混沌序列与一类基于移位寄存器的非线性序列的性能比较 [1]

米 良 朱中梁

(西南电子电信技术研究所 成都 610041)

摘 要 混沌序列与一类基于移位寄存器的非线性序列—非线性前馈逻辑 (Non-Linear Feed-Forward Logic, NLFFL) 序列都具有非线性、宽带类噪声、大的码族、长的周期且容易产生的特性. 通过对它们在产生方式、相关性能、多址性能以及抗相关攻击能力等方面进行分析和仿真研究, 说明混沌序列与该类非线性序列在性能上总体相当, 但对于短周期序列 ($N \leq 1023$), 混沌序列的抗相关攻击、抗干扰能力更强, 因此更具有实用价值.

关键词 混沌序列, 非线性序列, 相关攻击

中图号 TN911.7

1 引 言

由于混沌系统具有良好的类随机、非周期、非线性特点, 对初值和参数有极端敏感的依赖性, 但又是确定可再生的, 因此对混沌序列的研究引起了广泛的关注 [1−4].

除混沌序列外, 产生非线性序列的方法还有很多, 其中最常见的是将线性移位寄存器序列经过非线性变换后得到, 其产生方法如图 1 所示. 这种方法产生的非线性序列实现简单, 且序列周期可以足够长. 那么, 同为非线性序列, 混沌序列与这类基于线性移位寄存器的非线性序列孰优孰劣呢? 本文就此对混沌序列与一类基于移位寄存器的非线性序列在产生方式、相关性能、多址性能以及抗相关攻击能力等方面进行分析比较研究.

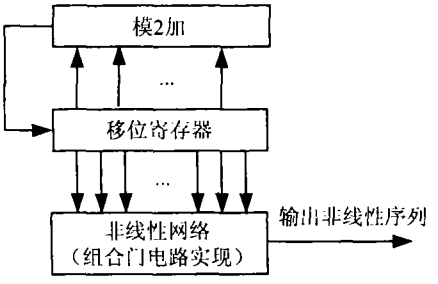

图 1 基于移位寄存器的非线性序列产生方法

2 序列的产生

混沌序列发生器的实现方法大致可分为以下几种: (1) 经典的一维混沌映射 [5], 形式简单且易实现, 便于理论设计和分析; (2) 采用高阶非线性数字滤波器 [6], 能部分地克服有限精度效应, 并可用 DSP 非常方便地实现; (3) 基于神经网络的方法 [7], 实质上是利用神经网络来学习和逼近一个混沌系统, 具有系统结构灵活的特点; (4) 基于高维的时空混沌 [8], 较低维的混沌映射其产生的混沌序列数量更多, 且易实现同步.

[1] 2002-06-24 收到, 2002-10-29 改回
国防抗干扰通信重点实验室基金资助项目 (No.99JS04.8.1.JB5101)

本文主要考虑第 1 种方法，即由一维混沌映射产生的混沌序列，最常见的是 Logistic 满映射：

$$x_{n+1} = f(x_n) = 1 - 2x_n^2, \qquad x_n \in [-1, 1] \tag{1}$$

和 k 阶的 Chebyshev 映射：

$$x_{n+1} = \cos(k\arccos(x_n)), \qquad x_n \in [-1, 1] \tag{2}$$

只要选取不同的参数和初始值，经过迭代就可以得到完全不同的混沌序列，因此其数量可以说是无穷的．下面就以这类一维混沌映射产生的周期为 N 的二元数字混沌序列 $\{a\}$ 为例来研究其性能，即数字混沌扩频序列 $\{a\}$ 由轨迹 $\{x_n\}$ 量化得到

$$a(n) = \mathrm{sgn}(x_n), \qquad n = 0, 1, \cdots, N-1 \tag{3}$$

其中 $\mathrm{sgn}(\cdot)$ 是符号函数， N 为混沌序列 $\{a\}$ 的周期．

本文研究的一类基于移位寄存器的非线性序列——非线性前馈逻辑 (Non-Linear Feed-Forward Logic) 的伪随机序列，以下简称 NLFFL 序列．它是线性反馈移位寄存器加上 NLFFL 函数构成的，即图 1 中的非线性网络由 NLFFL 函数实现，其具体构成参见文献 [9]．除采用“与”门构成 NLFFL 函数外，还可采用大数逻辑 ML(Majority Logic) 门来构成 [10]．该序列具有电路实现简单、线性复杂度高的特点，且数量众多，是一类较典型的非线性序列．

3 性能比较

由于对 NLFFL 序列难以进行精确的数学分析，下面就其与混沌数字序列在相关性能、平衡性能、线性复杂度和异步码分多址 (CDMA) 中的扩频多址性能作数值仿真比较，仿真结果如表 1 所示．研究的 NLFFL 序列分别是 2 输入“与”门、 3 输入“与”门和 3 输入 ML 门的平衡与非平衡 NLFFL 序列．混沌序列采用 Logistic 满映射和 4 阶 Chebyshev 映射产生的混沌数字序列，所有混沌序列初值均随机产生．序列长度 N 分别为 511 和 1023 ．

表 1 NLFFL 序列与混沌序列性能比较

序列	自相关旁瓣峰值		互相关峰值		线性复杂度		平衡性 (1 的个数)	
	$N=511$	$N=1023$	$N=511$	$N=1023$	$N=511$	$N=1023$	$N=511$	$N=1023$
2-AND (B)	0.1272	0.0635	0.1429	0.1105	45	55	256	512
2-AND (NB)	0.1272	0.0635	0.1546	0.0948	45	55	240	480
3-AND (B)	0.1546	0.0948	0.1389	0.1105	129	175	256	512
3-AND (NB)	0.4364	0.2805	0.3503	0.2649	129	175	136	304
3-ML (B)	0.1272	0.0635	0.1389	0.1085	45	55	256	512
3-ML (NB)	0.1272	0.0635	0.1429	0.0948	45	55	256	512
Logistic	0.1233	0.0968	0.1350	0.1202	257	512	252	523
Chebyshev	0.1429	0.0987	0.1429	0.1026	256	512	251	525

* 表中第一列的 B 表示平衡序列， NB 表示非平衡序列

3.1 相关性能

分别计算这些序列的周期自相关和互相关，所得的自相关旁瓣峰值和互相关峰值如表 1 所示．由表 1 中相关性能的比较可知，除了 3 输入“与”门的非平衡 NLFFL 序列的性能较差外，混沌数字序列与其它 NLFFL 序列的自相关性能和互相关性能相当．

3.2 线性复杂度

线性复杂度定义为能产生该序列的最短线性移位寄存器的阶数，在抗干扰应用中有特别重要的意义．混沌扩频序列本质上是随机二进制序列，因此它的线性复杂度的均值等于序列长度

的一半，方差约为 86/81[11]，具有较理想的线性复杂度特性，这是混沌扩频序列优于传统扩频序列的一个重要体现。对于 NLFFL 序列，其线性复杂度的 Key 上界 [12](由 E. L. Key 首先推导出而得名) 为

$$\mathrm{LC}_{key} \le \sum_{i=1}^{D} \binom{n}{i} \tag{4}$$

式中 n 是移位寄存器的级数，D 是在 NLFFL 函数中非线性的最高阶数 (即每个 "与" 门的输入个数)。根据 Berlekamp-Massey 算法 [11] 得到的这些序列的线性复杂度如表 1 所示。

表 1 中线性复杂度的比较说明，混沌序列的线性复杂度约为序列长度的一半，而 NLFFL 序列的线性复杂度则与序列长度和 NLFFL 函数中非线性的最高阶数有关，由 Berlekamp-Massey 算法得到的线性复杂度数值也与 (4) 式的 Key 上界相符。

3.3 平衡性能

由表 1 中的平衡性比较可知，平衡 NLFFL 序列的平衡性能优于混沌数字序列；除了 3 输入 ML 门的非平衡 NLFFL 序列的平衡性能较好外，其余两个非平衡 NLFFL 序列的平衡性能则劣于混沌数字序列。

3.4 异步 CDMA 扩频多址性能

考虑一个有 K 个用户的 BPSK 调制的异步直扩码分多址 (DS/CDMA) 系统，由文献 [13] 可知，其中第 j 个用户相关接收机输出端的平均信噪比可以用这 K 个用户的平均干扰参数和加性高斯白噪声 (AWGN) 信道的信噪比 E_b/N_0 来表示

$$\mathrm{SNR}_j = \left\{ \frac{N_0}{2E_b} + \frac{1}{6N^3} \sum_{i=1, i\ne j}^{K} r_{i,j} \right\}^{-1} \tag{5}$$

式中平均干扰参数 $r_{i,j}$ 定义为

$$r_{i,j} = 2\mu_{i,j}(0) + \mu_{i,j}(1) \tag{6}$$

对于二元序列，$\mu_{i,j}$ 可以定义为

$$\mu_{i,j}(n) = \sum_{m=1-N}^{N-1} C_{i,j}(m) C_{i,j}(m+n) \tag{7}$$

其中 $C_{i,j}(m)$ 表示部分相关函数。文献 [14] 指出，(6) 式可以用其右边第一项来近似表示，误差很小。因此平均干扰参数 $r_{i,j}$ 就变成

$$r_{i,j}(n) = 2 \sum_{m=1-N}^{N-1} |C_{i,j}(m)|^2 \tag{8}$$

由文献 [13] 可知，(5) 式中的第二项即多址干扰，对于完全随机、独立同分布的二元序列可以近似为 $(K-1)/(3N)$，即 (5) 式可以表示为

$$\mathrm{SNR}_j = \{N_0/(2E_b) + (K-1)/(3N)\}^{-1} \tag{9}$$

下面用这个近似公式作为 NLFFL 序列和混沌数字序列作异步 CDMA 扩频多址性能比较的一个标准。NLFFL 序列选 2 输入 "与" 门的平衡和非平衡序列，混沌序列选 Logistic 满映

射和 4 阶 Chebyshev 映射产生的数字混沌序列，序列长度为 1023 。同时工作的用户数 K 分别为 6， 8， 10， 12 和 14，仿真结果如图 2 所示。图 2 中横坐标表示相关接收机的输入信噪比 E_b/N_0(dB)，纵坐标表示接收机输出端的信噪比恶化量 (dB)，该恶化量是指接收机分别在单用户工作时与多用户工作时输出端的信噪比的差值。由图 2 可知，除了 2 输入 “与” 门的非平衡 NLFFL 序列的异步 CDMA 扩频多址性能稍差外，其余三个序列的多址性能都彼此相当。

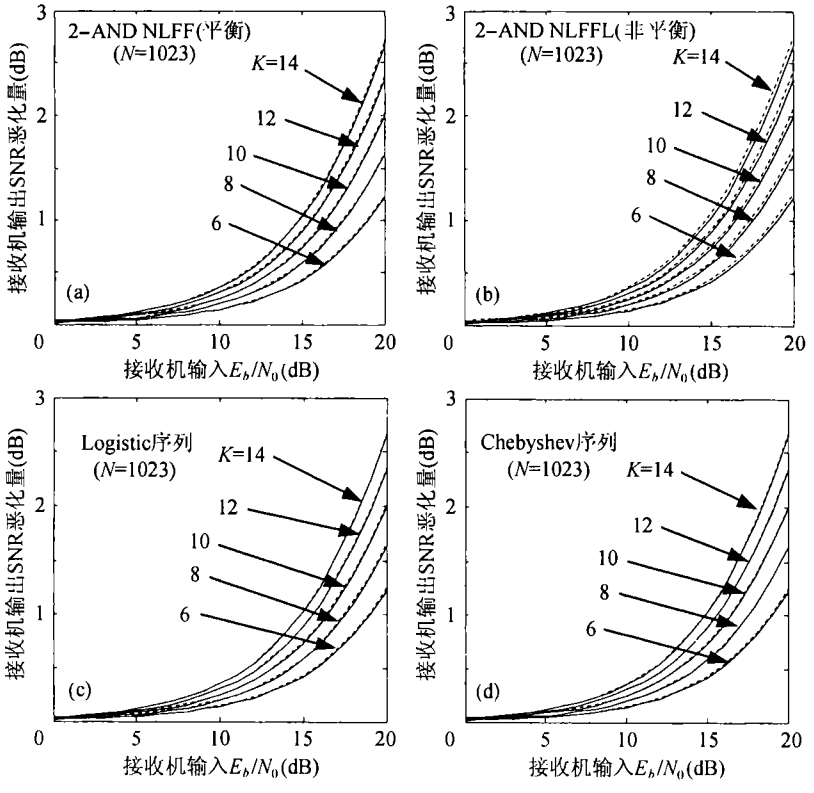

图 2 非线性序列扩频多址性能比较

(* 图中实线表示近似公式计算结果，虚线表示计算机仿真结果)

(a) 2-AND 门 NLFFL 平衡序列 (b) 2-AND 门 NLFFL 非平衡序列

(c) Logistic 混沌序列 (d) 4 阶 Chebyshev 混沌序列

4 抗相关攻击性能比较

相关攻击和统计分析是常用的信号截获分析方法。本文只讨论比较这两种非线性序列抗相关攻击的性能，并假设序列周期 $N \leq 1023$ 。由于生成 NLFFL 序列的基本 m 序列未知，因此只能用穷举 m 序列来攻击。而 m 序列的个数在一定的序列周期长度下 ($N \leq 1023$) 是确定的且数量较小，即对于 n 级线性移位寄存器， m 序列的码族为 $\Phi(2^n-1)/n$($\Phi(\cdot)$ 为欧拉函数) 。不妨假设我们已知非线性序列的周期为 1023 ，由此可知周期为 1023 的 m 序列个数为 60 。利用 m 序列良好的自相关性能，通过相关攻击，不难得到生成该 NLFFL 序列的基本 m 序列的本原多项式。

下面分别用周期为 1023 的 m 序列和混沌序列来攻击 4 种周期都为 1023 的非线性序列：混沌序列是 Logistic 序列和 Chebyshev 序列； NLFFL 平衡序列分别是由 3 输入的 “与” 门和

ML 门产生的，其基本 m 序列的特征多项式为 $P(x)=x^{10}+x^3+1$ 。假设经过尝试相关攻击，找到了作为生成被攻击 NLFFL 序列的基本 m 序列的特征多项式。并假设产生混沌序列的混沌映射形式未知，其初值也未知。采用 m 序列和 Logistic 混沌序列攻击的结果，其部分互相关函数分别如图 3 和 4 所示。图 3, 图 4 中横坐标表示时延 (单位： chip) ，纵坐标表示部分互相关函数 (Cross-Correlation Function, CCF) 。

由图 3 可知，尽管我们对 3 输入 "与" 门的个数及其连接关系未知，但只要找到正确的 m 序列的特征多项式，则 3 输入 "与" 门生成的 NLFFL 序列与攻击序列就会有较明显的相关性，说明该 NLFFL 序列可以被相关攻击；而 3 输入 ML 门生成的 NLFFL 序列的抗相关攻击性能有显著改善；两个混沌序列与基本 m 序列的相关性很弱，不易被相关攻击和干扰。

由图 4 可知，由于混沌序列的产生方式很多，因此很难确定其产生方法，即使碰巧使用了准确的产生被攻击混沌序列的混沌映射，但若其初始值不能精确得到，只要两者有微小的误差，由混沌对初值和参数的极端敏感依赖性可知，所得到的混沌攻击序列与被攻击混沌序列的互相关也很小，从而无法进行相关攻击和干扰所预期的混沌序列。

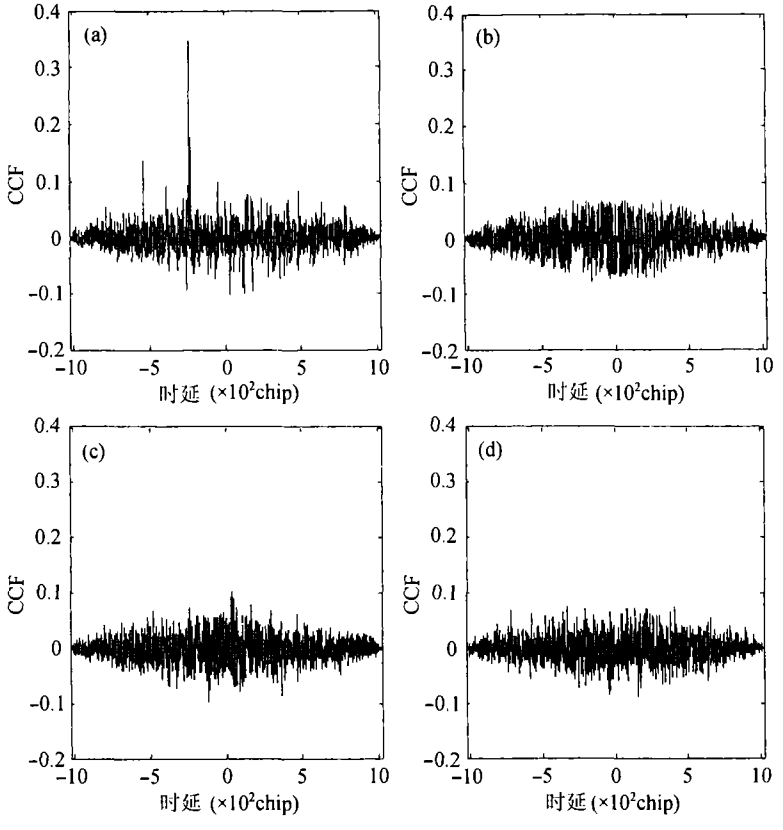

图 3　用 m 序列相关攻击四种非线性序列

(a) 相关攻击 3 输入 "与" 门 NLFFL 序列　(b) 相关攻击 3 输入 ML 门 NLFFL 序列

(c) 相关攻击 Logistic 混沌序列　(d) 相关攻击 Chebyshev 混沌序列

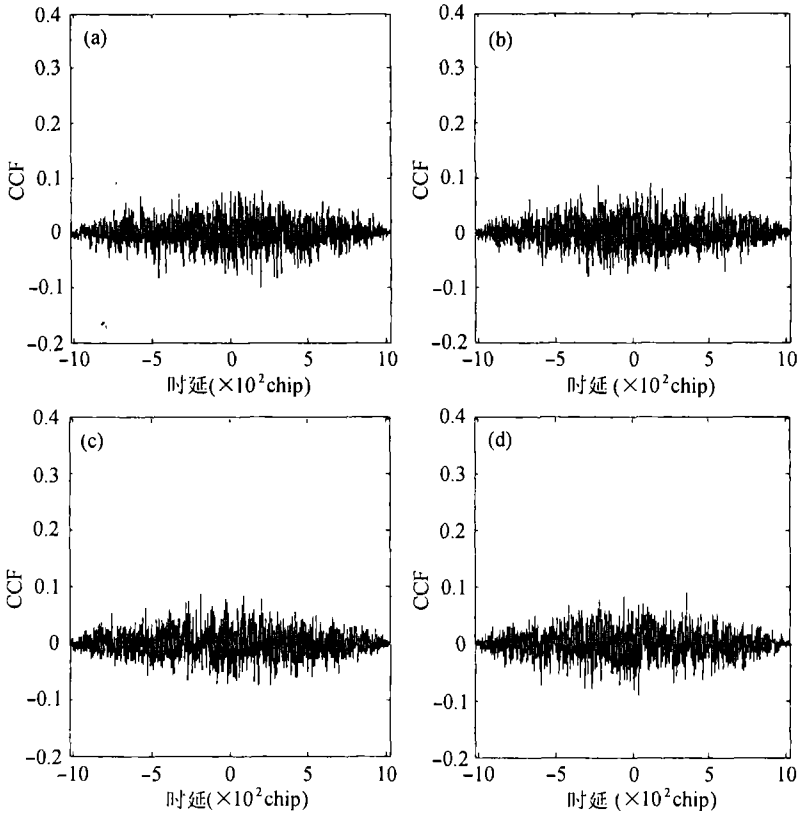

图 4 用 Logistic 序列相关攻击四种非线性序列

(a) 相关攻击 3 输入 "与" 门 NLFFL 序列 (b) 相关攻击 3 输入 ML 门 NLFFL 序列

(c) 相关攻击 Logistic 混沌序列 (d) 相关攻击 Chebyshev 混沌序列

5 结 论

通过将基于线性移位寄存器的 NLFFL 序列与混沌序列相比较，说明两者总体性能近似，但是这类基于移位寄存器的非线性序列变化更复杂，不同方法生成的各序列性能差异较大，应用时需要考虑选择的因素更多，并且由于它是在线性 m 序列的基础上产生的，在周期较短时 ($N \leq 1023$)，某些 NLFFL 序列的抗相关攻击能力较混沌序列有明显差距；而各种混沌序列的性能基本保持稳定，变化不显著，抗相关攻击、抗干扰能力更强，因而更便于应用，更具有实用价值。

参 考 文 献

[1] G. Heidari-Bateni, C. D. McGillem, A chaotic direct-sequence spread-spectrum communication system, IEEE Trans. on Commun., 1994, COM-42(2/3/4), 1524–1527.

[2] G. Mazzini, G. Setti, R. Rovatti, Chaotic complex spreading sequences for asynchronous DS-CDMA-Part I: System modeling and results, IEEE Trans. on Circuits and Syst., 1997, CAS-I, 44(10), 937–947.

[3] R. Rovatti, G. Setti, G. Mazzini, Chaotic complex spreading sequences for asynchronous DS-CDMA-Part II: Some theoretical performance bounds, IEEE Trans. on Circuits and Syst., 1998, CAS-I, 45(4), 496–506.

[4] Ling Cong, Li Shaoqian, Chaotic spreading sequences with multiple access performance better than random sequences, IEEE Trans. on Circuits and Syst., 2000, CAS-I, 47(3), 394–397.

[5] 凌聪，孙松庚，混沌扩频序列发生器，电子科学学刊，1998, 20(2), 235–240.

[6] K. Kelber, M. Gotz, W. Schwarz, Generation of signals with n-dimensional uniform probability distribution by digital filter structures, Proc. of the 7th IEEE Digital Signal Processing Workshop (DSPWS'96), Loen, Norway, September 2-4, 1996, 486–489.

[7] 荆涛，徐勇，杨怀江，宋建中，一种基于神经网络的混沌序列产生方法，通信学报，1999, 20(6), 77–81.

[8] Ren Yong, Xia Yongxiang, Shan Xiuming, Yuan Jian, Driving synchronization of spatiotemporal chaos and its application in CDMA communications, International Journal of Bifurcation and Chaos, 2001, 11(12), 3117–3124.

[9] E. J. Groth, Generation of binary sequences with controllable complexity, IEEE Trans. on Info. Theory, 1971, IT-17(3), 288–296.

[10] K. H. Karkkainen, Comparison of performance between AND and majority logic type nonlinear feedforward logic pseudonoise sequence generators, IEICE Trans. on Fundamentals, 1999, E82-A(8), 1641–1647.

[11] 杨义先，林须端，编码密码学，北京，人民邮电出版社，1992, 第十五章、第十六章.

[12] E. L. Key, An analysis of the structure and complexity of nonlinear binary sequence generator, IEEE Trans. on Info. Theory, 1976, IT-22(6), 732–736.

[13] M. B. Pursley, Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part I: System analysis, IEEE Trans. on Commun., 1977, COM-25(8), 795–799.

[14] K. H. Karkkainen, P. A. Leppanen, Comparison of the performance of some linear spreading code families for asynchronous DS/SSMA systems, MILCOM'91, Mclean, Virginia, USA, November 4-7, 1991, 784–790.

COMPARISON OF PERFORMANCE BETWEEN CHAOTIC SEQUENCES AND NONLINEAR SEQUENCES BASED ON SHIFT REGISTER

Mi Liang　　Zhu Zhongliang

(*Southwest Electronic & Telecommunication Technology Institute, Chengdu* 610041, *China*)

Abstract　Both chaotic sequences and nonlinear feed-forward logic (NLFFL) sequences based on linear shift register almost have the same properties: the ease of their generation and various families with a large family size and long sequence period, as well as their broadband noise-like and non-linear nature. Their generation methods, correlation properties, Code Division Multiple Access (CDMA) properties and their resistance against correlation attack are compared in the paper. By simulation, it shows that most of their properties are comparable, but chaotic sequences are less vulnerable to correlation attack and jamming than some NLFFL sequences when their period is less than or equal to 1023, so they have more practical value than these nonlinear sequences based on shift register.

Key words　Chaotic sequences, Nonlinear sequences, Correlation attack

米　良：　男，1970 年生，博士生，主要研究方向为抗干扰通信技术、混沌理论及其应用等.

朱中梁：　男，1936 年生，研究员，博士生导师，中科院院士. 研究方向为通信信息处理.