西安电子科技大学学报 2008 35 (4): 759-763 ISSN: 1001-2400 CN: 61-1076/TN

求GF(p^m)上周期为kn的序列线性复杂度的快速算法

戴小平, 周建钦

(安徽工业大学 计算机学院， 安徽 马鞍山 243002)

收稿日期 2007-7-9 修回日期 网络版发布日期 2008-7-4 接受日期

摘要 提出和证明了求GF(p^m)上周期为kn的序列线性复杂度和极小多项式的一个快速算法， 其中p是素数， gcd(n， p^m-1)=1且p^m-1=kt， n，k与t均为正整数. 该算法推广了陈豪提出的求GF(p^m)上周期为3n的序列线性复杂度的一个快速算法， 其中p是素数， gcd(n， p^m-1)=1且p-1=3t， n与t均为正整数. 结合一些已知的快速算法，可以快速计算GF(p^m)上周期为kn的序列线性复杂度， 最后给出一个具体例子.

关键词 密码学 周期序列 线性复杂度 极小多项式 快速算法

分类号 TN918.1 0236

Fast algorithm for determining the linear complexity of sequences over GF (p^m) with the period kn

DAI Xiao-ping,ZHOU Jian-qin

(Dept. of Computer Science, Anhui Univ. of Technology, Ma'anshan 243002， China)

Abstract

A fast algorithm is presented for determining the linear complexity and the minimal polynomial of sequences over GF(p^m) with the period kn, where p is a prime, gcd(n, p^m-1)=1, p^m-1=kt, and n, k and t are integers. The algorithm presented here covers the algorithm proposed by Chen Hao for determining the linear complexity of sequences over GF(p^m) with the period 3n, where p is a prime, gcd(n, p^m-1)=1, p-1=3t, and n and t are integers. Combining the proposed algorithm with some known algorithms, the linear complexity of sequences over GF(p^m) with the period kn can be determined more efficiently. Finally, an example for applying this algorithm is presented.

Key words cryptography periodic sequence linear complexity minimal polynomial fast algorithm

DOI:

通讯作者 戴小平 xpdai@ahut.edu.cn