电子与信息学报 2005 27 (5): 699-702 ISSN: 1009-5896 CN: 11-4494/TN

论文

满足*k*阶PC(*l*)的密码函数的新构造

韦永壮[①②], 高军涛[①], 胡子濮[①]

[①]西安电子科技大学ISN国家重点实验室信息保密研究所 西安 710071;[②]桂林电子工业学院通信与信息工程系 桂林 541004

收稿日期 2003-5-31 修回日期 2003-9-11 网络版发布日期 2008-4-9 接受日期

摘要
该文基于线性分组码和双射函数, 给出了满足*k*阶PC(*l*)的均衡相关免疫布尔函数新的构造方法。并据此进一步给出满足*k*阶PC(*l*)的(*n*,*m*, *t*)弹性函数的一般构造方法。此外, 该文还揭示了这些函数的其它良好的密码学性质, 如较高的非线性度、良好的代数次数、良好的构造计数等。

关键词 弹性函数 扩散性 线性码 双射函数

分类号 TN918.1

New Construction of Cryptographic Functions Satisfying PC(*l*) of Order *k*

Wei Yong-zhuang[①②], Gao Jun-tao[①], Hu Yu-pu[①]

Information Security & Privacy Institute ISN National Key Lab., Xidan University Xi’an 710071 China; [②]Dept of Comm. And Info. Eng., Guilin Univ. of Electronic Tech., Guilin 541004 China

Abstract
In this paper, a new generalized construction method for correlation immune Boolean function satisfying PC(*l*) of order *k* is provided. The construction is based on the use of linear error-correcting codes together with bijective functions. Furthermore, some new construction methods for (*n* , *m* , *t*) resilient functions satisfying PC(*l*) of order *k* is also discussed. In addition, the authors also show that these functions have many other good cryptographic properties such as high nonlinearity, good algebraic degree and so on .

Key words Resilient functions Propagation Characteristics（PC） Linear code Bijective functions

DOI:

通讯作者

作者个人主页 韦永壮[①②]; 高军涛[①]; 胡子濮[①]