文章编号：1673-9469（2018）02-0100-03 doi:10.3969/j.issn.1673-9469.2018.02.022

一种伪随机序列的线性复杂度及其稳定性研究

孙全玲，吕 虹，陈万里，戚 鹏

（安徽建筑大学 电子与信息工程学院，安徽 合肥 230601）

摘要：信息安全领域中，传统使用 *m* 序列为基序列，对序列进行非线性组合、非线性滤波和非均匀采样等产生线性复杂度很高的序列，其线性复杂度的稳定性却不如意。提出伪随机序列称为 *m* 子序列，*m* 子序列通过改变 *m* 序列的状态转换次序而得到的序列，*m* 子序列改变了 *m* 序列的输出次序，是非线性序列。实验数据表明其线性复杂度是移位寄存器个数的指数倍，同时其线性复杂度的稳定性很高，此序列的 *k*-error 线性复杂度随着移位寄存器的个数的增加而不变。

关键词：*m* 子序列；*m* 序列；线性复杂度；*k*-error 线性复杂度；状态转换；信息安全

中图分类号：TN801 **文献标志码**：A

Study on the linear complexity and stability of a Pseudorandom Sequence

SUN Quanling，LV Hong，CHEN Wanli，QI Peng

(Department of Electronic and Information Engineering，Anhui Jianzhu University，Hefei 230601，China)

Abstract：In the information security area，traditionally m-sequence is used as the base sequence on which non-linear combination，non-linear filtering and non-uniform sampling are applied to generate a sequence with high linear complexity. Yet the stability of linear complexity of such a sequence is not satisfactory. In this paper，we propose m-subsequence which is generated by changing the state transition order of the m-sequence. Since the m-subsequence is made by changed the order of the m -sequence，it is a non-linear sequence. The linear complexity is shown to be stable and exponential in the length of the shift register by testing data. In addition，the k-error linear complexity remains the same as the length of the shift register grows.

Key words：m-subsequence；m sequence；linear complexity；k-error linear complexity；state transition；information security.

序列密码的强度问题一直是密码系统研究者所关注的方面，线性复杂度是一些流密码系统强度的重要指标。为抗明文攻击，密钥流序列的线性复杂度应为足够大。但是高线性复杂度序列未必难以预测，例如有 *N* 位序列 *S*=11111……10，其线性复杂度 *L*(*S*)=*N*-1，但只要改变其中一个比特，则序列的线性复杂度就降为 1。因此线性复杂度的稳定性与序列的可测性是密切相关的。用作加密的密钥流序列须有足够大的线性复杂度，并且线性复杂度是稳定的，否则，这样的序列就是不安全的。我国学者丁存生、肖国镇等[1]率先创立了序列的稳定性理论，并提出球体复杂度、重量复杂度等稳定性度量指标，国外学者 M.Stamp 和 C.F.Martin[2] 提出了类似球体复杂度的 *k*-error 线性复杂度的稳定性指标，并提出计算周期为 2*n* 的周期序列的 *k*-error 线性复杂度的算法。*k*-error 线性复杂度的概念得到了国内外研究者的认同。文中说明了 *m* 子序列产生方式并使用软件方式产生了多级不同的 *m* 子序列，对 *m* 子序列的线性复杂度，*k*-error 复杂度进行计算。

收稿日期：2018-01-22

基金项目：国家自然科学基金资助项目 (61372094)；安徽省科技厅项目 (KJ2017JD08)；安徽省自然科学基金资助项目 (1708085MF167)

作者简介：孙全玲 (1976-)，女，安徽寿县人，硕士，讲师，从事计算机应用、信息安全方面的研究。

1 *k*−error 线性复杂度

序列的 *k*-error 线性复杂度是指对序列改变至多 *k* 个元素所得到的序列的线性复杂度的最小值，是衡量一个序列线性复杂度稳定性的一个重要指标。

k-error 线性复杂度的定义如下 [2]：

设 $s=(s_0, s_1, \cdots, s_{N-1})^\infty$ 是 F_q 上的 *N*- 周期序列，*k* 是非负整数，序列 *s* 的 *k*-error 线性复杂度 $LC_{N,k}(s)$ 为：$LC_{N,k}(s)=\min_{W_H(e,N)\le k} LC(s+e)$，其中 *e* 是跑遍 F_q 上所有满足 $W_H(e, N)\le k$ 的 *N*- 周期序列。从定义中可知 *k*-error 线性复杂度指在序列 *s* 中改变至多 *k* 位后得到的最小线性复杂度。

周期序列的 *k*-error 线性复杂度随着 *k* 值的增加而减少或者不变。*k*-error 线性复杂度谱中的第一个使序列的线性复杂度下降很明显的 *k* 值称为错误线性复杂度的第一下降点，错误线性复杂度谱的第一下降点反映了序列线性复杂度稳定性的好与坏。如果第一下降点很大，攻击者要使序列的线性复杂度下降的代价就越大。

2 Stamp−Martin 算法

Chan-Games 算法是求序列线性复杂度的广泛使用的算法，使用 $\sum_{j=0}^{k}\binom{N}{j}$ 次 Chan-Games 算法可以求出一个序列的 *k*-error 线性复杂度，但是计算量大，所以在此基础上，提出了改进算法，称为 Stamp-Martin 算法，此算法成为求 *k*-error 线性复杂度的经典算法，其算法详见文献 [2]。

3 传统伪随机序列的线性复杂度的稳定性

通过以 *m* 序列为基序列，对序列进行非线性组合、非线性滤波和非均匀采样等方法可以很容易取得线性复杂度很大的序列，但是，这些方法得到的序列的线性复杂度的稳定性却不如意。文献 [3] 给出下面的两个定理。

定理 1：设 s^∞ 是周期为 2^n-1 的最大长度二元序列，如果 $f_s(x)$ 不等于它的互反多项式，那么 $WP(s^\infty)=2^n-1$。

定理 2：设 s^∞ 是 GF(q) 上的一个最大长度序列且 p 是 GF(q) 的特征。如果 $\deg(f_s(x))=n$，那么 $WP(s^\infty)\ge q^n-n-1$。其中 $WP(s^\infty)$ 表示序列 s^∞ 的重量周期。

从上述定理可以看出，只要在这类序列的每个周期段的任意位置对应改变序列的一个比特，则序列的线性复杂度就会突增至 2^n-n-1。反之，则说明这样的高线性复杂度的稳定性较差。

4 *m* 子序列

最大线性反馈移位寄存器产生的 *m* 序列的周期特性、串分布特性和自相关特性在密码学意义中比较理想，但是它们的线性复杂度却是在同样周期的序列中是最小的。在 *m* 序列的状态转换过程中有低位互反且其他位相同的状态对，形如 0101 和 0100，1010 和 1011 等，这些状态对称为共轭状态，用 $s=(a_{n-1}, a_{n-2}, \cdots, a_1, a_0)$，$s^*=(a_{n-1}, a_{n-2}, \cdots, a_1, \tilde{a}_0)$ 表示。如果在这些状态中有对共轭状态的连线在 *m* 序列的状态转换过程中有交叉，可以通过改变 2^i，$i>1$ 对共轭状态的后继状态，形成一个新的同周期的状态转换的输出的新序列即为 *m* 子序列。其转换过程图 1 所示。

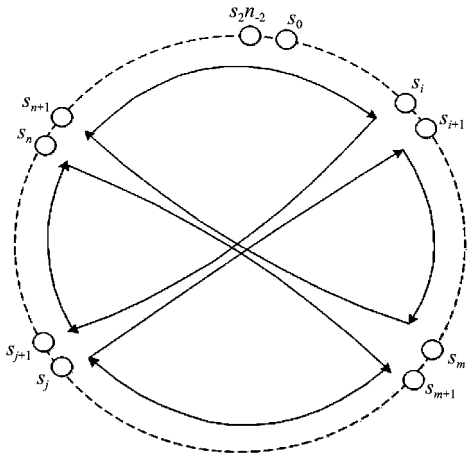

图 1　*m* 序列和 *m* 子序列的状态转换

Fig.1 State transitions of *m*-sequen and *m*-subesequence

图 1 中的虚线表示输出 *m* 序列的状态转换，实线表示输出 *m* 子序列的状态转换。从图中可以看出 *m* 序列的状态转换过程为：$s_0 \to \cdots \to s_i \to s_{i+1} \to \cdots \to s_m \to s_{m+1} \to \cdots \to s_j \to s_{j+1} \to \cdots s_n \to s_{n+1} \to \cdots \to s_{2^n-2}$，而 *m* 子序列的状态转换过程为：$s_0 \to \cdots \to s_i \to s_{j+1} \to \cdots \to s_n \to s_{m+1} \to \cdots \to s_j \to s_{i+1} \to \cdots \to s_m \to s_{n+1} \cdots \to s_{2^n-2}$。

一个 *n* 级线性反馈移位寄存器只能产生 $\varphi(2^n-1)/n$ 个平移不等价的 *m* 序列。如果对每一个 *m* 序列的状态转换过程中，找到相互交叉的共轭状态对并改变状

态转换顺序，可得到多种不同的序列。交叉共轭状态对的数量随着移位寄存器的级数的增加显著的增多，从而可以生成更多的新序列。文献 [4] 中已证明：一个周期为 2^n-1 的 m 序列，其移位寄存器的状态转换图内有 $(2^{n-1}-1)(2^{n-1}-2)/6$ 个两两交叉共轭状态对。

4.1 m 子序列的线性复杂度

m 子序列是改变了 m 序列的输出顺序，改变了 m 序列的线性性，是非线性序列，可以增强其安全性，增加破译的难度。采用 Chan-Games 算法对 m 子序列的复杂度进行计算，从表 1 结果可以看出，同级的 m 子序列比 m 序列的线性复杂度高很多，与移位寄存器个数有着指数级增长的关系。

4.2 m 子序列的线性复杂度谱

定义：设 n 是正整数，$\underline{s}$ 是有限域 F_q 上的长度不小于 n 的序列，序列 $\underline{s}$ 的 n 阶线性复杂度 $L_n(\underline{s})$ 是指在 F_q 能生成 $\underline{s}$ 的前 n 个元素的线性递归关系的最小阶数，整数序列 $L_1(\underline{s})$，$L_2(\underline{s})$，…称为 $\underline{s}$ 的线性复杂度谱。

文献 [5] 指出二元随机序列的 k-error 线性复杂度的均值有：$E'_{n,\,k} = N/2\text{-}o(n)$

早些时候 R.A.Rupped[6] 就提出，随机序列的线性复杂度谱应不规则地接近 $N/2$。

本次实验数据中 m 子序列的线性复杂度值基本上为周期的一半。对于周期为 $N=2^n-1$，$n>0$ 线性移位寄存器产生的序列，其线性复杂度在 $N/2$ 上下微小波动，满足 $LC(s)=N/2+O(1)$，$N=2^n-1$。

4.3 m 子序列的 k—error 线性复杂度

伪随机序列的 k-error 线性复杂度的分布对评价序列的随机性有非常重要的作用，如果某序列的 k-error 线性复杂度偏离均值较大的话，则断定该序列的伪随机性差。

文献 [7] 等对 F_q 上 n 长序列的 k-error 线性复杂度的均值估计为：$\frac{n}{2}-\frac{k}{2}\log_q(n)\overset{\leq}{\approx}E_{n,\,k,\,q}\overset{\leq}{\approx}\frac{n}{2}-\frac{k}{2}$。

并证明存在数量很多同时具有很大线性复杂度和 k-error 线性复杂度的序列。

这两种结果都是对 k-error 线性复杂度均值的估计，结果相似。

定义：设 k 是非负整数，$\underline{s}=(s_0, s_1, \cdots, s_{N-1})^\infty$ 是 F_q 上的 N- 周期序列，$\{LC_{N,\,k}(\underline{s})：k=0, 1, \cdots, N\}$ 称为序列 $\underline{s}$ 的错误线性复杂度谱。k=0 时为序列的线性复杂度，随着 k 值的增长其线性复杂度关系有：$\{LC(\underline{s})=LC_{N,\,0}(\underline{s}) \geq LC_{N,\,1}(\underline{s}) \geq \cdots LC_{N,\,WH(\underline{s})}(\underline{s})=0\}$。

图 2 是利用 Stamp-Martin 算法计算的具有 7 级反馈移位寄存器产生的 m 子序列的 k-error 线性复杂度谱，7 级移位寄存器产生的 m 子序列改变 k 值的情况下计算出的线性复杂度，其线性复杂度变化缓慢趋向减少。图中显示在 k 值为 3 时其线性复杂度明显下降。k=3 为其第一下降点。也就是说如果要使 7 级 m 子序列的线性复杂度明显降低需要至少改变其中 3 个位。

对于 9 级移位寄存器改变不同的共轭状态对产生的 m 子序列，其线性复杂度也没有随着 k 值的改变而改变。表中 9(1)9(2)9(3) 分别表示改变 9 级线性反馈移位寄存器中不同的三对交叉共轭状态对。分别是 011000010，011000011，000011000，000011001；111000000，111000001，001111000，001111001；011100000，011100001，110011000，110011001。

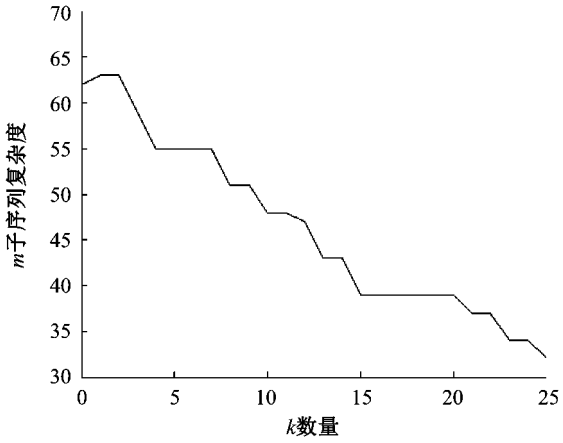

图 2 7 级 m 子序列的 k-error 线性复杂度谱

Fig.2 The k-error complexity of 7 level m subsequence

表 1 同级 m 序列和 m 子序列的线性复杂度

Tab.1 Complexities of the m-sequence and m-subsequence with the sea

级数	5	7	8	9	10	11	15	17
m 序列	5	7	8	9	10	11	15	17
m 子序列	17	64	128	298	513	1 028	9 165	65 532

（下转第 112 页）

324-331.

[12]GONG L，ZHU Z，WANG X，et al.Changeable focused field distribution of double-ring-shaped cylindrical vector beams[J].Optics Communications，2015，342：204-213.

[13]HUANG S，WANG X L，ZHU Z Q，et al. Focusing field of the radial vector beams with multi-vortex phases[J]. Optics communications，2016，366：142-147.

[14]SURESH P，RAVI V，RAJESH K B. Multiple Focal Segment Generation of Tightly Focused Non Diffracting Transversely Polarized Beam with Diffractive Optical Element[J]. J. Environ. Nanotechnol，2014，3(4)：73-77.

[15] 常 强，杨艳芳，何 英，等 .4pi 聚焦系统中振幅和相位调制的径向偏振涡旋光束聚焦特性的研究 [J]. 物理学报，2013，62(10)：104202.

[16]HUANG K，SHI P，CAO G W，et al. Vector-vortex Bessel-Gauss beams and their tightly focusing properties[J]. Opt. Lett，2011，36(6)：888-890 .

[17]WOLF E. Electromagnetic diffraction in optical systems I. An integral representation of the image field[J]. Proc. R. Soc. London Ser. A，1959，253：349-357.

[18]RICHARDS B，WOLF E. Electromagnetic diffraction in optical systems II. Structure of the image field in anaplanatic system[J]. Proc. Roy. Soc. A，1959，253：358-379.

（责任编辑 王利君）

（上接第 102 页）

表 2 *m* 子序列的 *k*—error 线性复杂度

Tab.2 The *k*-error linear complexity of some *m*-subsequence

m 子序列	*K*=0	*K*=1	*K*=2	*K*=3	*K*=4
N=9(1)	255	255	255	255	255
N=9(2)	255	255	255	255	255
N=9(3)	255	255	255	255	255
N=11	1 023	1 023	1 023	1 023	1 023

随着移位寄存器级数的增加，线性复杂度的稳定性也越强，通过对 11 级移位寄存器产生的 *m* 子序列使用 Stamp-Martin 算法计算其在改变 k 值的情况下，其线性复杂度并不改变。

从以上数据可以看出：*k* 值不变的情况下，*m* 子序列的线性复杂度不规则地接近周期的一半即 *N*/2，符合 R.A.Rupped 的观点。*k* 值改变，其线性复杂度不变并且接近周期的一半即 *N*/2，符合 H.Niederreiter 等对随机序列的 *k*-error 线性复杂度的估计。

5 结论

m 子序列是在不改变 *m* 序列的周期的方式中改变 *m* 序列的状态转换次序而得到的一类序列，实验数据可以说明这种序列的数量庞大但却大大提高来线性复杂度且线性复杂度的非常稳定。*m* 子序列可以在信息安全领域发挥巨大的作用。从实验分析，*m* 序列中有很多共轭交叉状态对，改变 2^i(i>=1) 对都可以形成新的输出序列，后续还需大量的工作验证和推理这样的序列的通用性质及密码学上的其他性质。

参考文献：

[1] DING Chunsheng，XIAO Guozhen，SHAN W.The stability theory of stream ciphers[J]. LNCS 561.Berlin：Springer-Verlag，1991.

[2]STAMP M，MARTIN C F. An algorithm for the *k*-error linear complexity of binary sequences with period 2n[J]. IEEE Transactions on Information Theory，1993，39(4)：1398-1401.

[3] KUROSAWA K，SATO F，SAKATA T，et al. A realationship between linear complexity and *k*-error linear complexiy[J].IEEE Transactions on Information Theory，2000，46(2)：694-698.

[4] TOR Helleseth，TORLEIV Klove. The number of Cross-Join Pairs in Maximum Length Linear Sequences[J].IEEE Transactions on information theory，1991，3(6)：1731-1733.

[5] NIU Zhihua. Analysis of the Linear complexity and Its Stability For Peridoic Sequences [D].Shanxi Xian：Xidian university，2005：25-49.

[6] RUPPEL R A. Analysis and Design of Stream Ciphers[J]. Springer-Verlag，1998.

[7] TAN Lin.On the *k*-error Linear Complexity of Pseudorandom Sequence [D]. Henan Zhengzhou：Pla information engingeering university，2012：11-18.

（责任编辑 王利君）