

Encryption For Digital Content

[DOWNLOAD HERE](#)

1;Preface;6 2;Contents;9 3;List of Figures;11 4;1 Fingerprinting Codes;14 4.1;Preliminaries;15
4.2;Definition of Fingerprinting Codes;16 4.3;Applications to Digital Content Distribution;18
4.4;Constructions;20 4.4.1;Combinatorial Constructions;20 4.4.2;The Chor-Fiat-Naor Fingerprinting
Codes;27 4.4.3;The Boneh-Shaw Fingerprinting Codes;31 4.4.4;The Tardos Fingerprinting Codes;34
4.4.5;Code Concatenation;42 4.5;Bibliographic Notes;45 5;2 Broadcast Encryption;47 5.1;Definition of
Broadcast Encryption;48 5.2;Broadcast Encryption Based on Exclusive-Set Systems;52 5.2.1;Security;56
5.2.2;The Subset Cover Framework;61 5.3;The Key-Poset Framework for Broadcast Encryption;62
5.3.1;Viewing Set Systems as Partial Orders;62 5.3.2;Computational Specification of Set Systems;67
5.3.3;Compression of Key Material;68 5.4;Revocation in the Key-Poset Framework;72 5.4.1;Revocation
in the key-poset framework: Definitions;73 5.4.2;A sufficient condition for optimal revocation;76
5.5;Constructions;81 5.5.1;Complete Subtree;81 5.5.2;Subset Difference;86 5.5.3;Key Chain Tree;93
5.6;Generic Transformations for Key Posets;100 5.6.1;Layering Set Systems;101
5.6.2;X-Transformation;104 5.7;Bibliographic notes;113 6;3 Traitor Tracing;118 6.1;Multiuser Encryption
Schemes;118 6.2;Constructions For Multiuser Encryption Schemes;120 6.2.1;Linear Length Multiuser
Encryption Scheme;120 6.2.2;Multiuser Encryption Schemes Based on Fingerprinting Codes;123
6.2.3;Boneh-Franklin Multiuser Encryption Scheme;130 6.3;Tracing Game: Definitions;134 6.4;Types of
Tracing Games;137 6.4.1;Non-Black Box Tracing Game.;137 6.4.2;Black-Box Tracing Game.;138
6.5;Traceability of Multiuser Encryption Schemes;141 6.5.1;Traceability of Linear Length Multiuser
Encryption Scheme;141 6.5.2;Traceability of Schemes Based on Fingerprinting Codes;145
6.5.3;Traceability of the Boneh-Franklin Scheme;153 6.6;Bibliographic Notes;156 7;4 Trace and Revoke
Schemes;161 7.1;Revocation Game: Definitions;162 7.2;Tracing and Revoking in the Subset Cover
Framework;167 7.3;Tracing and Revoking Pirate Rebroadcasts;171 7.4;On the effectiveness of Trace
and Revoke schemes;176 7.5;Bibliographic Notes;177 8;5 Pirate Evolution;180 8.1;Pirate Evolution:
Definitions;181 8.2;A Trace and Revoke Scheme Immune to Pirate-Evolution;183 8.3;Pirate Evolution for
the Complete Subtree Method ;185 8.4;Pirate Evolution for the Subset Difference Method;191

8.5;Bibliographic Notes;205 9;References;207 10;Index;215 EAN/ISBN : 9781441900449 Publisher(s): Springer, Berlin, Springer Science & Business Media Discussed keywords: Kryptographie / Kryptologie
Format: ePub/PDF Author(s): Kiayias, Aggelos - Pehlivanlu, Serdar

[DOWNLOAD HERE](#)

Similar manuals: