计算机工程 2010 36 (06): 128-130 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

针对低轮PRESENT的代数攻击

卜 凡，金晨辉

(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MiniSAT 2.0软件，研究对低轮PRESENT的代数攻击问题。提出将S盒表示为单项式个数较少的无冗余等效方程组的方法，将PRESENT的S盒表示为由14个单项式个数均≤6的8元布尔方程构成的等效方程组，并基于不同的已知明文量，利用MiniSAT软件对PRESENT进行代数攻击实验，获得了较好的攻击效果。实验表明，在已知明文条件下可以在121 h内求出80 bit密钥的5轮PRESENT的全部密钥比特，在选择明文条件下可以在203 h内求出6轮PRESENT的全部密钥比特。

关键词 代数攻击；MiniSAT软件；等效方程组；无冗余方程组；PRESENT算法

分类号 TN918.1

DOI:

通讯作者:

作者个人主页: 卜 凡;金晨辉