

博士论文

一种可分析保密性与认证性的模态逻辑

赵华伟¹, 秦 静²

(1. 山东财政学院计算机信息工程学院, 济南250014; 2. 山东大学数学与系统科学学院, 济南250100)

收稿日期 修回日期 网络版发布日期 2007-10-11 接受日期

摘要 提出了一种新的基于信念的模态逻辑——MBL逻辑, 来分析由单向函数构造的对称钥认证交换协议的安全性。该逻辑有严格的证明体系, 可证明推理规则在其语义模型下的正确性, 说明该逻辑具有合理性。其推理规则不仅能对单向函数保护的消息进行有关认证性的推理, 克服了以往逻辑系统使用不当的安全服务来分析协议认证性的缺陷, 而且可分析消息的保密性, 避免了其他逻辑分析协议时对可信中心的过分依赖, 可发现敌手通过欺骗可信中心而造成的攻击。

关键词 [模态逻辑](#); [MBL逻辑](#); [BAN类逻辑](#); [会话密钥](#)

分类号 [TP309](#)

DOI:

对应的英文版文章: [072015](#)

通讯作者:

作者个人主页: [赵华伟¹](#); [秦 静²](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (250KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [参考文献\[PDF\]](#)

▶ [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](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“模态逻辑; MBL逻辑; BAN类逻辑; 会话密钥”的 相关文章](#)

▶ 本文作者相关文章

· [赵华伟](#)

· [秦 静](#)