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

刘亚丽,秦小麟,殷新春.基于模m的n方根的前向安全数字签名方案的分析与改进[J].通信学报,2010,(6):82~88

基于模m的n方根的前向安全数字签名方案的分析与改进

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
刘亚丽	
秦小麟	
殷新春	

中文摘要：

前向安全在实际应用中起着有效减少因签名密钥泄露而带来损失的重要作用，在密码学研究中成为热点。针对基于模m的n方根难题的前向安全数字签名方案进行了详细的安全性分析，发现此类方案均存在安全隐患，不具备前向安全性，并总结出前向安全数字签名方案攻击者成功伪造有效签名的本质原因。同时，根据有限域上数字签名所基于的困难性问题，通过利用与当前私钥有关的信息进行签名的方法对其中一种前向安全数字签名方案进行了改进。详细的安全性和效率分析表明，改进方案具有前向安全性和抗伪造性，有效地提高了签名的速度。改进方法也同样适用于此类基于模m的n方根难题的其他签名方案，对于进一步设计前向安全代理签名、前向安全群签名、前向安全多重签名等一些特殊数字签名方案具有指导意义。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭