电子科技大学学报
Journal of University of Electronic Science and Technology of China

基于身份的强指定验证者签名的安全分析

作者：秦志光，廖永建

关键词：攻击; 授权; 指定验证者签名; 代理签名

摘要

针对基于身份的强指定验证者签名方案是不可授权的结论和基于身份的指定验证者代理签名方案设计，对两个方案进行安全性分析，首先证明了基于身份的指定验证者方案的签名是可授权的，然后证明了基于身份的指定验证者代理签名方案的签名是可伪造的，说明基于身份的强指定验证者签名方案的结论是不安全的；而基于身份的指定验证者代理签名方案的设计是不合理的。