International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **12**, December **2010**

 ISSN 1349-4198
pp. 5657–5664

LIGHTWEIGHT KEY MANAGEMENT OF DRM SYSTEMS

Tzung-Her Chen, Tsung-Hao Hung and Yan-Ting Wu

Department of Computer Science and Information Engineering
National Chiayi University
Chiayi City 60004, Taiwan
thchen@mail.ncyu.edu.tw

Received June 2009; revised October 2009

Abstract. *In the past decade, digital rights management's (DRM) goal of helping creators of digital content protect their intellectual property has captured the attention of both academia and industry. The DRM concept has emerged as a blanket term for copyright protection, ownership assertion, digital content authentication, access control and so on. Many corporations, such as Microsoft and Apple, have developed their own DRM systems; however, certain trust relationships are central to their success, especially the content owner's trust in the license server, but such trust is not always justified. This paper first addresses the security problem related to collusion attacks in the approach proposed by Jeong et al. Then it presents an efficient and secure key-delivery scheme in a DRM system based on the realistic assumption that the license server may be tempted by extra profit from illegal distribution. The proposed method's main contributions include 1): reducing the threat of collusion attacks by preventing the license server from obtaining a complete content-encryption key; 2): lower computational costs without the need for a public key infrastructure; 3): easy implementation in lightweight mobile devices.*
Keywords: Digital rights management, Copyright protection, Key management, Mobile device

1. **Introduction.** Online music shops having overtaken traditional audio CD distribution have been both a blessing and a curse. While they provide a flexible way of transporting and consuming digital content, they also make unauthorized transport of digital content easier. Digital content has been characterized as high quality and easy to copy, manage and distribute, and it is because of these characteristics that digital rights management (DRM) systems have emerged to help music creators and providers forestall illegal use of digital content.

Some software based on peer-to-peer architecture over the Internet, such as BitTorrent [2], e-mule [8] and Foxy [9], can help users distribute digital content simply by clicking a mouse. Absent any protection mechanism, users can distribute an illegal copy through peer-to-peer software freely, and this illegal activity impacts the financial objectives of media companies, as well as the content creator's ability to be supported directly by either media companies or customers.

DRM systems [15,16] protect digital content from illegal access by allowing users access only when they satisfy the conditions set by the provider under the DRM system. A secret key is generally necessary in the DRM system, as it is in encryption, authentication and watermarking, so key management [4,11] is critical to security. While DRM systems do not always succeed in protecting digital content, the well known Content Scrambling System (CSS), which was developed to protect the digital content stored on DVDs [3,5,21],

This work was presented in part at 2007 Electronic Commerce and Digital Life (ECDL2007), Taiwan, March 17, 2007.