	9
1.2.4 Confidential Broadcasts and Restricting Access to Legitimate Receivers	9
1.3 Security Requirements for Broadcast Applications	10
1.4 Novel Contributions	12
1.5 Scope of this Book	13
1.6 Book Overview	13
2. CRYPTOGRAPHIC FUNDAMENTALS	19
2.1 Broadcast Network Requirements	19
2.2 Cryptographic Primitives	20
2.2.1 Symmetric and Asymmetric Cryptography	20
2.2.2 One-Way Functions and Hash Functions	20
2.2.3 Pseudo-Random Generator (PRG)	22
2.2.4 Message Authentication Code (MAC)	22
2.2.5 Pseudo-Random Function (PRF)	22
2.3 Efficiency of Cryptographic Primitives	23
2.4 Commitment Protocols	24

