

信息与网络安全

一种入侵容忍的广播通讯KDC方案

商建伟<sup>1</sup>;李锋<sup>1</sup>;张燕燕<sup>2</sup>

山东大学网络信息安全研究所<sup>1</sup>

山东政法学院 司法信息系<sup>2</sup>

收稿日期 2006-11-30 修回日期 网络版发布日期 2007-4-27 接受日期

**摘要** 在使用密钥管理中心(KDC)进行广播通讯密钥分配的网络安全协议中,保证KDC的安全并提供高效率的密钥服务是一个非常重要的课题。区别于目前的域分割和服务器备份方案,使用双变量多项式作为门限构造函数,在多个分布式KDC服务器上分发不同的伪随机数产生函数,需要特定数目的授权服务器联合才能计算出最终的对称密钥,保证少于一定数目的KDC服务器被攻击后不能对系统产生威胁,从而保证了分布式KDC的安全性,并且能够避免广播通讯密钥分配过程中的效率瓶颈和单点失败。

**关键词** [密钥管理中心](#) [伪随机数产生函数](#) [分布式](#) [入侵容忍](#) [对称密钥](#)

分类号

**DOI:**

对应的英文版文章: [6117437](#)

通讯作者:

商建伟 [shangjw@yahoo.com.cn](mailto:shangjw@yahoo.com.cn); [shangjw\\_007@163.com](mailto:shangjw_007@163.com)

作者个人主页: 商建伟 李锋 张燕燕

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF \(805KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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“密钥管理中心”的  
相关文章](#)

▶ [本文作者相关文章](#)

· [商建伟](#)

· [李锋](#)

· [张燕燕](#)