计算机工程 2010 36 (2): 1-3 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期 下一期

博士论文

基于DNA计算的RSA密码系统攻击方法

杨学庆1,2，柳重堪1,2

(1. 北京航空航天大学数学、信息与行为教育部重点实验室，北京 100083；2. 北京航空航天大学电子信息工程学院，北京 100083)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对RSA公钥密码体制的陷门库特点，提出一种新的DNA计算模型：并类计算模型，阐述基于该模型的RSA密码系统的攻击方法。该方法采用DNA分子编码陷门库与公钥，通过组合、设置、分离、清除等操作筛选出陷门，由电泳确定陷门的值，再用陷门计算私钥的值。该方法所需的时间复杂度为O(1bn)3，DNA分子的体积不超过1 m3。

关键词 DNA计算；RSA公钥密码；并类计算模型

分类号 TP309

DOI:

通讯作者:

作者个人主页: 杨学庆1;2;柳重堪1;2