计算机工程　2010 36 (1): 177-180　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

冗余方程对基于Minisat的代数攻击影响

卜 凡

(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　分析基于Minisat软件的代数攻击方法，发现由该代数攻击方法对某些密码算法所建立的方程组中存在冗余方程，研究去除所有冗余方程的预处理方法，基于该方法提出先去除冗余方程，再利用Minisat软件求解无冗余方程组的代数攻击方法。实验结果表明，对CTC算法，新的攻击方法的攻击时间平均缩短了1/2，冗余方程的存在降低了基于Minisat软件的代数攻击的效率。

关键词　代数攻击；非线性方程组；冗余方程；CTC算法

分类号　TN918.1

DOI:

通讯作者:

作者个人主页: 卜 凡