

对利用密度分布来攻击整数 Logistic Map 的考察

宋寒松, 董际国

(上海海潮新技术研究所 上海市 200070)

摘要: 我们通过计算机实验确认了计算精度 N 比特的整数 logistic map $X_{t+1} = [4X_t(2^N - X_t)2^{-N}]$ 与 logistic map $x_{t+1} = 4x_t(1 - x_t)$ 有着近似的密度分布, 进而给出了整数 logistic map 的数值系列 $\{X_t\}$ 中任意一个数值 X_t 属于被检索区间 $(0, 2^m)$ 的概率的近似值。

关键词: Logistic map; 整数 logistic map; 密度分布函数

An Investigation of Attack on Integer Logistic Map Using Density Distribution

SONG Han-song, DONG Ji-guo

(Shanghai Haichao Institute of New Technology, Shanghai 200070, China)

Abstract: We have verified that the logistic map $X_{t+1} = [4X_t(2^N - X_t)2^{-N}]$ of the calculated precision N bits has an approximate density distribution with the logistic map $x_{t+1} = 4x_t(1 - x_t)$, and then give an approximation of the probability that any X_t of the numerical values of the integer logistic map $\{X_t\}$ belongs to the retrieved interval $(0, 2^m)$.

Key words: Logistic map; Integer logistic map; Density distribution function

1. 前言

由于混沌具有初值敏感性, 遍历性, 混合性, 确定性, 和伪随机性等的动力学性质, 而这些性质与密码学中两大基本原则“混淆”和“扩散”相对应, 使得研究者们期待能利用混沌来构建更为安全的通信系统和密码体制 [1]。

一方面, 随着计算机技术和通讯技术的发展, 作为产业技术的信息处理和传输已经数字化, 也就是说, 所有的信息处理已离不开计算机。并且, 作为产业技术的信息处理, 必须要有再现性。

另一方面, 作为自然现象的混沌, 不具有再现性。而定义于实数的混沌函数则无法用有限精度的数字计算机来计算, 也就是严格地说, 产业技术无法利用混沌。

作为产业技术的成果, 产品有寿命, 因此并不需要无限, 也无法利用无限 (混沌)。但是, 如同

伪随机数时, 我们也可以利用数字混沌, 只要其足够像混沌: 有着我们需要的特性。

在应用上, 数字混沌所存在的最大问题是在有精度下的特性退化 [1]。因此, 用混沌函数来产生数字混沌序列, 并以此来产生伪随机数时, 需要知道该数字混沌序列的主要特性有了什么变化? 以确定该数字混沌序列是否可以应用。

我们提出了对整数 logistic map (L M A P) $X_{t+1} = [4X_t(2^N - X_t)2^{-N}]$, $(0 < X_t < 2^N)$, $t = 0, 1, \dots$ 所产生的数值系列进行搅拌来产生伪随机数的方法 [2-3]:

$$R_t = H(X_t) = [4X_t(2^N - X_t) / 2^N] \oplus (4X_t(2^N - X_t) \bmod 2^N)$$

显然, 在利用数字混沌来产生伪随机数系列时, 我们想要知道所产生的数值系列与原来的混沌函数所产生的系列有什么不同。因此, 我们考察了整

数 LMAP 的一些主要性质，如初值敏感性，周期性及系列进入不动点的轨道的检出方法 [4-5]。

我们已经知道 L M A P $x_{t+1} = 4x_t(1-x_t)$, $0 < x_t < 1, t = 0,1,\dots$ $\mu(x) = 1/(\pi\sqrt{x(1-x)})$ 的密度分布函数。而对于整数 LMAP，我们难以导出其密度分布函数。根据经验，我们已经知道其产生的数值系列与 LMAP 同样有着 U 字形分布。但是，由于我们没有整数 LMAP 的密度分布函数，因而无法得到其在高计算精度时的，任意值域区间的密度分布。如果我们能够确认整数 LMAP 与 LMAP 有着同等或者相近的密度分布，那么我们就可以利用 LMAP 的密度分布函数来对整数 LMAP 所产生的数值系列来做一些（近似的）分析。

本文以计算机数值计算实验来确认整数 LMAP 的密度分布是否与 LMAP 的密度分布一致。由于用搅拌函数 H 来产生伪随机数 $R_t = H(X_t)$ 的伪随机数产生法所产生的伪随机数 R_t 和 X_t 之间是 1 对 1 的关系，虽然 R_t 显示出均匀分布的统计特性，但 X_t 的系列呈 U 字形的分布，也就是，整数 LMAP 所产生的系列中，其值域两端比值域中间的值的出现频度要高得多。因此，我们可以容易地想象出对于某一值域区间的 X_t 所对应的 R_t 建立数据库。也就是说，可以利用 X_t 的系列呈 U 字形分布的特性，来提高对 X_t (R_t) 的检出（攻击成功）率。

本文将给出对于计算精度 N 比特时的，值域区间 $(0,2^m)$ 内的，任意的 X_t 的检出概率 ($m < N$ 为整数)。由此，我们可以逆算出在一定的 X_t 的检出概率下的，可能建立的数据库的容量时的，保障安全所需要的计算精度 N 。也就是，可以作为在系统设计时的决定计算精度 N 的一个指标。

本文的构成如下。2. 是介绍整数 LMAP 及其主要性质，3. 是关于 LMAP 的任意区间的分布密度。4. 是通过计算机数值实验来考察计算精度 N 比特时的整数 LMAP 的区间密度。并给出整数 LMAP 的数值系列 $\{X_t\}$ 中任意一个数值 X_t 属于被检索区间 $(0, 2^m)$ 的概率的近似值。最后，5. 是结语。

2. 整数 LMAP 及其主要性质

2.1 整数 LMAP

2.1.1 整数 LMAP

对于混沌函数 LMAP:

$$x_{t+1} = 4x_t(1-x_t), \quad 0 < x_t < 1, \quad t = 0,1,\dots \quad (1)$$

我们定义了其整数计算的形态:

$$X_{t+1} = \left[4X_t(2^N - X_t) / 2^N \right] \quad (2)$$

$0 < X_t < 2^N, t = 0,1,\dots$, $[]$ 为舍去小数点以下的部分的计算 [2-3]。

显然，当 $N \rightarrow \infty$ 时，式 (1) 和式 (2) 等价。

由于几乎所有的计算机都备有高速乘法器，而对于高精度的式 (2) 的计算，可以用分割计算的方法，利用高速乘法器来实现。而在 FPGA 上实现式 (2) 的计算，显然可以通过并列计算来得到更高的速度。

随机数的产生速度依存于所使用的计算机和编程方法。表1为各计算精度时的随机数的产生速度的一例。表中， N 为计算精度， S 为随机数的产生速度，PC为使用Genuine Intel(R) 1.50GHz的笔记本电脑，MC为使用ATmega168V 8MHz的8位微型计算机。

N (bit)		3	64	96	12	16	19	22	25
		2			8	0	2	4	6
S	PC(Gbps)	1.9	1.0	0.7	0.5	0.5	0.4	0.3	0.3
	MC(Kbps)	26	16	12	10	80	67	60	54

表 1 计算精度和随机数产生速度

2.1.2 利用整数 logistic map 的随机数产生法

我们提出了利用整数 LMAP 来产生伪随机数的搅拌方法:

$$R_t = \left[4X_t(2^N - X_t) / 2^N \right] \oplus (4X_t(2^N - X_t) \bmod 2^N) \quad (3)$$

我们对用上搅拌方法产生的随机数，进行了 8 项目的统计检定，确认了其具有良好的统计学的均等分布特性 [3]。

此伪随机数产生方法用整数的乘法，加法，移位，反转来对混沌函数进行计算，从而以小的计算量实现了所产生的随机数具有非线性性。而其特殊的搅拌方法则以最少的计算量实现了所产生的伪随机数具有均匀分布的特性。由于混沌函数的计算具有逆向不可算性（一方向性），又由于搅拌方法采用了 XOR 计算，而 XOR 计算同样具有逆向不可算性，从而使得所产生的伪随机数具有不可推测性。也就是，在计算精度足够长的条件下，所产生的伪随机数是可应用于信息安全领域的，安全的伪随机数。

几乎所有的计算机（包括产业用微型机，单片机）都装备有整数的乘法器，因此，我们可以很容易地实现费用和性能的最佳组合，以较低的费用取得较高的性能。

2.2 整数 LMAP 的主要性质

2.2.1 发散（初值敏感性的存在范围）

对于 $N \geq 2$,

$$X < \frac{3}{8}2^N \text{ 或 } X > \frac{5}{8}2^N \quad (4)$$

时，初值敏感性存在 [4-5]。

2.2.2 收缩

利用式 (3) 的逆对应 $\tilde{X}_{t+1} \rightarrow (\tilde{X}_{t+}, \tilde{X}_{t-})$,

$$\tilde{X}_{t\pm} = \left[\frac{2^N}{2} \pm \frac{\sqrt{2^N(2^N - \tilde{X}_{t+1})}}{2} \right] \quad (5)$$

($1 \leq \tilde{X}_{t+1} < 2^N$ 的任意的整数, $t \geq 0$ 。)

我们可以检出进入任意值（不动点）的轨道（值）[4-5]。

2.2.3 周期性

计算精度 N 和能够得到的平均非周期状态长 L_c 之间的关系 [4,5]:

$$L_c \approx 5 \cdot 2^{N/2-3}$$

3. LMAP 的区间分布密度

本节我们将根据 LMAP 的密度分布函数来导出 LMAP 的任意值域区间 $[x_1, x_2]$ ($0 < x_1 < x_x < 1$) 的密度。

3.1 LMAP 的密度分布函数

LMAP 的密度分布函数如式 (6):

$$\mu(x) = 1/(\pi\sqrt{x(1-x)}) \quad (6)$$

利用式 (6) 我们可以计算出 LMAP 的任意值域区间 $(x_1, x_2]$ 的密度。

3.2 LMAP 的区间分布密度

对于 LMAP 的值域 (0,1) 内的任意微小区间 dx , 当 $dx \rightarrow 0$ 则区间 dx 的密度 P_x 为 $P_x = (1/(\pi\sqrt{x(1-x)}))dx$ 。于是，我们可以得到 LMAP 的任意值域区间 $(x_1, x_2]$ 的密度 P 为:

$$P = \int_{x_1}^{x_2} (1/(\pi\sqrt{x(1-x)}))dx \quad (7)$$

对于式 (7), 我们使 $x = \sin^2 \alpha$, $\alpha : (0, \pi/2)$,

则 $dx = 2 \sin \alpha \cos \alpha$, $\alpha = \arcsin \sqrt{x}$,

由此, 可得

$$P = \int_{\alpha_1}^{\alpha_2} (1/\sqrt{\sin^2 \alpha(1-\sin^2 \alpha)})d(\sin^2 \alpha) \quad (8)$$

在此, $0 < \alpha_1 < \alpha_2 < \pi/2$ 。

由式 (8) 和 $\alpha = \arcsin \sqrt{x}$, 可得式 (9):

$$P = (2/\pi)(\arcsin \sqrt{x_2} - \arcsin \sqrt{x_1}). \quad (9)$$

3.2.1 值域 (0,1) 内 256 等区间分布密度

将区间 (0,1) 分为 256 等份, 也就是 $((0, 1/256], (1/256, 2/256], \dots, (254/256, 255/256], (255/256, 1))$ 。则利用式(9) 可以计算出各区间的分布密度为

$$(0.039815, 0.016529, \dots, 0.016529, 0.039815)$$

此分布密度显示由式 (1) 产生的数值系列的任意一个值属于各区间的概率。

3.2.2 $(0, 2^{-N/2})$ 区间的密度

显然, 由式 (9), 我们可以得到 $(0, 2^{-N/2})$ 区间的密度为:

$$P_0 = (2/\pi)(\arcsin \sqrt{2^{-N/2}}) \quad (10)$$

当 N 分别为 (64, 96, 128, 160, 192, 256) 时, 其 $(0, 2^{-N/2})$ 区间的密度分别为 (9.71e-6, 3.79e-8, 1.48e-10, 5.79e-13, 2.26e-15, 8.83e-18)。此密度显示由式 (1) 产生的数值系列的任意一个值属于 $(0, 2^{-N/2})$ 区间的概率。

4. 计算精度 N 时的整数 LMAP 的区间密度

对于随机数的检定, 我们可以利用 χ (chi) 二乘检定法 [6]。同样, 想要确认整数 LMAP 的密度分布与 LMAP 的密度分布是否一致, 我们可以将 LMAP 的密度分布作为期待值来与由计算机实验得来的整数 LMAP 的密度分布值做比较, 以得出判断。本节, 我们通过计算机数值实验来考察计算精度 N 比特时的整数 LMAP 的区间密度。并与 LMAP 的相同区间的密度做比较, 来考察整数 LMAP 的密度分布与 LMAP 的密度分布是否一致。并给出当计算精度为 N 比特, 计算机的检索可能的数据量为 $N * 2^m / 8$ 字节时, 整数 LMAP 的数值系列 $\{X_i\}$ 中

任意一个数值 X_i 属于被检索区间 $(0, 2^m)$ 的概率的近似值。

4.1 全域 256 区间的密度分布

4.1.1 实验方法

计算精度 N 比特时的整数 LMAP 的值域为 $(0, 2^N)$ 。将区间 $(0, 2^N)$ 分割为 256 等间距的区间。也就是 $([1, 2^N/2^8], (2^N/2^8, 2 \times 2^N/2^8], \dots, (254 \times 2^N/2^8, 255 \times 2^N/2^8], (255 \times 2^N/2^8, 2^N))$ 。对 $N = 64, 96, 128, 160, 192, 224, 256$ 按以下的步骤做实验。

步骤 1. 任意取一个初值 X_0 , 使 $t = 0, T = 2^{24}$ 。

步骤 2. 计算式 (2) 一次, 使 $t = t + 1$ 。

步骤 3. 确定由步骤 2 的计算所得到的 X_t 的所属区间并计数。

步骤 4. 如果 $t < T$ 则重复步骤 2 到步骤 4。

4.1.2 实验结果

整数 LMAP, $N = 256$ 时 X_i 的 256 等区间分布的实验结果如图 1 上的黑点所示。我们将上述 3.2.1 节的 LMAP 的 256 等分割区间的分布密度乘样本数 T , 即可得到 LMAP 的 256 等分割区间的分布数值, 如图 1 上的紫色细线所示。从图 1 的分布图, 我们可以观察到: 整数 LMAP, $N = 256$ 时 X_i 的 256 等区间分布和 LMAP 的 256 等分割区间的分布非常接近。而对其他计算精度的实验也得到了同等的结果。

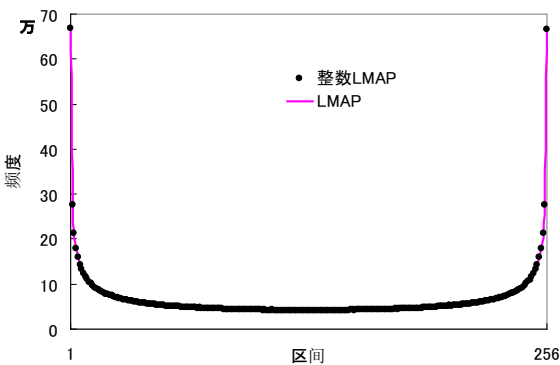


图 1 整数 LMAP 时的 256 等区间分布和 LMAP 的比较
为得到一个更为准确的判断, 我们将 LMAP 的 256 等分割区间的分布值作为期待值, 与整数 LMAP, $N = 64, \dots, 256$ 时 X_i 的 256 等区间分布值做统计量的比较, 也就是 χ 二乘分析。对于 1000 次实验得到的上述统计量的自由度 255 的 χ 二乘值的分布

于 p 的范围的数量如表 2 所示。表中 $N(bit)$ 的列的数值为计算整数 LMAP 时的计算精度。所对应的各列为该计算精度时的, 实验所得到的 χ 二乘值小于某一数值适当的概率 (%) 时的数量。比如, 第一列 1% 时的适当的数量应该是 $1000 \times 1\% = 10$ 左右, 而实验结果却为 70 以上。

$N(bit)$	χ 二乘分布 ($p <$)						
	1 %	5 %	25 %	50 %	75 %	95 %	99 %
64	75	18 1	377	524	697	857	932
96	75	15 1	354	516	670	845	937
128	78	16 9	368	522	694	860	922
160	92	19 6	396	560	716	875	933
192	74	14 7	353	526	690	860	932
224	71	17 3	380	524	675	863	939
256	83	17 5	382	547	698	865	927

表 2 256 区间 χ 二乘值的分布

从表 2 中我们可以看到, 不同计算精度的各 p 的范围的数量各不相同, 但没有大的差异, 也就是说, 并不因计算精度而异。另外, 还显示出以下 2 个特征:

1. 1%, 5%, 25% 的 3 列的数量都明显大于该列的适当的比例。
2. 最后的 3 列的数量都明显小于该列的适当的比例。

由于 χ 二乘值较小, 表示所比较的数值之间较为接近, 因此, 从上述结果我们可以做出以下的推测。上述特征 1 的结果, 显示出当 $N \rightarrow \infty$ 时式 (1) 和式 (2) 等价的, 整数 LMAP 与 LMAP 的共性的部分。而特征 2 的结果, 则显示出当 N 为有限值时式 (1) 和式 (2) 的不同的部分。

对于, 特征 2 的 $P > 99\%$, 我们做了进一步的调查, 其结果如表 3 所示。

N	64	96	128	160	192	224	256
数量	68	63	78	67	68	61	73
平均	33 0.3	328. 2	329. 4	332. 7	335. 5	330. 4	335.2
最小	31 0.7	311. 0	310. 9	310. 7	310. 8	310. 9	311.2
最大	37 6.8	382. 9	421. 9	406. 4	417. 3	409. 3	393.5

表 3 $P > 99\%$ 的 χ 二乘值的数量, 平均, 最小, 最大值

表中 N 行的数值为计算整数 LMAP 时的计算精度。对应的各列为该计算精度时，实验所得到的 χ 二乘值大于 310.634 时的数量和 χ 二乘值的平均，最小，最大值。

从表中我们可以观察到，虽然不同的计算精度下有着不同的数值。但实验结果与计算精度的高低不存在相关关系。其平均值与阈值 310.634 相差不足 10%。即使其最大值也与阈值 310.634 相差不足 36%。

上述实验结果说明，式 (1) 和式 (2) 所产生的系列的密度分布并不同等，但比较接近。因此，我们可以考虑用 LMAP 的密度分布来作为整数 LMAP 的密度分布的近似，来对整数 LMAP 做近似分析。

由于上述实验的 256 区间的分割，相对地比较粗糙。而受计算机的计算能力的限制，我们也无法将实验的区间分割得太细。因此，我们采用做以下的实验，来对整数 LMAP 的密度分布做进一步的观察。

4.2 $(0, 2^{N/2})$ 区间的分布密度

4.2.1 方法

对于计算精度 N 比特时的整数 LMAP 的值域为 $(0, 2^N)$ ，我们对由任意的初值所产生的数值系列中属于区间 $[1, 2^{N/2}]$ 内的值的密度做调查。我们对 $N = 64, 96, 128$ 按以下的步骤做实验。

- 步骤 1. 任意取一个初值 X_0 ，使 $t = 0, T = 2^{32}$ 。
- 步骤 2. 计算式(2)一次，使 $t = t + 1$ 。
- 步骤 3. 如果 $X_t \leq 2^{N/2}$ 则累计其数。
- 步骤 4. 如果 $t < T$ 则重复步骤 2 到步骤 4。

4.2.2 结果

同样，我们将 LMAP 的 $(0, 2^{N/2})$ 区间的分布值作为期待值，与整数 LMAP， $N = 64, 96, 128$ 时 X_t 的 $[1, 2^{N/2}]$ 区间分布值做统计量的比较，也就是 χ 二乘分析。对于 $N = 64, 96$ 的 1000 次， $N = 128$ 的 100 次的实验结果与 LMAP 比较所得到的 χ 二乘表明，式 1 和式 2 所产生的系列的密度分布并不同等，但比较接近。在此，将 $N = 64, 96, 128$ 时的实验所得到的区间 $[1, 2^{N/2}]$ 内的分布密度分别显示于图 2，图 3，图 4。

图 2 中，横向轴表示实验的序号，竖向轴表示系列长 $T = 2^{32}$ 时的在检索区间内的数量。图中黑

点为每次实验进入 $[1, 2^{N/2}]$ 的 X_t 的数量，紫色直线为由式 (10) 计算得来的 $T = 2^{32}$ 时，LMAP 的 $(0, 2^{N/2})$ 区间的分布值 10430.3784。

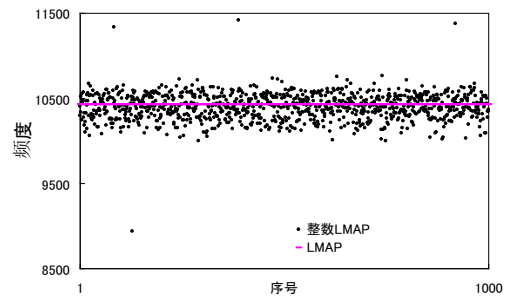


图 2 $N = 64$ 时的区间 $[1, 2^{N/2}]$ 内的 X_t 的数量的分布

从图中，我们可以观察到，在靠近紫色直线附近黑点较密，而即使是离紫色直线最远的点，也在 20% 范围内。这一结果，与上述 4.1 节 256 分割时的实验结果一致。

图 3，图 4 中，紫色直线分别为由 $T = 2^{32}$ ， $T = 2^{37}$ 时，式 (10) 计算得来的，LMAP 的 $(0, 2^{N/2})$ 区间的分布值 162.9747，20.3718。

从图中，我们可以观察到，在靠近紫色直线附近黑点较密，这与图 2 的结果基本上是一致的。由于 $N = 128$ 时的计算量太大，图 4 中显示的是 100 次的实验结果。

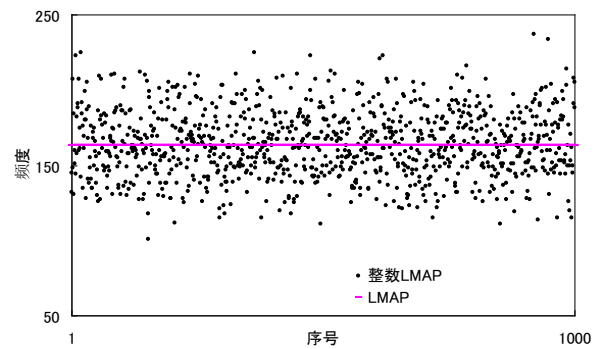


图 3 $N = 96$ 时的区间 $[1, 2^{N/2}]$ 内的 X_t 的数量的分布

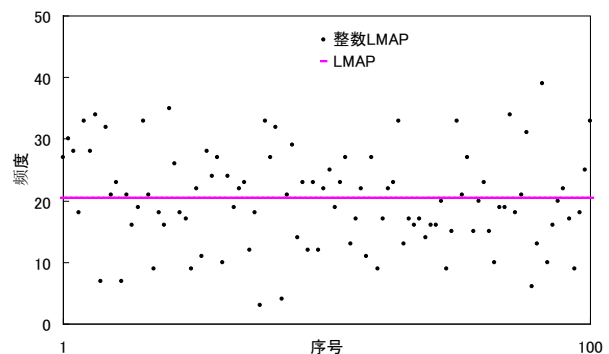


图 4 $N = 128$ 时的区间 $[1, 2^{N/2}]$ 内的 X_t 的数量的分布

我们将上述实验进行了 5 次, 得到了同等的结果。根据实验结果, 我们可以得出以下判断,

1. 式 (1) 和式 (2) 所产生的数值系列, 在分布密度上不能认为同等。

2. 式 (1) 和式 (2) 所产生的数值系列的分布密度的差, 仅在一个有限的比较小的范围内。

因此, 我们可以在需要用密度函数对整数 LMAP 进行分析时, 可以利用式 (1) 的密度分布函数来做近似分析。

4.3 计算精度 N 与检出概率

对于整数 LMAP 的任意值域区间 $[X_1, X_2]$, 且 $0 < X_1 < X_2 < 2^N$, 当 $X_2 - X_1 = 2^m$ 时 ($m < N$ 为整数), 我们可以得到相对应的 LMAP 的区间, $[x_1, x_2]$, $0 < x_1 < x_2 < 1$, $x_2 - x_1 = 2^{m-N}$ 。在此, $x_1 = X_1 / 2^N$, $x_2 = X_2 / 2^N$ 。从 LMAP 的密度函数, 我们可以知道, 当 $x_2 - x_1 = 2^{m-N}$ 时, 式 (9) 的 P 在 x_1 为最小或者 x_2 为最大值时得到最大值。基于 LMAP 的密度函数的对称性, 在此, 我们仅考虑 x_1 为最小值时的场合。

当 N 足够大时, 我们可以得到, $x_1 \approx 0$ 。而当 2^{m-N} 足够小时, 我们可以得到, $\arcsin(2^{(m-N)/2}) \approx 2^{(m-N)/2}$ 。由此, 我们可以得到

$$P^* = (2/\pi)2^{(m-N)/2} \quad (11)$$

式 (11) 显示当计算精度为 N 比特, 计算机的检索可能的数据量为 $N * 2^m / 8$ 字节时, 整数 LMAP 的数值系列 $\{X_i\}$ 中任意一个数值 X_i 属于被检索区间 $(0, 2^m)$ 的概率的近似值。

反之, 在已知计算机的检索可能的数据量参数 m 和所需 P^* 值时, 由式 (11) 我们可以得到所需的计算精度 N 。也就是, 在设计系统时, 我们可以根据现有计算机的检索能力和系统的安全性要求来给出一个决定系统的计算精度 N 的参考值。

显然, 由式 (11), 我们可以知道, 对于这样的攻击方法, 64 比特的计算精度不能认为是安全的, 而 128 比特则相对安全, 而 256 比特则可以认为是安全的。

5. 结语

本文对整数 LMAP 所产生的系列, 利用其密度分布来攻击的可能性进行了考察。本研究通过计算机实验, 确认了整数 LMAP 与 LMAP 有着不等同但相近的密度分布, 进而利用 LMAP 的密度分布函数, 给出了当计算精度为 N 比特, 计算机的检索可能的数据量为 $N * 2^m / 8$ 字节时, 整数 LMAP 的数值系列 $\{X_i\}$ 中任意一个数值 X_i 属于被检索区间 $(0, 2^m)$ 的概率的近似值。

一般, 由计算混沌所产生的数值系列具有不均匀的分布。因此, 本文所提示的方法, 也可以应用于其他混沌函数。

参考文献

- [1] 胡汉平. 混沌保密通信学[M]. 武汉, 湖北科技出版社, 2015: 9.
- [2] 董际国, 宋寒松. 基于整数 logistic map 的伪随机数产生法和多维坐标法[A]. 中国密码学会 2015 年混沌保密通信专委会第一届学术会议论文集[C]. 2015, (10): 527-532.
- [3] Jiguo D, Hiroyoshi M. Random Numbers Generation by Means of Integer Logistic Map and Mixing Operation[A]. IEICE vol.J94-A[C], 2011, (12): 923-931.
- [4] 董际国. 整数 logistic map 的诸性质: 发散、收缩、周期性[A]. 中国密码学会 2015 年混沌保密通信专委会第二届学术会议论文集[C]. 2016, 10.
- [5] Jiguo D, Hiroyoshi M. Various Characters of Integer Logistic Map: Divergence, Convergence, and Periodicity[A]. IEICE[C], 2013, (2): 90-99.
- [6] Knuth D. E. The Art of Computer Programming, Seminumerical Algorithms[M], Third Ed., Addison-Wesley, 1997.