计算机工程 2010 36 (2): 127-129 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

不可能差分攻击中的明文对筛选方法

张庆贵

(解放军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 接受日期

摘要 基于快速排序原理，提出用于筛选明文对的基本算法和改进算法，改进算法的计算复杂性可以将由直接检测方法的O(n2)降为O(nlogn)。基于上述结果以改进算法分析对ARIA等分组密码算法的几个不可能攻击的计算复杂性，证明ICISA2008上发表的某个针对对ARIA的不可能攻击的数据筛选过程的计算复杂性远高于密钥求解过程的计算复杂性。

关键词 密码学；密码分析；不可能差分攻击；明文对筛选；计算复杂性；ARIA算法

分类号 TN918.1

DOI:

通讯作者:

作者个人主页: 张庆贵