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

舒剑,许春香.基于口令的认证密钥协商协议的安全分析与改进[J].通信学报,2010,(3):51~56

基于口令的认证密钥协商协议的安全分析与改进

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
舒剑	
许春香	

中文摘要：

对基于口令的标准模型下可证明安全的认证密钥协商协议进行安全分析，指出该协议易受反射攻击。同时给出了一个改进方案，该方案不仅弥补了原方案的缺陷，而且改善了协议的性能。最后，基于DDH假设，在标准模型下证明了协议的安全性。结果表明，改进后的协议还具有完美前向安全特性。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭