通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

马 骏,马建峰,郭渊博.可证明安全的智能移动终端私钥保护方案[J].通信学报,2012,(12):108~115

可证明安全的智能移动终端私钥保护方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
马 骏	
马建峰	
郭渊博	

中文摘要：

提出一种可证明安全的智能移动终端私钥保护方案。充分利用口令保护、密钥分割与服务器动态交互获取部分私钥等技术保证用户私钥安全。与其他方案相比，该方案的优势在于：减少了智能移动终端的计算量和存储量，简化了交互过程参数的设置；将时间同步贯穿整个方案的设计过程，防止重放攻击的同时，更提供了便捷高效的用户私钥失效方案。方案达到了安全私钥获取和高效私钥失效的效果，符合智能移动终端的安全应用需求，在随机预言机模型下是可证明安全的。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭