



多播水印协议MAMWP的BAN逻辑分析

陆正福, 叶锐, 王国栋

云南大学, 数学系, 云南, 昆明, 650091

BAN logic analysis of MAMWP protocol

LU Zheng-fu, YE Rui, WANG Guo-dong

Department of Mathematics, Yunnan University, Kunming 650091, China

- [摘要](#)
- [参考文献](#)
- [相关文章](#)

全文: [PDF \(538 KB\)](#) [HTML \(KB\)](#) 输出: [BibTeX](#) | [EndNote \(RIS\)](#) [背景资料](#)

摘要 用形式化的方法分析密码协议可以检测出协议中的漏洞和证明协议的安全性,BAN类逻辑是目前使用最广泛的一种形式化分析密码协议的方法.文章介绍了基于移动代理的多播水印协议MAMWP和BAN逻辑,并给出了用BAN逻辑分析MAMWP协议的详细过程.

关键词: [多播水印协议](#) [BAN类逻辑](#) [移动代理](#) [数字水印](#) [数字指纹](#)

Abstract: Formal methods can be useful to detect errors and prove security in cryptographic protocols.BAN-like logic has been the most widely used formal method by far.It is discussed the MAMWP protocol and BAN logic,and discribed a process of analysis of MAMWP protocol using BAN logic.

Key words: [multicast watermarking protocol](#) [BAN-like logic](#) [mobile agent](#) [watermarking](#) [fingerprinting](#)

收稿日期: 2004-03-17;

基金资助: 云南省自然科学基金资助项目(2002F0012M); 云南大学理(工)科校级科研项目资助(2003Z010C)

引用本文:

陆正福,叶锐,王国栋. 多播水印协议MAMWP的BAN逻辑分析[J]. 云南大学学报(自然科学版), 2005, 27(1): 18-21.

LU Zheng-fu, YE Rui, WANG Guo-dong. BAN logic analysis of MAMWP protocol[J]. , 2005, 27(1): 18-21.

没有本文参考文献

没有找到本文相关文献

服务

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [E-mail Alert](#)
- ▶ [RSS](#)

作者相关文章

- ▶ [陆正福](#)
- ▶ [叶锐](#)
- ▶ [王国栋](#)

版权所有 © 《云南大学学报(自然科学版)》编辑部

编辑出版：云南大学学报编辑部（昆明市翠湖北路2号，650091）

电话：0871-5033829(传真) 5031498 5031662 E-mail: yndxxb@ynu.edu.cn yndxxb@163.com