

# **Privacy-Preserving Multiparty Digital Rights Management**

**Ronald Petrlic, M.Sc.**

Dissertation

accepted by the

*Faculty of Computer Science, Electrical Engineering, and Mathematics*

**University of Paderborn**

in partial fulfillment of the requirements for the degree of

Doctor rerum naturalium (Dr. rer. nat.)

May 2014

**Dissertation Place:**

University of Paderborn, Germany

**Reviewers:**

Prof. Dr. Christoph Sorge, Saarland University; formerly University of Paderborn

Prof. Dr. Dirk Westhoff, Hochschule Furtwangen University

Berichte aus der Informatik

**Ronald Petrlic**

**Privacy-Preserving Multiparty  
Digital Rights Management**

D 466 (Diss. Universität Paderborn)

Shaker Verlag  
Aachen 2014

**Bibliographic information published by the Deutsche Nationalbibliothek**

The Deutsche Nationalbibliothek lists this publication in the Deutsche

Nationalbibliografie; detailed bibliographic data are available in the Internet at

<http://dnb.d-nb.de>.

Zugl.: Paderborn, Univ., Diss., 2014

Copyright Shaker Verlag 2014

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 978-3-8440-2830-0

ISSN 0945-0807

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen

Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9

Internet: [www.shaker.de](http://www.shaker.de) • e-mail: [info@shaker.de](mailto:info@shaker.de)

# Contents

<b>Acknowledgment</b>	<b>V</b>
<b>Abstract</b>	<b>VII</b>
<b>1 Introduction</b>	<b>1</b>
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
<b>2 Terminology, Related Work, and Preliminaries</b>	<b>13</b>
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
<b>3 System Model</b>	<b>41</b>
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

## *Contents*

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
<b>4</b>	<b>Concept</b>	<b>55</b>
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
<b>5</b>	<b>Evaluation and Discussion</b>	<b>83</b>
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
<b>6</b>	<b>Conclusion and Outlook</b>	<b>115</b>
<b>A</b>	<b>Cryptography Background, Proofs, and Further Analysis</b>	<b>117</b>
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
<b>List of Figures</b>		<b>IX</b>
<b>List of Tables</b>		<b>XI</b>
<b>List of Definitions</b>		<b>XIII</b>
<b>List of Listings</b>		<b>XV</b>
<b>Acronyms</b>		<b>XVII</b>
<b>Bibliography</b>		<b>XIX</b>
		<b>III</b>

