

软件技术与数据库

一种安全协议的形式化分析方法

王 昕, 袁超伟

(北京邮电大学信息与通信工程学院, 北京 100876)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 对快速、高效的形式化分析安全协议进行研究, 提出“信任域”的概念。采用与图形化相结合的分析方法, 使得协议流程的推导过程清晰、直观。该方法直接分析协议参与主体的信任域, 简化分析过程和步骤。实验结果表明, 与传统方法相比, 该方法更快速、直观, 并能为分析协议的冗余性提供具体方法和依据。

关键词 [形式化分析](#); [安全协议](#); [BAN逻辑](#); [NSSK协议](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: [王 昕](#); [袁超伟](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (306KB)
- ▶ [\[HTML全文\]](#) (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“形式化分析; 安全协议; BAN逻辑; NSSK协议”的 相关文章](#)
- ▶ [本文作者相关文章](#)