

Table of Contents

ACM DRM 2002

A White-Box DES Implementation for DRM Applications	1
<i>Stanley Chow, Phil Eisen, Harold Johnson (Cloakware Corporation), and Paul C. van Oorschot (Carleton University)</i>	
Attacking an Obfuscated Cipher by Injecting Faults	16
<i>Matthias Jacob (Princeton University), Dan Boneh (Stanford University), and Edward Felten (Princeton University)</i>	
Breaking and Repairing Asymmetric Public-Key Traitor Tracing	32
<i>Aggelos Kiayias (University of Connecticut) and Moti Yung (Columbia University)</i>	
Key Challenges in DRM: An Industry Perspective	51
<i>Brian A. LaMacchia (Microsoft Corporation)</i>	
Public Key Broadcast Encryption for Stateless Receivers	61
<i>Yevgeniy Dodis and Nelly Fazio (New York University)</i>	
Traitor Tracing for Shortened and Corrupted Fingerprints	81
<i>Reihaneh Safavi-Naini and Yejing Wang (University of Wollongong)</i>	
Evaluating New Copy-Prevention Techniques for Audio CDs	101
<i>John A. Halderman (Princeton University)</i>	
Towards Meeting the Privacy Challenge: Adapting DRM	118
<i>Larry Korba (National Research Council of Canada) and Steve Kenny (Independent Consultant)</i>	
Implementing Copyright Limitations in Rights Expression Languages	137
<i>Deirdre Mulligan and Aaron Burstein (University of California)</i>	
The Darknet and the Future of Content Protection	155
<i>Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman (Microsoft Corporation)</i>	
Replacement Attack on Arbitrary Watermarking Systems	177
<i>Darko Kirovski and Fabien A.P. Petitcolas (Microsoft Research)</i>	
FAIR: Fair Audience InfeRence	190
<i>Rob Johnson (University of California) and Jessica Staddon (Palo Alto Research Center)</i>	

Theft-Protected Proprietary Certificates 208
Alexandra Boldyreva (University of California)
and Markus Jakobsson (RSA Laboratories)

Author Index 221



<http://www.springer.com/978-3-540-40410-1>

Digital Rights Management

ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA,

November 18, 2002, Revised Papers

Feigenbaum, J. (Ed.)

2003, X, 222 p., Softcover

ISBN: 978-3-540-40410-1