电子科技大学学报
Journal of University of Electronic Science and Technology of China

布尔函数的代数攻击

作者：杨文峰，胡予濮，高军涛

关键词：代数方法; 布尔函数; 密码分析; 密码学

摘要

基于代数攻击，提出了一种已知部分真值表还原整个布尔函数的方法。对于n元d次布尔函数, 该方法的空间复杂度和数据复杂度均为$O(N)$，计算复杂度为$O(N^3)$，其中。由复杂度可知，所求密码函数的代数次数越低，该方法的有效性越高。攻击方法表明密码设计中应该谨慎使用代数次数较低的布尔函数。

请点击下载（右键另存为）或浏览:UESTC20100606.pdf