

信息安全

基于椭圆曲线密码体制的CDMA网络鉴权设计

李彬, 郝克刚

收稿日期 修回日期 网络版发布日期 接受日期

摘要 由于我国并未掌握蜂窝鉴权与语音加密算法(CAVE)的实现,使得CDMA网络并未实现真正的安全。提出了一种基于椭圆曲线的CDMA网络鉴权方案,通过公钥签名机制完成对用户身份的识别和管理。与CAVE算法相比,该方案除具备自主知识产权外,还减轻了鉴权中心的负担。最后通过实验证明这种鉴权方案是完全可行的。

Abstract

关键词

Key words

分类号

DOI:

通讯作者:

作者个人主页: 李彬;郝克刚

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (538KB)

▶ [\[HTML全文\]](#) (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 无 相关文章](#)

▶ 本文作者相关文章

· [李彬](#)

· [郝克刚](#)