

安全技术

GF(2)上周期为 $2pn$ 序列的 $m(s)$

赵 峰<sup>1,2</sup>, 冯金磊<sup>2</sup>

(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 $p^2$ 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<sup>1,2</sup>;冯金磊<sup>2</sup>

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (272KB)
- ▶ [\[HTML全文\]](#) (0KB)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“密码; 流密码; 线性复杂度; 最小多项式”的 相关文章](#)
- ▶ [本文作者相关文章](#)