计算机工程　2008 34 (1): 156-157　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于ECC的组合公钥技术的安全性分析

赵美玲，张少武

(信息工程大学电子技术学院，郑州 450004)

收稿日期　修回日期　网络版发布日期 2007-12-28　接受日期

摘要　分析了唐文等人提出的一种基于ECC(椭圆曲线密码体制)的组合公钥技术的安全性特点，给出了两种合谋攻击的方法。第1种方法称之为选择合谋攻击，一个用户与其选择的具有某些映射特点的w(2)个用户合谋，可以得到2w-w-1个不同用户的私钥。第2种方法称之为随机合谋攻击，两个合谋用户首先计算其公钥的差值 和 ，然后在公开的公钥因子矩阵中任意选取组合公钥，通过计算所选取的公钥与两个合谋用户之一的公钥的差值是否等于 或 ，从而达到攻击的目标。

关键词　公钥密码；私钥；椭圆曲线

分类号　TP309

DOI:

对应的英文版文章：01-56c

通讯作者:

作者个人主页: 赵美玲;张少武