List of Figures

0.1 Organization of the work *page* xvi
0.2 Rough organization of this volume xvii
0.3 Plan for one-semester course on the foundations of cryptography xviii
1.1 Cryptography: two points of view 25
2.1 One-way functions: an illustration 31
2.2 The naive view versus the actual proof of Proposition 2.3.3 49
2.3 The essence of Construction 2.6.3 81
3.1 Pseudorandom generators: an illustration 102
3.2 Construction 3.3.2, as operating on seed $s_0 \in \{0, 1\}^n$ 114
3.3 Hybrid H_n^k as a modification of Construction 3.3.2 115
3.4 Construction 3.4.2, as operating on seed $s_0 \in \{0, 1\}^n$ 129
3.5 Construction 3.6.5, for $n = 3$ 151
3.6 The high-level structure of the DES 166
4.1 Zero-knowledge proofs: an illustration 185
4.2 The advanced sections of this chapter 185
4.3 The dependence structure of this chapter 186
B.1 The Blum-Goldwasser public-key encryption scheme [35] 342

Downloaded from https://www.cambridge.org/core. ETH-Bibliothek, on 22 Mar 2017 at 13:28:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511546891

Cambridge Books Online © Cambridge University Press, 2009