
Contents

1	Fingerprinting Codes	1
1.1	Preliminaries	2
1.2	Definition of Fingerprinting Codes	3
1.3	Applications to Digital Content Distribution	5
1.4	Constructions	7
1.4.1	Combinatorial Constructions	7
1.4.2	The Chor-Fiat-Naor Fingerprinting Codes	14
1.4.3	The Boneh-Shaw Fingerprinting Codes	18
1.4.4	The Tardos Fingerprinting Codes	21
1.4.5	Code Concatenation	29
1.5	Bibliographic Notes	32
2	Broadcast Encryption	35
2.1	Definition of Broadcast Encryption	36
2.2	Broadcast Encryption Based on Exclusive-Set Systems	40
2.2.1	Security	44
2.2.2	The Subset Cover Framework	49
2.3	The Key-Poset Framework for Broadcast Encryption	50
2.3.1	Viewing Set Systems as Partial Orders	50
2.3.2	Computational Specification of Set Systems	55
2.3.3	Compression of Key Material	56
2.4	Revocation in the Key-Poset Framework	60
2.4.1	Revocation in the key-poset framework: Definitions	61
2.4.2	A sufficient condition for optimal revocation	64
2.5	Constructions	69
2.5.1	Complete Subtree	69
2.5.2	Subset Difference	74
2.5.3	Key Chain Tree	81
2.6	Generic Transformations for Key Posets	88
2.6.1	Layering Set Systems	89
2.6.2	X-Transformation	92

2.7	Bibliographic notes	101
3	Traitor Tracing	107
3.1	Multiuser Encryption Schemes	107
3.2	Constructions For Multiuser Encryption Schemes	109
3.2.1	Linear Length Multiuser Encryption Scheme	109
3.2.2	Multiuser Encryption Schemes Based on Fingerprinting Codes	112
3.2.3	Boneh-Franklin Multiuser Encryption Scheme	119
3.3	Tracing Game: Definitions	123
3.4	Types of Tracing Games	126
3.4.1	Non-Black Box Tracing Game.	126
3.4.2	Black-Box Tracing Game.	127
3.5	Traceability of Multiuser Encryption Schemes	130
3.5.1	Traceability of Linear Length Multiuser Encryption Scheme	130
3.5.2	Traceability of Schemes Based on Fingerprinting Codes	134
3.5.3	Traceability of the Boneh-Franklin Scheme	142
3.6	Bibliographic Notes	145
4	Trace and Revoke Schemes	151
4.1	Revocation Game: Definitions	152
4.2	Tracing and Revoking in the Subset Cover Framework	157
4.3	Tracing and Revoking Pirate Rebroadcasts	161
4.4	On the effectiveness of Trace and Revoke schemes	166
4.5	Bibliographic Notes	167
5	Pirate Evolution	171
5.1	Pirate Evolution: Definitions	172
5.2	A Trace and Revoke Scheme Immune to Pirate-Evolution	174
5.3	Pirate Evolution for the Complete Subtree Method	176
5.4	Pirate Evolution for the Subset Difference Method	182
5.5	Bibliographic Notes	196
	References	199
	Index	207