计算机工程 2007 33 (12): 191-192,204 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

针对RSA快速实现算法的计时攻击

张 鹏，陈开颜，赵 强

(军械工程学院计算机工程系，石家庄 050003)

收稿日期 修回日期 网络版发布日期 2007-6-15 接受日期

摘要 给出了一种改进的计时攻击方法。针对采用Montgomery模指数运算和中国剩余定理的RSA快速实现算法，通过分析在Montgomery模指数运算中额外约简发生的概率，得到RSA输入参数与运行时间之间的关系，并通过选择密文输入，计时分析按位获取RSA的秘密因子，最终破解了RSA的因子分解。

关键词 RSA 计时攻击 Montgomery约简 中国剩余定理 额外约简

分类号 TN918

DOI:

对应的英文版文章:58

通讯作者:

作者个人主页: 张 鹏;陈开颜;赵 强