# Table of Contents

## ACM DRM 2002

A White-Box DES Implementation for DRM Applications .......................... 1  
*Stanley Chow, Phil Eisen, Harold Johnson (Cloakware Corporation),  
and Paul C. van Oorschot (Carleton University)*

Attacking an Obfuscated Cipher by Injecting Faults ............................. 16  
*Mathias Jacob (Princeton University), Dan Boneh  
(Stanford University), and Edward Felten (Princeton University)*

Breaking and Repairing Asymmetric Public-Key Traitor Tracing .......... 32  
*Aggelos Kiayias (University of Connecticut)  
and Moti Yung (Columbia University)*

Key Challenges in DRM: An Industry Perspective ............................ 51  
*Brian A. LaMacchia (Microsoft Corporation)*

Public Key Broadcast Encryption for Stateless Receivers ........................ 61  
*Yevgeny Dodis and Nelly Fazio (New York University)*

Traitor Tracing for Shortened and Corrupted Fingerprints ..................... 81  
*Reihaneh Safavi-Naini and Yejing Wang (University of Wollongong)*

Evaluating New Copy-Prevention Techniques for Audio CDs .................... 101  
*John A. Halderman (Princeton University)*

Towards Meeting the Privacy Challenge: Adapting DRM ....................... 118  
*Larry Korba (National Research Council of Canada)  
and Steve Kenny (Independent Consultant)*

Implementing Copyright Limitations in Rights Expression Languages ...... 137  
*Deirdre Mulligan and Aaron Burstein (University of California)*

The Darknet and the Future of Content Protection ............................ 155  
*Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman  
(Microsoft Corporation)*

Replacement Attack on Arbitrary Watermarking Systems ...................... 177  
*Darko Kirovski and Fabien A.P. Petitcolas (Microsoft Research)*

FAIR: Fair Audience InfeRence .................................................. 190  
*Rob Johnson (University of California)  
and Jessica Staddon (Palo Alto Research Center)*
Theft-Protected Proprietary Certificates ........................................ 208
Alexandra Boldyreva (University of California)
and Markus Jakobsson (RSA Laboratories)

Author Index ................................................................. 221