吉首大学学报自然科学版 » 2012, **Vol. 33** » Issue (3): 32-35 DOI: 10.3969/j.issn.1007-2985.2012.03.009

周期二元序列的部分4-错误序列计数公式

(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243032)

On the 4-Error Sequence Distribution of 2n-Periodic Binary Sequences

(1.Telecommunication School,Hangzhou Dianzi University,Hangzhou 310018,China;2.Computer Science School,Anhui University of Technology,Ma'anshan 243032,Anhui China)

- 摘要
- 参考文献
- 相关文章

全文: PDF (293 KB) HTML (1 KB) **输出:** BibTeX | EndNote (RIS) **背景资料**

摘要 k-错线性复杂度是度量密钥流序列的密码强度的一个重要指标.为了更好地刻画和研究序列的随机性，研究了周期为2n的二元序列s的k-错线性复杂度(LCk(s的分布情况，讨论了满足LCks)=LC(s+e)条件下的k-错误序列e的分布情况.基于Games-Chan算法，通过将k-错线性复杂度的计算转化为求Hamming重量最小的错误序列的方法，给出了线性复杂度小于2n的2n周期二元序列的部分4-错误序列的计数公式.

关键词: 序列密码 线性复杂度 k-错线性复杂度 k-错误序列

Abstract: The k-error linear complexity of a sequence has been used as one of the important measure of keystream strength.In order to better depict and study randomicity of sequences,the k-error sequencesedistribution that corresponds with LCk(sLC(s+e) is discussed by studying the distribution of k-error linear complexity of binary sequences (s) with period 2n.Based on Games-Chan algorithm,it is proposed that the computation of k-error linear complexity should be converted to finding error sequences with minimal Hamming weight.For k=4,some the counting functions on the k-error sequences of 2n-periodic binary sequences with linear complexity less than 2n are derived.

Key words: stream cipher linear complexity k-error linear complexity k-error sequences

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
- 刘军

基金资助:

浙江省自然科学基金资助项目(Y1100318;R1090138)

作者简介: 周建钦（1963-），男，山东巨野人，安徽工业大学计算机学院教授，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,刘军. 周期二元序列的部分4-错误序列计数公式[J]. 吉首大学学报自然科学版, 2012, 33(3): 32-35.

ZHOU Jian-Qin,LIU Jun. On the 4-Error Sequence Distribution of 2n-Periodic Binary Sequences[J]. Journal of Jishou University(Natural Sciences Edit, 2012, 33(3): 32-35.

[1] DING Cun-sheng,XIAO Guo-zhen，SHAN Wen-juan.The Stability Theory of Stream Ciphers [M].LNCS 561.Berlin:Springer-Verlag,1991:85-88.

[2] STAMP M，MARTIN C F.An Algorithm for the k-Eerror Linear Complexity of Binary Sequences with Period 2n [J].IEEE Transactions on Information Theory,1993,39(4):1 398-1 401.

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

[4] 谭林,戚文峰.F2上2n周期序列的k错误序列 [J].电子与信息学报,2008,30(11):2 592-2 595.

[5] 李鹤龄,戚文峰.Fp上pn-周期序列的k-错误序列 [J].通信学报,2010,31(6):19-24.

[6] 周建钦.具有2n线性复杂度的2n周期二元序列的3错线性复杂度 [J].应用数学学报,2012,35(3).

[7] FU Fang-wei,NIEDERREITER H,SU Ming.The Characterization of 2n-Periodic Binary Sequences with Fixed 1-Error Linear Complexity [C]// GONG G,HELLESETH T,SONG H-Y,et al.SETA 2006,LNCS,Vol. 4 086,Springer,2006:88-103.

[1] 周建钦, 赵起, 崔洪成. **2^n周期平衡二元序列的8错线性复杂度**[J]. 吉首大学学报自然科学版, 2012, 33(2): 28-34.

[2] 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.