

安全技术

UMTS系统鉴权和密钥分配机制的改进

叶敦范, 宁涛

(中国地质大学机械与电子工程学院, 武汉 430074)

收稿日期 修回日期 网络版发布日期 2008-4-14 接受日期

摘要 为防止用户的永久身份信息不被窃取, 研究第三代移动通信系统的安全结构。通过对UMTS系统接入安全机制, 即鉴权和密钥分配机制进行分析, 提出一种终端用户安全鉴权的方案。利用USIM对鉴权随机参数RAND进行验证, 如果验证失败则给出错误的鉴权结果, 反之给出正确的鉴权结果。该方案能最大限度地保证用户的身份信息不被监听窃取, 同时提高身份的机密性, 且实施周期短。

关键词 [鉴权; 随机数RAND; 密钥; 安全](#)

分类号 [TP393.08](#)

DOI:

对应的英文版文章: [080865B](#)

通讯作者:

作者个人主页: 叶敦范; 宁涛

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(74KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“鉴权; 随机数RAND; 密钥; 安全”的 相关文章](#)
- ▶ 本文作者相关文章
 - [叶敦范](#)
 - [宁涛](#)