

研发、设计、测试

版权保护系统的安全水印协议设计

任旭峰¹, 张贵仓¹, 张旭²

1.西北师范大学 数学与信息科学学院, 兰州 730070

2.中国人民解放军炮兵学院, 合肥 230031

收稿日期 2008-5-16 修回日期 2008-8-21 网络版发布日期 2008-11-28 接受日期

摘要 根据安全威胁分析和利用水印技术和密码技术, 研究对象是版权保护系统的安全协议设计。在协议设计上引入认证机制、时间戳机制和可信第三方的公钥跟踪机制以及多播机制, 设计了一个安全可靠的版权保护协议, 避免了现有协议的缺陷, 实验证明本协议满足版权所有者和购买者的应用需求, 可以抵抗现有的协议层安全隐患, 并对其性能做出分析, 说明了其实际可行性。

关键词 [版权保护](#) [数字水印](#) [协议设计](#) [协议攻击](#) [协议层安全](#)

分类号

Design for secure protocol of digital right management

REN Xu-feng¹, ZHANG Gui-cang¹, ZHANG Xu²

1.College of Mathematics and Information, Northwest Normal University, Lanzhou 730070, China

2.Artillery Academy of PLA of China, Hefei 230031, China

Abstract

Based on the analysis of security threat and using watermarking technology and encryption technology, a protocol security model of copyright marking system is proposed. Through protocol mechanism with digital watermarking technology, the proposed protocol security model can resistant to the protocol attack effectively, and protects not only the benefit of the copyright owners but also the benefit of the purchasers. The design of the protocol security model reflects the effectiveness and the convenience of making use of protocol techniques to counteract protocol attacks.

Key words [digital rights management](#) [digital watermarking](#) [protocol design](#) [protocol attacks](#) [protocol layer security](#)

DOI: 10.3778/j.issn.1002-8331.2008.34.021

通讯作者 任旭峰 renxuf@163.com

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(589KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [复制索引](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“版权保护” 的相关文章](#)

▶ 本文作者相关文章

· [任旭峰](#)

· [张贵仓](#)

· [张旭](#)