计算机工程　2007 33 (22): 21-22　ISSN: 1000-3428　CN: 31-1289/TP

博士论文

两个可证安全短签名方案的密码学分析

明 洋，王育民

（西安电子科技大学综合业务网络国家重点实验室，西安 710071）

收稿日期　修回日期　网络版发布日期 2007-11-16　接受日期

摘要　随机预言机模型下的可证明安全性不能保证数字签名方案在具体实现时的安全性，因此在标准模型下的可证明安全的数字签名方案更具有吸引力。针对在标准模型下可证安全的两个短签名方案，该文指出这两个方案在多用户环境下是不安全的，不能抵抗密钥替换攻击，即一个攻击者能够生成一个新公钥满足合法签名者生成的合法签名。

关键词　密钥替换攻击；短签名；双线性对

分类号　TP918.1

DOI:

对应的英文版文章：072206

通讯作者：

作者个人主页：明 洋;王育民