计算机工程　2010 36 (1): 164-165,169　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

GF(2)上周期为2pn序列的m(s)

赵 峰1,2，冯金磊2

(1.安徽工业大学管理科学与工程学院，马鞍山243002；2. 安徽工业大学计算机学院，马鞍山243002)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　给出多项式的若干引理，并对引理进行证明。在此基础上，给出GF(2)上周期序列线性复杂度的表达形式，应用该表达式得出周期N=2pn的二元序列线性复杂度和m(s)之间的关系，其中p是个奇素数，并且2是一个模p2的本源根。结合魏算法，给出2个实例进行证明，结果表明该结果的正确性。

关键词　密码；流密码；线性复杂度；最小多项式

分类号　TP309.2

DOI:

通讯作者:

作者个人主页: 赵 峰1;2;冯金磊2