电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2010, Vol. 32 » Issue (10) :2521-2525 DOI: 10.3724/SP.J.1146.2010.00191

研究简报

bent函数和半bent函数的二阶非线性度下界

李雪莲① 胡予濮② 高军涛②*

①(西安电子科技大学应用数学系 西安 710071)
②(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

The Lower Bounds on the Second Order Nonlinearity of Bent Functions and Semi-bent Functions

Li Xue-lian① Hu Yu-pu② Gao Jun-tao②*

①(Department of Applied Mathematics, Xidian University, Xi' an 710071, China)
②(Key Laboratory of Computer networks & Information Security, Xidian University, Xi' an 710071, China)

摘要 | 参考文献 | 相关文章

Download: PDF (232KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘 要 该文研究了形如$f(x,y)$的$n+1$变元bent函数和半bent函数的二阶非线性度，其中$x\in GF(2^n)$, $y\in GF(2)$。首先给出了$f(x,y)$的2^n-1个导数非线性度的精确值；然后推导出了函数$f(x,y)$的其余2^n个导数的非线性度紧下界。进而给出了$f(x,y)$的二阶非线性度的紧下界。通过比较可知所得下界要优于现有的一般结论。结果表明$f(x,y)$具有较高的二阶非线性度，可以抵抗二次函数逼近和仿射逼近攻击。

关键词： 密码学 布尔函数 Walsh变换 非线性度

Abstract: This paper studies the lower bounds on the second order nonlinearity of bent functions and semi-bent functions $f(x,y)$ with $n+1$ variables, where $x\in GF(2^n)$, $y\in GF(2)$. Firstly, the values of the nonlinearity of the 2^n-1 derivatives of the Boolean function $f(x,y)$ are given. Then, the tight lower bounds on the other 2^n derivatives of $f(x,y)$ are deduced. Furthermore, the tight lower bounds on the second order nonlinearity of $f(x,y)$ are presented. The derived bounds are better than the existing general ones. The results show that these functions $f(x,y)$ have higher second order nonlinearity, and can resist the quardratic and affine approximation attacks.

Keywords: Cryptography Boolean functions Walsh transforms Nonlinearity

Received 2010-03-04;

本文基金:

国家973计划项目(2007CB311201)，国家自然科学基金项目(60833008，60803149)和广西信息与通讯技术重点实验室基金(20902)资助课题.

通讯作者: 李雪莲 Email: xuelian202@163.com

引用本文:
李雪莲, 胡予濮, 高军涛.bent函数和半bent函数的二阶非线性度下界[J] 电子与信息学报, 2010,V32(10): 2521-2525

Li Xue-Lian, Hu Yu-Pu, Gao Jun-Tao.The Lower Bounds on the Second Order Nonlinearity of Bent Functions and Semi-bent Functions[J] , 2010,V32(10): 2521-2525

链接本文:
http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2010.00191 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I10/2521