Contents

Acknowledgment V

Abstract VII

1 Introduction 1

1.1 Digital Rights Management 1

1.1.1 Towards a Definition of DRM 2

1.1.2 “Traditional” DRM 3

1.1.3 Cloud Computing and Multiparty DRM 5

1.2 Privacy Protection 9

1.2.1 Privacy in the Cloud? 9

1.2.2 Privacy in DRM? 10

1.2.3 A Note on Business Secrecy 11

1.3 Research Gap and Contribution 11

1.4 Dissertation Outline 12

2 Terminology, Related Work, and Preliminaries 13

2.1 Terminology 13

2.2 Related Work 17

2.2.1 Digital Rights Management 18

2.2.2 Privacy-Enhancing Technologies 23

2.2.3 Systematization of Unlinkability 28

2.2.4 Conclusion of Related Work 32

2.3 Preliminaries 32

2.3.1 Ciphertext-Policy Attribute-Based Encryption 32

2.3.2 Proxy Re-Encryption 34

2.3.3 Additively Homomorphic Encryption 35

2.3.4 Anonymous Payment Scheme 36

2.3.5 Trusted Computing 39

3 System Model 41

3.1 Requirements to a PPM-DRM System 41

3.1.1 General DRM Requirements Analysis 41

3.1.2 Stakeholder and Incentive Determination 42

Bibliografische Informationen
http://d-nb.info/1051452929

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3.1.3 Requirements Determination for the proposed PPM-DRM System . . . 45
3.2 Security and Privacy in a Multiparty DRM System . . . 47
3.2.1 The Role of Trust . . . 47
3.2.2 Security and Privacy Model . . . 49
3.2.3 Security and Privacy Requirements . . . 50

4 Concept **55**
4.1 PPM-DRM System without a Trusted Third Party . . . 55
4.1.1 Revised System Model . . . 55
4.1.2 Protocol Description . . . 57
4.2 PPM-DRM System Based on Secure Hardware . . . 61
4.2.1 Revised System Model . . . 61
4.2.2 Protocol Description . . . 63
4.3 PPM-DRM System Based on a Semi-Trusted Third Party . . . 67
4.3.1 Approaches Based on Re-Encryption . . . 68
4.3.2 Approach Based on Trusted Computing . . . 77

5 Evaluation and Discussion **83**
5.1 Evaluation of the Proposed Approaches . . . 83
5.1.1 DRM Requirements . . . 83
5.2 Security and Privacy Discussion . . . 84
5.2.1 Evaluation Model for Unlinkability . . . 85
5.2.2 Approach without a TTP . . . 87
5.2.3 Approach Based on Secure Hardware . . . 91
5.2.4 Approaches Based on Re-Encryption . . . 94
5.2.5 Approach based on Trusted Computing . . . 98
5.3 Implementation Details . . . 99
5.3.1 Overhead Analysis . . . 99
5.3.2 Secure Hardware . . . 100
5.4 Integration into Application Scenarios . . . 101
5.4.1 On-The-Fly Computing . . . 101
5.4.2 State-of-the-art DRM Systems . . . 105
5.5 Comparison of My Approaches . . . 106
5.5.1 Supported Models . . . 108
5.5.2 Need for TTP . . . 108
5.5.3 Resistance to Collaboration Attacks . . . 108
5.5.4 Computation Overhead . . . 109
5.5.5 Communication Overhead . . . 109
5.5.6 Conclusion: Proposed Approaches . . . 110
5.6 Comparison to Related Work . . . 110
5.6.1 Need for TTP . . . 110
5.6.2 Need for Trusted Hardware . . . 112
5.6.3 Flexibility in Choosing a Rights Model . . . 112

5.6.4 Unlinkability of Content Purchases 112
5.6.5 Unlinkability of Content Executions 113
5.6.6 Resistance against Collaboration Attacks 113
5.6.7 Flexibility in Choosing a Content Execution Center 114
5.6.8 Conclusion: Comparison to Related Work 114

6 Conclusion and Outlook **115**

A Cryptography Background, Proofs, and Further Analysis **117**
A.1 CPA Security 117
A.2 Distribution of the Temporary User's Public Key 117
A.3 Randomized Re-Encryption Security 117
A.4 Further Overhead Analysis 119
A.4.1 Supported Models 119
A.4.2 Need for TTP 119
A.4.3 Resistance to Collaboration Attacks 119
A.4.4 Computation Overhead 120
A.4.5 Communication Overhead 120

List of Figures **IX**

List of Tables **XI**

List of Definitions **XIII**

List of Listings **XV**

Acronyms **XVII**

Bibliography **XIX**