

# Table of Contents

Practice-Oriented Provable Security .....	1
<i>Mihir Bellare</i>	
Introduction to Secure Computation .....	16
<i>Ronald Cramer</i>	
Commitment Schemes and Zero-Knowledge Protocols .....	63
<i>Ivan Damgård</i>	
Emerging Standards for Public-Key Cryptography .....	87
<i>Burt S. Kaliski Jr.</i>	
Contemporary Block Ciphers .....	105
<i>Lars R. Knudsen</i>	
Primality Tests and Use of Primes in Public-Key Systems .....	127
<i>Peter Landrock</i>	
Signing Contracts and Paying Electronically .....	134
<i>Torben P. Pedersen</i>	
The State of Cryptographic Hash Functions .....	158
<i>Bart Preneel</i>	
The Search for the Holy Grail in Quantum Cryptography .....	183
<i>Louis Salvail</i>	
Unconditional Security in Cryptography .....	217
<i>Stefan Wolf</i>	

Lectures on Data Security

Modern Cryptology in Theory and Practice

Damgård, I. (Ed.)

1999, 250 p., Softcover

ISBN: 978-3-540-65757-6