计算机工程　2007 33 (14): 125-127　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

Smartcard上椭圆曲线密码算法的能量攻击和防御

张 涛，范明钰，王光卫，鲁晓军

(电子科技大学计算机科学与工程学院，成都 610054)

收稿日期　修回日期　网络版发布日期 2007-7-17　接受日期

摘要　能量攻击是一种新的密码攻击方法，其密钥搜索空间要远小于传统的数学分析方法。该文介绍了目前对椭圆曲线密码系统能量攻击的几种攻击方法，提出了一种基于Width-w NAF的改进算法RWNAF(Refined Width-w NAF)，该算法通过Masking技术隐藏密码算法的真实能量消耗信息，能有效地防御SPA、DPA、RPA与ZPA攻击；通过对密钥d的奇偶性分析，对预计算表进行优化，减少了存储需求和计算开销。RWNAF与Mamiya提出的WBRIP算法相比，具有相同的抗能量攻击能力，但在计算开销与存储开销上均优于WBRIP方法。

关键词　能量攻击；椭圆曲线密码系统；Smartcard

分类号　TP301.6

DOI:

对应的英文版文章：071443

通讯作者:

作者个人主页: 张 涛;范明钰;王光卫;鲁晓军