第 37 卷 第 19 期
Vol.37 No.19

计 算 机 工 程
Computer Engineering

2011 年 10 月
October 2011

• 专栏 •

文章编号：1000—3428(2011)19—0012—05 文献标识码：A 中图分类号：TP309.7

级联混沌系统 Lyapunov 指数研究

金建国[a]，魏明军[a]，邸志刚[b]，许广利[a]，贾春荣[b]，赵宏微[a]

(河北联合大学 a. 理学院；b. 电气工程学院，河北 唐山 063009)

摘 要：在现有变参级联混沌通信系统中，系统密钥出现短周期态会导致密钥泄漏。针对该问题，分析级联混沌系统中 Lyapunov 指数随级联子系统参量变化的分布情况以及实时加解密系统的安全性，指出即使各独立子系统的 Lyapunov 指数均为正，其级联系统的 Lyapunov 指数也可能为负，负 Lyapunov 指数将导致密钥泄漏。为此，设计一个短程相关性线程对系统密钥进行实时监测，防止短周期态的发生，从而较好解决密钥泄漏问题。

关键词：级联混沌系统；Lyapunov 指数；级联子系统；密钥泄漏

Research on Lyapunov Exponent of Cascade Chaos System

JIN Jian-guo[a], WEI Ming-jun[a], DI Zhi-gang[b], XU Guang-li[a], JIA Chun-rong[b], ZHAO Hong-wei[a]

(a. College of Sciences; b. College of Electrical Engineering, Hebei United University, Tangshan 063009, China)

【Abstract】According to the encrypt leakage of existing variable parameters cascade chaotic real-time secure communication system which occurs because of the emergence of short periodic state, this paper analyzes the Lyapunov exponents which vary with parameters in cascade system and the security of encryption and decryption in real-time variable parameters cascade chaotic system, points that even all the Lyapunov exponents in every independent subsystem are positive, the Lyapunov exponents in cascade system may be negative, and negative Lyapunov exponents will lead to secret key leakage. According to the problem, it designs a short-range correlation thread for real-time monitoring of system secret key to prevent the occurrence of short period state, result shows that this method can solve the secret key leakage problem.

【Key words】cascade chaos system; Lyapunov exponent; cascade subsystem; secret key leakage

DOI: 10.3969/j.issn.1000-3428.2011.19.004

1 概述

近 20 年，混沌加密成为国际上研究的一个热点。利用混沌加密的重要原因之一是它可以高效、便捷地实现一密一钥[1]。为了防止数字混沌退化及相空间重构[2]等方法的攻击，提高系统的密钥周期长度和混乱度等，通常采用变参、扰参、变步长、恒 Lyapunov 指数谱[3]级联混沌[4]等常见方法达到提高密钥质量的目的。

然而，笔者在文献[4]基础上进行变参级联混沌系统研究时发现，即使各个独立子系统 Lyapunov 指数均为正，其级联系统的 Lyapunov 指数也有出现负的情况。负 Lyapunov 指数使系统进入周期 1 或周期 2 等周期状态。系统进入周期态将发生密钥泄漏。特别是对于实时语音级联变参混沌通信系统极易发生该情况。尽管人们关于级联混沌系统方面已经开展大量的理论与实验研究[4-5]，但关于同构异参的 m 级子系统构成的级联系统的 Lyapunov 指数的研究仍较少。

本文对同构异参的 m 级子系统构成的级联系统的 Lyapunov 指数的值计算和在理论上进行探讨，并对级联系统 Lyapunov 指数随子系统参量全局变化的分布进行研究，为系统安全性、密钥(混乱度)质量科学评价提供重要依据。

2 级联混沌系统 Lyapunov 指数

2.1 级联子系统的 Lyapunov 指数

本文讨论重点是级联混沌系统的 Lyapunov 指数，为方便起见，采用 Logistic 模型为构成级联的元素，其表达式为 $x_{i+1}=f_1(\mu,x_i)=1-\mu x_i^2$。取 m 个子系统参量各异($\mu_i \neq \mu_j$)的混沌构成级联加密系统，如图 1 所示。

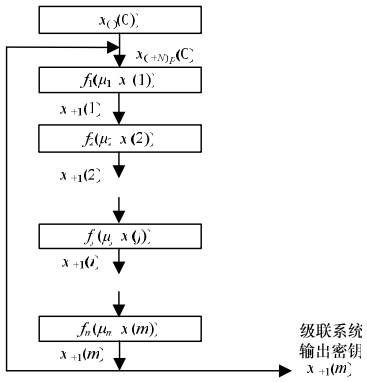

图 1 混沌级联模型

各子系统方程为：

$$\begin{cases} x_{i+1}(1)=f_1(\mu_1,x_i(1)) \\ x_{i+1}(2)=f_2(\mu_2,x_i(2)) \\ \quad\vdots \\ x_{i+1}(j)=f_j(\mu_j,x_i(j)) \\ \quad\vdots \\ x_{i+1}(m)=f_m(\mu_m,x_i(m)) \end{cases} \tag{1}$$

基金项目：河北省教育厅自然科学基金资助项目(2008451, 2008457)

作者简介：金建国(1956－)，男，教授，主研方向：信息安全，混沌加密；魏明军，副教授；邸志刚，讲师、博士；许广利、贾春荣、赵宏微，讲师、硕士

收稿日期：2011-04-07 **E-mail：**jjg@heut.edu.cn

为使 m 个子系统实现级联驱动，上一级(第 j 级)的第 i 次输出 $x_{i+1}(1)$ 作为下一级(第 j+1 级)的第 i 次输入 $x_i(j+1)$。最后一级(第 m 级)的第 i 次输出 $x_{i+1}(m)$ 作为下一个轮次(第 i+1 次)的第 1 级的输入 $x_{i+1}(1)$，从而实现闭合循环级联驱动。在式(1)中取：

$$\begin{cases} x_i(j+1)=x_{i+1}(j) \quad j=1,2,\cdots,(m-1) & \text{(1a)} \\ x_{i+1}(1)=x_{i+1}(j) \quad j=m & \text{(1b)} \end{cases}$$

设 m 次级联系统的函数为 $F_m(x)$，则 $F_m(x)$为由 $f_j(\mu_j,x)$ 构成的 m 次嵌套(复合)函数，即：

$$F_m(x)=f_m(\mu_m,f_{m-1},f_{m-2}(\mu_{m-2},\mu_{m-3},\cdots, f_j(\mu_j,\mu_{j+1},\cdots,f_2(\mu_2,f_1(\mu_1,x)))))$$

设 $F'_{mm}(x)$为 $F_m(x)$ 的导数，并且将 $f_j(\mu_1,x)$ 记为 f_j，则：

$$F'_m(x)=\frac{d}{dx}F_m(x)=\frac{\partial f_m}{\partial f_{m-1}}\frac{\partial f_{m-1}}{\partial f_{m-2}}\cdots\frac{\partial f_j}{\partial f_{j-1}}\cdots\frac{\partial f_2}{\partial f_1}\frac{\partial f_1}{\partial x} \tag{2}$$

由于 $F_m(x)$ 是 $f_j(\mu_1,x)$ 的 m 次嵌套，因此令：

$$f'_j=\frac{\partial f_j}{\partial f_{j-1}} \tag{3}$$

将式(3)代入式(2)得：

$$F'_m(x)=f'_m f'_{m-1}\cdots f'_j\cdots f'_2 f'_1=\prod_{j=1}^{m}f'_j \tag{4}$$

其中，式(4)中 f'_j 的原函数 f_j 为 $f_j=f_j(\mu_j,x(j))$，f_j 为第 j 个子系统函数。将第 j 个子系统的第 i 次迭代值记为 $f_{j,i}$，有 $f_{j,i}=f_j(\mu_j,x_i(j))$。因此，第 j 个子系统的第 i 次迭代的导函数值 $f'_{j,i}$ 为：

$$f'_{j,i}=f'_{j,i}(u_j,x_i(j)) \tag{5}$$

式(4)、式(5)联立得到级联系统的第 i 次迭代导函数值为：

$$F'_m(x_i)=\prod_{j=1}^{m}f'_{j,i} \tag{6}$$

设 $F_m^{(n)}(x)$ 为 $F_m(x)$ 的 n 次迭代，可得 $F_m^{(n)}(x)$ 的一阶导数 $F_m^{\prime(n)}(x)$ 为：

$$F_m^{\prime(n)}(x)=\frac{\mathrm{d}F_m^{(n)}(x)}{\mathrm{d}x}=\prod_{i=0}^{n-1}F'_m(x_i) \tag{7}$$

设 λ_s 为级联系统 $F_m(x)$ 的 Lyapunov 指数，根据定义有：

$$\lambda_s=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|F'_m(x_i)\right| \tag{8}$$

将式(6)代入式(8)得：

$$\lambda_s=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\prod_{j=1}^{m}f'_{j,i}\right|=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=1}^{m}\ln\left|f'_{j,i}\right|= \sum_{j=1}^{m}\left(\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'_{j,i}\right|\right) \tag{9}$$

令：

$$\lambda_j=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'_{j,i}\right| \tag{10}$$

将式(10)代入式(9)得：

$$\lambda_s=\sum_{j=1}^{m}\lambda_j \tag{11}$$

式(11)为级联系统 $F_m(x)$ 的 Lyapunov 指数，式(10)中 λ_j 为第 j 个子系统在级联系统中有前级串扰时的 Lyapunov 指数，结合式(10)、式(11)可看出级联系统 $F_m(x)$ 的 Lyapunov 指数 λ_s 等于有串扰时各级子系统 Lyapunov 指数的代数和。

2.2　级联子系统与孤立(子)系统的 Lyapunov 指数区分

对应图 1，在式(1)中，如果去掉所有其他级次，仅保留第 j 级子系统独立运行。那么第 j 级子系统自身就构成一个孤立(无串扰)子系统，如图 2 所示。

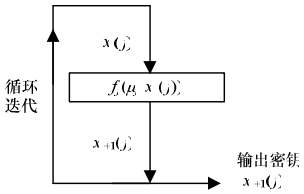

图 2　第 j 级孤立子系统模型

为区别上述有串扰时的 λ_j，设 λ_j^* 为第 j 级孤立子系统(无串扰时)的 Lyapunov 指数，设 $x_i^*(j)$ 为第 j 级(无串扰时)孤立子系统第 i 次迭代值，根据定义得：

$$\lambda_j^*=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'_j(\mu_j,x_i^*(j))\right| \tag{12}$$

其中：

$$x_i^*(j)=f_j(\mu_j,x_{i-1}^*(j))=f_j(\mu_j,x_{i-2}^*(j))= f_j(\mu_j,\mu_{j+1},\cdots,f_j(x_0^*(j))) \tag{13}$$

$x_i^*(j)$ 在式(12)的 n 次迭代中均为来自同一个子系统 $f_j(\mu_j,x_i^*(j))$ 的迭代值，即 $x_i^*(j)$ 不受外界(前级)干扰。

下文分析第 j 级子系统在级联系统中有前级串扰时的 Lyapunov 指数。由式(10)、式(5)联立得有前级串扰时第 j 级子系统 Lyapunov 指数为：

$$\lambda_j=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'_{j,i}(\mu_j,x_i(j))\right| \tag{14}$$

其中：

$$x_i(j)=f_j(\mu_j,x_{i-1}(j)) \tag{15}$$

由于式(14)有前级串扰，因此根据式(1a)将式(15)展开为：

$$x_i(j)=f_j(\mu_j,x_{i-1}(j))=f_j(\mu_j,x_i(j-1))= f_j(\mu_j,f_{j-1}(\mu_{j-1},f_{j-2}(\mu_{j-2},\mu_{j-3},\cdots,f_1(\mu_1,x_i(1))))) \tag{16}$$

从式(16)可看出，有串扰时第 j 个子系统的第 i–1 次迭代 $f_{j,i-1}$ 的值 $x_i(j)$ 受到 f_{j-1} 及以前的逐级串扰。同理，有串扰时第 j 个子系统的第 i 次迭代 $f_{j,i}$ 的值 $x_{i+1}(j)$ 同样受到 f_{j-1} 及以前的逐级串扰，即式(14)的 λ_j 受到 f_{j-1} 以前的逐级串扰。因此，一般情况下有：

$$\lambda_j\neq\lambda_j^* \tag{17}$$

式(17)表明对于第 j 个子系统 $f_j(\mu_j,x(j))$，当 f_j 独立(无串扰)运行时与在级联系统中(受到前级串扰)运行时的 $f_{j,i}$ 两者的 Lyapunov 指数不再相等。

为表述方便，设 λ_s^* 为各级子系统(无串扰)独立运行时的 Lyapunov 指数 λ_j^* 的代数和。因此，根据定义可得：

$$\lambda_s^*=\sum_{j=1}^{m}\lambda_j^* \tag{18}$$

由式(11)、式(17)、式(18)比较可得：

$$\lambda_s\neq\lambda_s^* \tag{19}$$

根据式(19)结合式(11)、式(18)分别说明级联系统 $F_m(x)$ 的 Lyapunov 指数 λ_s，其等于有串扰时各级子系统 Lyapunov 指数 λ_j 的代数和，不等于各级子系统独立运行时的 Lyapunov 指数 λ_j^* 的代数和 λ_s^*。

综上所述可以看出，一般情况对于第 j 个子系统 $f_j(\mu_j,x(j))$，其独立运行时的 Lyapunov 指数 λ_j^* 与其作为级联系统中受到串扰时的第 j 级子系统的 Lyapunov 指数 λ_j 两者不等；级联系统 $F_m(x)$的 Lyapunov 指数 λ_s 等于有串扰时各级

子系统的 Lyapunov 指数 λ_j 的代数和，而不等于各级子系统独立运行时的 Lyapunov 指数 λ_j^* 的代数和。

2.3 级联系统 Lyapunov 指数的数值计算与理论比较

如上所述，关于级联系统的 Lyapunov 指数已经对其中的 λ_j、λ_j^*、λ_s 与 λ_s^* 4 个参数进行了理论分析。级联系统有串扰时系统的 Lyapunov 指数 λ_s 与 λ_j^* 或 λ_s^* 不存在等式函数关系，只存在比较关系。为了便于比较，本文设计了 3 种仿真计算方案，并计算得到了孤立子系统与级联系统中有串扰时子系统的 Lyapunov 指数的参数比较如表 1~表 3 所示。其中，表 1 是级联级次 m=10 的情况，表 2、表 3 均是 m=5 的情况，但两者区别是子系统的参数 μ 值大小排序不同。表 2 中的 μ_j 值大小为倒序，表 3 中的 μ_j 值大小为正序。以表 1 为例，第 1 列 j 代表第 j 个子系统编号为 j；第 2 列 μ_j 代表第 j 个子系统的参量的取值；第 3 列 λ_j^* 代表第 j 个子系统独立运行(无串扰)时该子系统的 Lyapunov 指数，参照图 2、根据式(12)、式(13)得到表 1 中 λ_j^* 的各个数值；第 4 列 λ_j 代表第 j 个子系统在级联串扰运行时子系统的 Lyapunov 指数，根据式(14)、式(16)得到表 1 中 λ_j 的各个数值。表 2、表 3 中各列数据意义同上。另外，在上述计算过程中对所有参量、变量均取 double 型。为了确保所得结果 Lyapunov 指数 λ_j^* 和 λ_j 的统计特性，在对每个 λ_j^* 或 λ_j 的值计算过程中均各取 100 000 个轨道点对其求平均。

表 1 当 m=10 时子系统 Lyapunov 指数的参数比较

j	μ_j	λ_j^*	λ_j	$\lambda_j-\lambda_j^*$
1	2.00	0.693 147 882	0.414 166 778	–0.278 981 100
2	1.90	0.549 569 492	0.734 268 944	0.184 699 452
3	1.80	0.403 985 295	0.452 132 571	0.048 147 276
4	1.75	–1.29E–06	0.437 549 791	0.437 551 079
5	1.60	0.369 930 126	0.339 829 223	–0.030 100 900
6	1.50	0.241 631 862	0.139 287 476	–0.102 344 390
7	1.99	0.649 343 790	0.750 856 566	0.101 512 776
8	1.75	–1.29E–06	0.590 278 582	0.590 279 870
9	1.85	0.503 290 596	0.420 815 458	–0.082 475 140
10	1.45	0.170 923 581	0.211 753 873	0.040 830 292

表 2 当 m=5、μ_j 为倒序时子系统 Lyapunov 指数的参数比较

j	μ_j	λ_j^*	λ_j	$\lambda_j-\lambda_j^*$
1	2.0	0.693 147 882	0.507 523 018	–0.185 624 860
2	1.9	0.549 569 492	0.751 954 705	0.202 385 213
3	1.8	0.403 985 295	0.494 675 512	0.090 690 217
4	1.7	0.435 665 967	0.237 293 534	–0.198 372 430
5	1.6	0.369 930 126	0.413 726 701	0.043 796 575

表 3 当 m=5、μ_j 为正序时子系统 Lyapunov 指数的参数比较

j	μ_j	λ_j^*	λ_j	$\lambda_j-\lambda_j^*$
1	1.6	0.369 930 126	1.163 039 058	0.793 108 932
2	1.7	0.435 665 967	0.712 389 646	0.276 723 679
3	1.8	0.403 985 295	0.335 923 371	–0.068 061 920
4	1.9	0.549 569 492	1.017 642 335	0.468 072 843
5	2.0	0.693 147 882	–3.549 164 947	–4.242 312 830

将表 1 中第 3 列 λ_j^* 数据代入式(18)可得各级子系统独立运行时的 Lyapunov 指数 λ_j^* 的代数和 λ_s^* 为：

$$\lambda_{s1}^* = \sum_{j=1}^{m} \lambda_j^* = 3.581\ 820\ 04$$

同理，将表 1 中第 4 列 λ_j 数据代入式(11)可得有串扰时各级子系统的 Lyapunov 指数 λ_j 的代数和 λ_s 为：

$$\lambda_{s1} = \sum_{j=1}^{m} \lambda_j = 4.490\ 939\ 26$$

绝对误差：

$$\Delta\lambda = \lambda_{s1} - \lambda_{s1}^* = 0.909\ 119\ 214$$

相对误差：

$$(\lambda_{s1} - \lambda_{s1}^*)/\lambda_{s1}^* = 0.253\ 814\ 876 \approx 25\%$$

级联系统的 Lyapunov 指数 λ_s 与各子系统独立运行时 Lyapunov 指数的代数和 λ_s^* 相比，其级联系统 Lyapunov 指数 λ_s 增大了 25%。此时，级联系统系统产生的密钥更适合用于加密。

根据表 2 数据可得子系统独立运行时的 Lyapunov 指数 λ_j^* 的代数和 λ_s^* 为：

$$\lambda_{S2}^* = \sum_{j=1}^{m} \lambda_j^* = 2.452\ 298\ 76$$

同理可得有串扰时各级子系统的 Lyapunov 指数 λ_j 的代数和 λ_s 为：

$$\lambda_{s2} = \sum_{j=1}^{m} \lambda_j = 2.405\ 173\ 47$$

绝对误差：

$$\Delta\lambda = \lambda_{s2} - \lambda_{s2}^* = -4.712\ 529\ 17\times10^{-2}$$

相对误差：

$$(\lambda_{s2} - \lambda_{s2}^*)/\lambda_{s2}^* = -1.921\ 678\ 24\times10^{-2} \approx -1.9\%$$

此时，λ_s 随为正，但 λ_s 与 λ_s^* 两者相比较，其级联系统系统 Lyapunov 指数 λ_s 减小了 1.9%。

根据表 3 数据可得子系统独立运行时的 Lyapunov 指数 λ_j^* 的代数和 λ_s^* 为：

$$\lambda_{s3}^* = \sum_{j=1}^{m} \lambda_j^* = 2.452\ \ 298\ \ 76$$

同理可得有串扰时各级子系统的 Lyapunov 指数 λ_s 的代数和 λ_s 为：

$$\lambda_{s3} = \sum_{j=1}^{m} \lambda_j = -0.320\ 170\ \ 53$$

绝对误差：

$$\Delta\lambda = \lambda_{s3} - \lambda_{s3}^* = -2.772\ \ 469\ \ 29$$

相对误差：

$$(\lambda_{s3} - \lambda_{s3}^*)/\lambda_{s3}^* = -1.130\ \ 559\ \ 35 \approx -100.13\%$$

此时，λ_s 与 λ_s^* 两者相比较，其级联系统系统 Lyapunov 指数 λ_s 不但减小了 100.13%，且 λ_s 为负。负的 Lyapunov 指数将导致致命的密钥泄漏。

2.4 级联系统 Lyapunov 指数的分布情况

关于级联系统的 Lyapunov 指数，对于其中的 4 个参数 λ_j、λ_j^*、λ_s 与 λ_s^* 的讨论，在上述讨论中采用的是数值计算列表与理论比较的方法。但是，该方法对级联系统 Lyapunov 指数 λ_s 随子系统参量 μ_j 全局变化的分布将不再适用。下面将采用图解比较的方法对级联系统 Lyapunov 指数 λ_s 随子系统参量 μ_j 全局变化的分布进行研究。

参照图 1 在式(1)中，取 m=7，μ_1 作为循环变量，使 μ_2、μ_3、μ_4、μ_5、μ_6、μ_7 各参量保持为常量。其中，μ_1 取值范围为 1~2，步长为 0.000 01；μ_2=1.52；μ_3=1.62；μ_4=1.72；μ_5=1.82；μ_6=1.92；μ_7=2.00。对应各子系统(无串扰)独立运行的

Lyapunov 指数分别为：

$\lambda_2^* = 0.281\,476\,142\,835\,619$

$\lambda_3^* = 0.374\,390\,008\,890\,639$

$\lambda_4^* = 0.437\,856\,001\,805\,404$

$\lambda_5^* = 0.465\,346\,075\,835\,066$

$\lambda_6^* = 0.570\,009\,012\,259\,970$

$\lambda_7^* = 0.693\,147\,882\,269\,976$

即 λ_2^*、λ_3^*、λ_4^*、λ_5^*、λ_6^*、λ_7^* 均为正。根据式(10)、式(11)计算得级联系统的 Lyapunov 指数 λ_s 随子系统参量 μ_1 的全局变化分布曲线如图 3 所示，其中，λ_s 的最大值 $\lambda_{s\max}$=3.406；为了便于比较，本文同时根据式(12)、式(13)绘制对应 μ_1 的单级(独立)子系统的 Lyapunov 指数 λ_1^* 随 μ_1 全局变化的分布，如图 4 所示，其中，λ_1 的最大值 $\lambda_{1\max}$=0.693 1，绘出 λ_1 是为了通过 λ_s 与 λ_1^* 横标比较以便于对 λ_s 的横标定位。

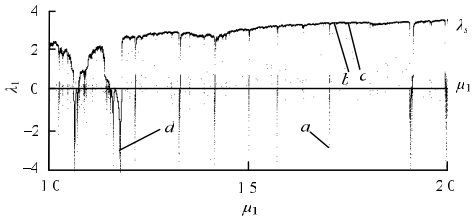

图 3　Lyapunov 指数 λ_s 随子系统参量 μ_1 全局变化的分布情况

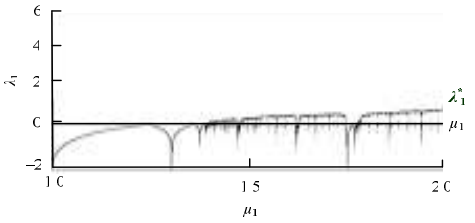

图 4　Lyapunov 指数 λ_1 随子系统参量 μ_1 全局变化的分布情况

根据对图 3、图 4 的比较可以看出，当 λ_1^*、λ_2^*、λ_3^*、λ_4^*、λ_5^*、λ_6^*、λ_7^* 均为正时，其级联级联系统(图 3 中的 *b* 位置) λ_s 可以为正(表 2 对应这种情况)，λ_s (图 3 中 *a* 位置)可能为负(表 3 对应 Lyapunov 指数 λ_s =−0.320 170 53<0 就属于这种情况)；从图 3、图 4 可看出，当 λ_1^* 为负时，其级联系统(图 3 横坐标位于 *c* 位置，其恰位于对应图 4 的 μ_1 值为 1.749~1.809 范围的周期 3 窗口内) λ_s 可以为正，λ_s (图 3 横坐标位于 *d* 位置)可能为负。总之，λ_s 是 μ_j 的函数(j=1,2,⋯,m)，由于 λ_s 的非线性和高度复杂性，因此从式(10)、式(11)无法直接观察或预测出它的变化规律或正负。即使对简单的单级情况，也仅是在 μ_∞ 附近具有非线性关系[6]，其表达式为：

$$\lambda^*(\mu) \propto \left|\mu - \mu_\infty\right|^\beta \quad \beta = 0.449\ 8$$

图 3 反映了级联系统 Lyapunov 指数 λ_s 随子系统参量 μ_j 全局变化的整体分布情况。λ_s 的整体分布图对于子系统参量 μ_j 的取值变化范围的选取具有理论上的指导意义(关于 λ_s 更精细的细节展开图及深入讨论，受篇幅所限，这里从略)。

3　实验结果及对策分析

3.1　实验结果分析

综合表 1、表 2、表 3 的实验数据和相应计算可看出，由表 1 计算得到的 λ_s 与 λ_s^* 两者相比，其级联系统系统 Lyapunov 指数 λ_s 增大 25%；对应表 2 其级联系统系统 Lyapunov 指数 λ_s 减小 1.9%；对应表 3 其级联系统系统 Lyapunov 指数 λ_s 减小 100.13%。综上所述，关于 λ_j、λ_j^*、λ_s 与 λ_s^* 4 个参数可得到以下结论：

(1)对于同构异参级联系统，由于非线性的存在，因此第 j 级子系统在级联系统中有前级串扰时的 Lyapunov 指数 λ_j 与第 j 级孤立子系统无串扰时的 Lyapunov 指数 λ_j^* 一般情况下不再相等。

(2)当构成级联系统的子系统所选参量各不相同时，级联系统 Lyapunov 指数 λ_s 不等于各子系统独立运行时 Lyapunov 指数的代数和 λ_s^*。由于非线性的存在，因此导致级联系统的 Lyapunov 指数 λ_s 与各子系统独立运行时 Lyapunov 指数的代数和 λ_s^* 相比，λ_s 有时会随子系统所选参量的选取不同而增大(见表 1)，有时会出现随子系统所选参量的不同而变小(见表 2、表 3)。

(3)从表 2、表 3 可见，即使构成级联系统的子系统所选两组参量完全相同，如果子系统的所选参量排序不同，则级联系统的 λ_s 也会随子系统所选参量排序不同而增大或变小程度也显著不同。

(4)从表 3 可见，尽管构成级联系统的各子系统独立运行时的 Lyapunov 指数 λ_j^* 均为正($\lambda_j^*>0$, j=1,2,3,4,5)，但其构成的级联系统 Lyapunov 指数 λ_s 却为负。换言之，由 Lyapunov 指数 λ_j^* 均为正的子系统构成的级联系统的 Lyapunov 指数 λ_s 不一定是正的，其值 λ_s 可能为负，也可能为正。这是非线性的必然反映。

(5)由于级联系统的 Lyapunov 指数 λ_s 随子系统所选参量变化呈非线性变化关系，因此其因果规律没有一般性的解析解。即不能据一般性的解析解预测级联系统的 Lyapunov 指数 λ_s 的具体数值大小或正负。只能是各案处理，采用数值迭代法一案一解，或采用图解方法研究全局分布规律。

3.2　实时语音加解密系统中发现的问题与对策

在文献[4]的实时语音加解密系统中，对于出现表 3 中的数据情况，尽管各子系统独立运行 Lyapunov 指数 λ_j^* 均为正，但系统的 λ_s 为负，λ_{s3} =−0.320 170 53，λ_{s3} 为负说明级联系统没有进入混沌态，而是进入周期态，经实际计算得知此时系统进入了周期 1 态，具体各子系统不动点数据为：

$x(1)$=−0.599 669 477 472 335

$x(2)$=0.388 674 080 239 696

$x(3)$=0.728 078 426 829 688

$x(4)$=−7.186 571 668 107 43E−03

$x(5)$=0.999 896 706 375 318

系统处于周期态时所产生的密钥是糟糕的随机数，糟糕的随机数是不能作为密钥使用。另外，当级联系统总的 Lyapunov 指数 λ_s 为负时，构成级联系统某些子系统的 Lyapunov 指数 λ_j 即使大于 0，其具体数值也不再具有实际意义。因为，总体已进入周期态，各子系统也一定进入了周期态，此时只是起到中间过程量的作用。当 λ_s 为正时，λ_j 的数值才具有实际意义，它反映了有串扰时第 j 个子系统产生的密钥 $x_{i+1}(j)$(对应相关性)的相关程度或混乱度。

综上所述，由于变参级联系统的 Lyapunov 指数 λ_s 不能预测，因此只能通过实时计算才能知其正负。为了有效避免 Lyapunov 指数 λ_s 为负时产生糟糕的随机数作为密钥，本文

采用一个用于密钥短程相关性监测的专门线程对系统密钥进行实时监测。其总体方案是在文献[4]的方案中加开了一个相关性监测线程，如图 5 所示。

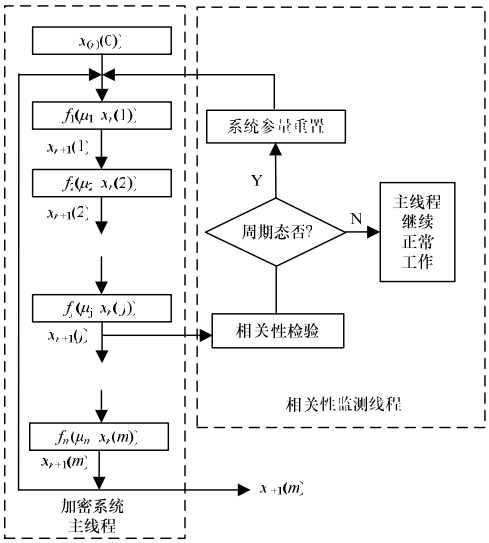

图 5 短程相关性监测线程

由于该线程的任务只是专门防止周期态的出现，并且只要其中一个子系统的端口每组数据的最后 n 个点数据进入周期态，则整个系统必进入周期态。因此为了满足实时性的要求，本文所采用的专线程是在文献[4]方案的 m 个端口中只对其中一个子系统端口的 1 024 为一组的最后 16 个密钥数据点进行短程相关性计算。短程相关性实时监测线程如果监测到有周期态发生，则以消息方式通知产生密钥主线程重新改变子系统参数，且重新产生密钥。在文献[4]系统中的检验测试表明，该方案有效，较好地解决了因系统密钥出现短周期而产生密钥泄漏的问题，且较好地满足实时性要求。因受篇幅所限，关于 2 个系统同步问题参见文献[4]，相关性的细节讨论、检验测试等细节也不再赘述。

4 结束语

本文针对现有变参混沌级联实时保密通信系统中因短周期态的出现而发生的密钥泄漏问题，提出一种密钥保护方案。通过采用短程相关性实时监测的方法，实现了密钥实时保护。对级联系统 Lyapunov 指数随子系统参量全局变化的分布进行分析，其结果在理论上为系统安全性、密钥质量的科学评价提供了重要依据。系统测试和分析结果表明，该方案有效、安全，较好地解决了密钥泄漏的问题。

参考文献

[1] Alvarez G. Security Problems with a Chaos-based Deniable Authentication Scheme[J]. Chaos, Solitons and Fractals, 2005, 26(1): 7-11.

[2] Huang Fangjun, Guan Zhihong. Cryptosystem Using Chaotic Keys[J]. Chaos, Solitons and Fractals, 2005, 23(3): 851-855.

[3] 李春彪, 王翰康. 推广恒 lyapunov 指数谱混沌系统及其演变研究[J]. 物理学报, 2009, 58(11): 7514-7523.

[4] 金建国, 林 瑞, 张庆凌, 等. 基于混沌级联的语音频域实时加密系统[J]. 计算机工程, 2009, 35(11): 137-139.

[5] 周黎晖, 彭召旺, 冯正进, 等. 混沌加密系统的保密性能[J]. 上海交通大学学报, 2001, 35(1): 133-136.

[6] 郝柏林. 从抛物线谈起——混沌动力学引论[M]. 上海: 上海科学技术出版社, 1993: 122-125.

编辑 陆燕菲

(上接第 11 页)

[2] 刘 强, 崔 莉, 陈海明. 物联网关键技术与应用[J]. 计算机科学, 2010, 37(6): 1-10.

[3] 孙其博, 刘 杰, 黎 彝, 等. 物联网: 概念、架构与关键技术研究综述[J]. 北京邮电大学学报, 2010, 33(3): 1-9.

[4] 刘尚合, 孙国至. 复杂电磁环境内涵及效应分析[J]. 装备指挥技术学院学报, 2008, 19(1): 1-5.

[5] 刘尚合, 原 亮, 褚 杰. 电磁仿生学——电磁防护研究的新领域[J]. 自然杂志, 2009, 31(1): 1-7.

[6] Mahdavi S J S, Mohammadi K. Reliability Enhancement of Digital Combinational Circuits Based on Evolutionary Approach[J]. Microelectronics Reliability, 2010, 50(3): 415-423.

[7] 朱继祥, 李元香, 夏学文, 等. 基于演化硬件的在线自适应系统[J]. 计算机科学, 2009, 36(7): 267-287.

[8] 褚 杰, 原 亮, 赵 强, 等. 基于 TMR-EHW 的高可靠性电机控制系统[J]. 计算机工程, 2009, 35(23): 10-11, 14.

[9] Yao Rui, Wang Youren, Yu Shenglin, et al. Research on the Online Evaluation Approach for the Digital Evolvable Hardware[C]//Proc. of ICES'07. Wuhan, China: [s. n.], 2007: 57-66.

[10] Sekanina L. Evolutionary Functional Recovery[M]. [S. l.]: ACM Press, 2000.

[11] Wang Jin, Chen Wen, Lee Chong Ho. Design and Implementation of a Virtual Reconfigurable Architecture for Different Applications of Intrinsic Evolvable Hardware[J]. IET Computers & Digital Techniques, 2008, 2(5): 386-400.

[12] Tempesti G, Vannel F, Mudry P A. A Novel Platform for Complex Bio-inspired Architectures[C]//Proc. of IEEE Workshop on Evolvable and Adaptive Hardware. Hawaii, USA: [s. n.], 2007: 8-14.

[13] 陈利光. 适合于硬件进化的 FPGA 平台设计实现[D]. 上海: 复旦大学, 2009.

[14] Yang Huaqiu, Chen Liguang, Liu Shaoteng, et al. A Flexible Bit-stream Level Evolvable Hardware Platform Based on FPGA[C]//Proc. of AHS'09. San Francisco, California, USA: IEEE Press, 2009: 51-56.

[15] Stomeo E, Kalganova T, Lambert C. Generalized Disjunction Decomposition for Evolvable Hardware[J]. IEEE Transactions on Systems, Man and Cybernetics, 2006, 36(5): 1024-1043.

[16] Stomeo E, Kalganova T, Lambert C. Analysis of Genotype Size for an Evolvable Hardware System[J]. Proceedings of Word Academy of Science, Engineering and Technology, 2005, (7): 74-79.

[17] Stomeo E, Kalganova T, Lambert C. Chose the Right Mutation Rate for Better Evolve Combinational Logic Circuits[J]. International Journal of Computational Intelligence, 2005, 2(4): 268-277.

[18] Movsovic K, Stomeo E, Kalganova T. Feasibility of the Evolutionary Algorithm Using Different Behaviours of the Mutation Rate to Design Simple Digital Logic Circuits[J]. Proceedings of World Academy of Science, Engineering and Technology, 2006, (12): 324-327.

编辑 金胡考