List of Figures

0.1	Organization of this work	*page* xvi
0.2	Rough organization of this volume	xvii
0.3	Plan for one-semester course on Foundations of Cryptography	xviii
5.1	Private-key encryption schemes: an illustration	375
5.2	Public-key encryption schemes: an illustration	376
6.1	Message-authentication versus signature schemes	500
6.2	Collision-free hashing via block-chaining (for $t = 7$)	519
6.3	Collision-free hashing via tree-chaining (for $t = 8$)	522
6.4	Authentication-trees: the basic authentication step	546
6.5	An authentication path for nodes 010 and 011	547
7.1	Secure protocols emulate a trusted party: an illustration	601
7.2	The functionalities used in the compiled protocol	658
7.3	Schematic depiction of a canonical protocol	690

Downloaded from https://www.cambridge.org/core. ETH-Bibliothek, on 22 Mar 2017 at 13:37:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721656

Downloaded from https://www.cambridge.org/core. ETH-Bibliothek, on 22 Mar 2017 at 13:37:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721656