吉首大学学报自然科学版 » 2011, **Vol. 32** » Issue (6): 27-32 DOI:

周期为2pn的q元序列m紧错线性复杂度

(1.杭州电子科技大学通信工程学院,浙江 杭州 310018；2.安徽工业大学计算机学院,安徽 马鞍山 243002)

m-Tight Error Linear Complexity of Sequences with Period 2pn over GF(q)

(1.College of Telecommunication,Hangzhou Dianzi University,Hangzhou 310018,China;2.College of Computer Science and Technology,Anhui University of Technology,Maanshan 243002,Anhui China)

- 摘要
- 参考文献
- 相关文章

全文: PDF (280 KB) HTML (1 KB) **输出:** BibTeX | EndNote (RIS) **背景资料**

摘要 结合k错线性复杂度曲线和最小错误的理论,提出m紧错线性复杂度的概念来研究序列线性复杂度的稳定性.首先优化魏-肖-陈算法的结构,即GF(q)上求周期为2pn的q元序列线性复杂度的快速算法；然后通过采用联合代价的方法,给出一个GF(q)上求周期为2pn的q元序列k错线性复杂度的快速算法；接着给出周期为2pn的q元序列的m紧错线性复杂度快速算法，其中p和q是奇素数，q为模p2的一个本原根.

关键词: 流密码 序列 线性复杂度 k错线性复杂度 m紧错线性复杂度

Abstract: Using the theories of the minimum error and the k-error linear complexity profile of sequences,m-tight error linear complexity is presented to study the stability of the linear complexity of sequences.First,the structure of the Wei-Xiao-Chen algorithm for the linear complexity of sequences with period 2pn over GF(q) is optimized,where p and q are odd primes and q is a primitive root (mod p2).Second,the union cost is used,so that an efficient algorithm for computing the k-error linear complexity of a sequence with period 2pn over GF(q) is derived,where p and q are odd primes and q is a primitive root (mod p2).Finally,an efficient algorithm for computing m-tight error linear complexity of sequences with period 2pn over GF(q) is given,where p and q are odd primes and q is a primitive root (mod p2).

Key words: stream cipher sequence linear complexity k-error linear complexity m-tight error linear complexity

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 周建钦
- 上官成

基金资助:

浙江省自然科学基金资助项目(Y1100318,R1090138);国家自然科学基金委员会与中国工程物理研究院联合基金资助(10776077);
上海市信息安全综合管理技术研究重点实验室开放课题(AGK2009007)

作者简介: 周建钦（1963-），男，山东巨野人，教授，硕士，主要从事通信、密码学与理论计算机科学研究.

引用本文:

周建钦,上官成. 周期为2pn的q元序列m紧错线性复杂度[J]. 吉首大学学报自然科学版, 2011, 32(6): 27-32.

ZHOU Jian-Qin,SHANG Guan-Cheng. m-Tight Error Linear Complexity of Sequences with Period 2pn over GF(q)[J]. Journal of Jishou University(Natural Sciences Edit, 2011, 32(6): 27-32.

[1] DING Cun-sheng,XIAO Guo-zhen,SHAN Wei-juan.The Stability Theory of Stream Ciphers [M].Springer Verlag：Lecture Notes in Computer Science,1991：561.

[2] STAMP M,MARTIN C F.An Algorithm for the k-Error Linear Complexity of Binary Sequences with Period 2n [J].IEEE Trans. on Information

Theory,1993,39(4):1 398-1 401.

[3] GAMES R A,CHAN A H.A Fast Algorithm for Determining the Complexity Pseudo Random Sequence with Period 2n [J].IEEE Trans. on Information Theory,1983,29(1):144-146.

[4] WEI Shi-min,XIAO Guo-zhen,CHEN Zhong.A Fast Algorithm for Determining the Minimal Polynomial of a Sequence with a Period 2pn Over GF (q) [J].IEEE Trans. on Information Theory,2002,48(10):2 754-2 758.

[5] 戴小平,周建钦.求周期为2pm二元序列k错线性复杂度的快速算法 [J].兰州大学学报：自然科学版,2008,44(1):65-70.

[6] KUROSAWA K,SATO F,SAKATA T,et al.A Relationship Between Linear Complexity and k-Error Linear Complexity [J].IEEE Trans. on Information Theory,2000,46(2):694-698.

[7] LAUDER A,PATERSON K.Computing the Error Linear Complexity Spectrum of a Binary Sequence of Period 2n [J].IEEE Trans. on Information Theory,2003,49(1):273-280.

[8] 魏仕民,肖国镇,陈钟.确定周期为2npm二元序列线性复杂度的快速算法 [J].中国科学：E辑,2002,32(3):401-408.

[1] 卓月明. **基于聚类技术的XML文件代表性结构获取**[J]. 吉首大学学报自然科学版, 2011, 32(6): 55-58.