文章编号:2095-476X(2014)06-0073-05

一种混沌块加密算法

危锋

(河南经贸职业学院 信息管理系, 河南 郑州 450046)

摘要:针对混沌理论在密码学应用中的安全问题,基于离散耦合映像格子和渐进确定性随机理论,设计了一种混沌块加密算法.该算法使用渐进确定性随机产生的密钥对明文进行扩散,并通过对离散耦合映像格子的迭代而进行加密.对其进行有效性测试及敏感度分析和抵抗统计分析,结果表明,该混沌加密算法具有较高的安全性.

关键词:混沌块加密算法;混沌分组密码;离散耦合映像格子;渐进确定性随机

中图分类号:TP301.6 **文献标志码**:A **DOI**:10.3969/j.issn.2095-476X.2014.06.016

A chaotic block encryption algorithm

WEI Feng

(*Department of Information Management, He'nan Economy and Trade Vocational College, Zhengzhou* 450046, *China*)

Abstract: Aiming at the security problem of chaos theory in cryptography application, a chaotic block encryption algorithm was designed based on the theory of discrete coupled map lattice and asymptotic deterministic randomness. The algorithm used aymptotic deterministic randomness key to diffuse the plaintext, and through the iteration of the discrete coupled map lattice the plaintext was encrypted. Then the validity, sensitivity and resistance of algorithm were tested and analyzed. The results showed that the security of chaotic encryption algorithm was higher.

Key words: chaotic block encryption algorithm; discrete coupled map lattice; asymptotic deterministic randomness

0 引言

混沌理论的一些特性与密码学中扩散和混乱的行为极具相似性,这些特性包括遍历性、初值敏感性和近似随机性.文献[1-3]论证了混沌理论和密码学之间的相似关系,并对混沌理论用于密码学的可行性进行了论证.文献[4-5]分别从不同角度进行了混沌理论与密码学结合的算法设计,具有很强的实用性和参考价值.近年来应用混沌构建加密系统的研究已取得了可喜的进展[6-7].但是,混沌理论在密码学应用中的安全问题一直是研究热点,且久攻不下,亟待解决.鉴于此,本文拟提出一种基于离散耦合映像格子和渐进确定性随机的安全混沌块加密算法,以期为混沌理论在密码学应用中安全问题的研究提供参考和借鉴.

1 离散耦合映像格子和渐进确定性随机

1.1 离散耦合映像格子

耦合映像格子CML(coupled map lattice)是一种动力学系统,能够描述非线性系统的行为.CML在时域和空域离散,在状态域连续,通常包含一组方程(耦合的或非耦合的)、有限数量的变量、一种全局或者局部耦合的方法以及相关的耦合项.K.

收稿日期:2014-04-14

作者简介:危锋(1981—),男,湖北省天门市人,河南经贸职业学院讲师,硕士,主要研究方向为网络与软件工程.

Kaneko[8] 于 1984 年提出了一个典型的 N 点耦合映像格子模型:

$$x_{n+1}^{i} = (1-e)f_i(x_n^i) + e/2[f_{i-1}(x_n^{i-1}) + f_{i+1}(x_n^{i+1})]$$

其中,x_n^i 为每个格点对应状态,$f_1: I \to I$ 是区间 $I=[a,b]$ 上的单峰映射函数(如 Logistic,Skewed Tent 映射等),e 表示耦合系数,时间步数 $n=1,2,\cdots$, $i=1,2,\cdots,N$ 表示格子的位置. 定义 F 为每个格点的生成函数 f_i,同时定义 $\boldsymbol{A}$ 为耦合矩阵,则 CML 可以改写为

$$x_{n+1} = H(x_n)$$

其中,$H = A \circ F$, $H: I^N \to I^N$.

对于 CML,可以使用耦合矩阵 $\boldsymbol{A}$ 与单峰映射 $f_i(x)$ 进行映射. 将使用高维的 Cat 映射对离散 Skewed Tent 映射进行耦合,并以此来构造离散耦合映像格子与其逆函数. 一个典型的二维 Cat 映射矩阵可表示为

$$\boldsymbol{A} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix}$$

其中,控制参数 a 和 b 都是负整数. 可以根据方程 $\boldsymbol{AA} = \boldsymbol{A}_{12}\boldsymbol{A}_{13}\boldsymbol{A}_{14}\boldsymbol{A}_{23}\boldsymbol{A}_{24}\boldsymbol{A}_{34}$ 生成 1 个四维的 Cat 映射矩阵.

考虑任意四维向量 $\boldsymbol{X} = [X_1, X_2, X_3, X_4]^{\mathrm{T}}$,其中 $X_i \in \{1,2,\cdots,M-1\}$, $i=1,2,3,4$,则 $\boldsymbol{X}$ 的离散耦合映像格子 $G(\boldsymbol{X})$ 可以表示为

$$G(\boldsymbol{X}) = \boldsymbol{AA} = \begin{bmatrix} F_A(X_1) \\ F_A(X_2) \\ F_A(X_3) \\ F_A(X_4) \end{bmatrix} \bmod M \qquad ①$$

其中,函数 F_A 为离散 Skewed Tent 映射,可以推导得该离散耦合映像格子的逆函数为 $G^{-1}(\boldsymbol{X}) = \begin{bmatrix} F_A^{-1}(\tilde{X}_1) \\ F_A^{-1}(\tilde{X}_2) \\ F_A^{-1}(\tilde{X}_3) \\ F_A^{-1}(\tilde{X}_4) \end{bmatrix}$,其中 $\begin{bmatrix} \tilde{X}_1 \\ \tilde{X}_2 \\ \tilde{X}_3 \\ \tilde{X}_4 \end{bmatrix} = \boldsymbol{AA}^{-1} \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{bmatrix} \bmod M$, $\boldsymbol{AA}^{-1}$ 是四维 Cat 映射矩阵 $\boldsymbol{AA}$ 的逆矩阵.

1.2 渐进确定性随机

考虑表达式 $x_n = p(\theta z^n)$,其中,$p(t)$ 是周期函数,z 是整数,θ 定义了初始状态,T 是函数 $p(t)$ 的周期. 当 $p(t) = \sin^2(t)$ 并且 $z=2$ 时,则该表达式即为一维 Logistic 映射的显式解. 接下来以 $x_n = \sin^2(\theta z^n)$ 为例进行分析,令 $\theta = \theta_0 + q^m k$,且 z 是有理数,$z = p/q$,其中,p 和 q 都是质数,m 和 k 都是整数. 给定序列 $x_0, x_1, x_2, \cdots, x_m$,该序列由式 $x_n = \sin^2(\theta z^n)$ 产生,序列中下个元素 x_{n+1} 的取值有 q 种可能(这种情形被称为多值对应),导致序列在短时间内不可预测. 为了与确定性混沌有所区别,这种现象被称为确定性随机[9-10].

文献[9-11]利用分段线性或非线性映射和不可逆非线性变换来构造确定性随机系统,并对其进行了研究. 本文主要针对文献[9]中的如下系统进行分析和研究:

$$x_{n+1} = h(a, x_n) \qquad y_n = h(b, x_n) \qquad ②$$

其中,$h(a,t) = \mathrm{mod}(a \times t, 1)$. 当 $a = p/q > 2$ 为互质假分数,并且 $b = q^N$ 时,y_n 和 y_{n+m} $(m=1,2,\cdots N)$ 可以与 $p^m : q^m$ 形成完整的多值对应关系,这类映射系统被称为李沙育映射Ⅱ. 产生确定性随机的内在因素是初始值不同,产生的序列也不同,但是这些序列具有相同的前一项和不同的后一项. 比如方程 $x_n = \sin^2(\theta z^n)$,当初始值 $\theta = \theta_0 + q^m k$ 可以等概率地选取时,下一项的值也等概率地具有不同的选择. 假设 $y_n = Y$ 由李沙育映射Ⅱ产生,由于序列 $\{x_n\}$ 在区间[0,1]上等概率分布,则初始值 $x_n = \dfrac{Y+i}{b}$, $i = 0,1,\cdots,b-1$ 可以由相同的概率产生.

2 混沌块加密算法

针对上述分析和讨论,笔者提出了一种基于离散耦合映像格子和渐进确定性随机的混沌块加密算法. 本加密算法利用渐进确定性随机产生密钥序列,并通过离散耦合映像格子对明文进行迭代得到密文.

现代计算机数据储存和传输一般用字节为基本单位,为便于加密计算机数据,本算法仍以字节为基本单位,每个字节单位使用其相应的十进制数值表示. 这样明文可以表示为 $P = p_1, p_2, \cdots$,密文可以表示为 $C = c_1, c_2, \cdots$. 为了利用式①所示的四维离散耦合映像格子,将每 4 个字节作为一个分组,则第 i 个分组的消息可以表示为 $\{p_{1+i\times4}, p_{2+i\times4}, p_{3+i\times4}, p_{4+i\times4}\}$, $i=0,1,\cdots$. 对于每一个 4 字节分组,该块加密方案主要步骤如下:

步骤 1 $B_j = p_{j+i\times4} \oplus c_{j+(i-1)\times4}$, $j=1,2,3,4$;

步骤 2 $B_j = B_j \oplus k_{j+i\times4}$, $j=1,2,3,4$,然后 $[B_1, B_2, B_3, B_4]^{\mathrm{T}} = G(B_1, B_2, B_3, B_4)$,通过上述运算得到的 B_j 用于下一轮运算;

步骤 3 $B_j = B_j \oplus k_{j+1+i\times4}$, $j=1,2,3,4$,然后 $[B_1, B_2, B_3, B_4]^{\mathrm{T}} = G(B_1, B_2, B_3, B_4)$,通过上述运算得到的 B_j 用于下一轮运算;

步骤 4　$B_j = B_j \oplus k_{j+2+i\times4}, j = 1,2,3,4$,然后 $[B_1,B_2,B_3,B_4]^{\mathrm{T}} = G(B_1,B_2,B_3,B_4)$,通过上述运算得到的 B_j 用于下一轮运算;

步骤 5　$B_j = B_j \oplus k_{j+i\times4}, j = 1,2,3,4$,然后 $[B_1,B_2,B_3,B_4]^{\mathrm{T}} = G(B_1,B_2,B_3,B_4)$,通过上述运算得到的 B_j 用于下一轮运算;

步骤 6　$B_j = B_j \oplus k_{j+1+i\times4}, j = 1,2,3,4$,然后 $[B_1,B_2,B_3,B_4]^{\mathrm{T}} = G(B_1,B_2,B_3,B_4)$,通过上述运算得到的 B_j 用于下一轮运算;

步骤 7　最后 $B_j = B_j \oplus k_{j+2+i\times4}, j = 1,2,3,4$,接着将 $G(B_1,B_2,B_3,B_4)$ 的运算结果作为第 i 个分块的密文 $(c_{1+i\times4},c_{2+i\times4},c_{3+i\times4},c_{4+i\times4})$.

上述加密方案中,非线性方程 G 是离散耦合映像格子. 加密用的密钥序列 $\{k_i\}$ 由渐进确定性随机产生,产生序列的方法是对式②进行反复迭代. 为了避免暂态的影响,密钥序列的前 100 次迭代结果不被使用. 此时,迭代得到的序列不能直接使用,需要用式 $k_i = [256 \cdot y_{i+100}], i = 1,2,\cdots$ 对其进行处理,使其序列值位于区间[1,255],且为整数. 易知,解密算法是加密算法的逆过程.

在进行加密算法编写时,有一点需要注意,在通过离散耦合映像格子迭代进行加密时,式①的离散 Skewed Tent 映射的定义域为[1,256],而计算机中 8 位无符号整型值区间为[0,255],且加密字节在通过异或操作后可能等于 0. 因此在通过离散 Skewed Tent 映射前需要先将加密字节进行类型转换后再加 1,解密时,在通过离散 Skewed Tent 逆映射后对计算值减 1.

在本加密方案中,使用了 3 组参数:第 1 组用于产生四维 Cat 映射矩阵 $\{a_{12},b_{12}\},\{a_{13},b_{13}\},\cdots,\{a_{34},b_{34}\}$;第 2 组是离散 Skewed Tent 映射的控制参数 A;第 3 组用于产生密钥序列的初始值 x_0.

3　实验结果与分析

测试对象是一段 16 位 8 kHz 采样的语音,加解密语音见图 1.

3.1　有效性测试

测试中所使用的参数如下:初始值 $x_0 = 0.125$;离散 Skewed Tent 映射的控制参数 $A = 25$;四维 Cat 映射 $\{a_{i,j}\}_{i,j=1,2,3,4}$ 是 $\boldsymbol{AA} = \begin{bmatrix} 1 & 54 & 3\,362 & 20\,445 \\ 7 & 379 & 23\,598 & 143\,504 \\ 8 & 434 & 27\,025 & 164\,344 \\ 9 & 308 & 18\,816 & 114\,464 \end{bmatrix}$,其

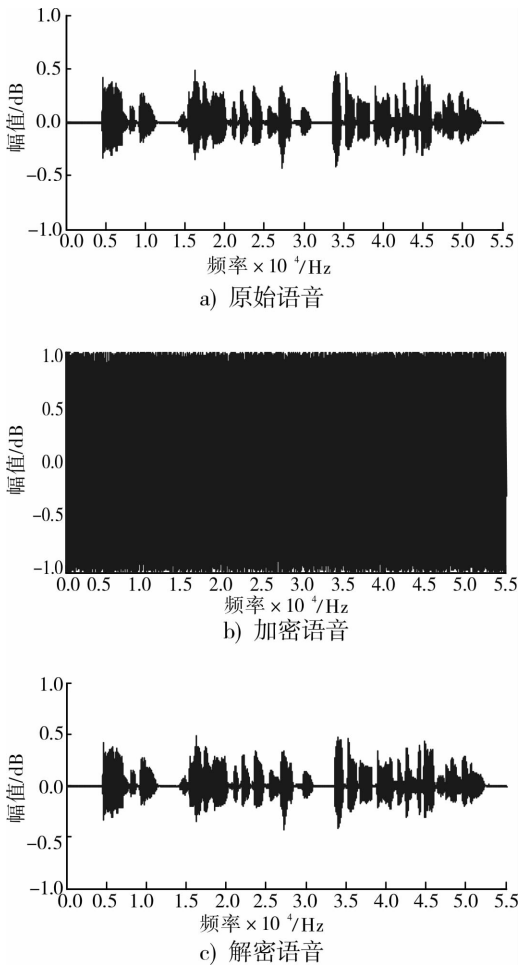


图 1　加解密语音

中产生矩阵四维 Cat 映射的参数是

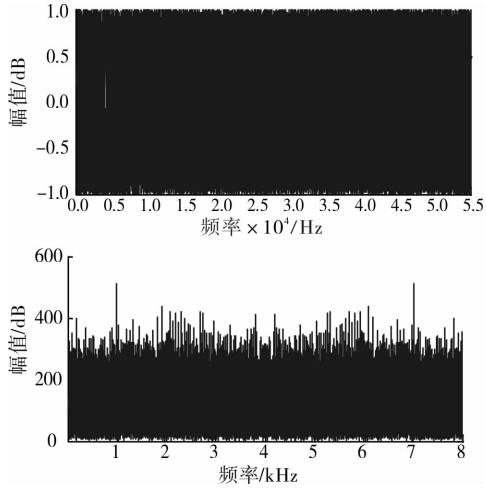
$$\begin{bmatrix} b_{34} & a_{12} & a_{13} & a_{14} \\ b_{24} & b_{23} & a_{23} & a_{24} \\ b_{14} & b_{13} & b_{12} & a_{34} \end{bmatrix} = \begin{bmatrix} 12 & 1 & 2 & 3 \\ 11 & 10 & 4 & 5 \\ 9 & 8 & 7 & 6 \end{bmatrix}$$

由图 1 可见,原始语音经本方案加密后,从加密语音中无法获取有用信息,解密后可获得原始语音. 由此可证明本方案有效可行.

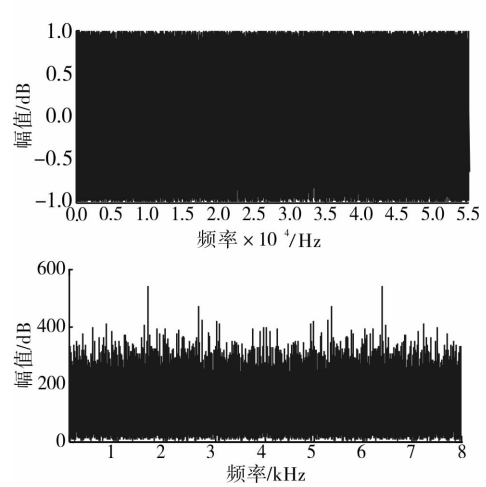
3.2　密钥敏感度分析

在 Matlab 软件平台下,利用函数 wavread( ) 对语音信号进行采样,获取采样频率和采样位数,[z1, fs,bits] = wavread('D:\语音采样\fan. wav') 运行结果:fs = 8 000, bits = 16. 对采样的语音样本进行了密钥敏感度测试. 首先,给定产生密钥的参数 $\{a_{i,j}\}_{i,j=1,2,3,4}$,$A$ 和 x_0,接着使用本文提出的块加密算法对语音进行加密,然后改变其中某个参数,保持另外两个参数不变,利用改变参数的加密算法重新对语音进行加密. 改变参数后,对使用不同参数

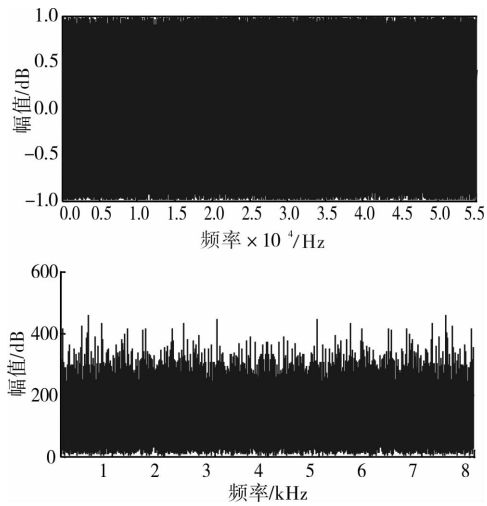
的加密语音的频谱进行比较,以测试密钥敏感度,结果见图 2.



a) 错误密钥 $x'_0 = 0.125 + 2^{-50}$ 解密的语音及其频谱图



b) 错误密钥 $\boldsymbol{A}' = 24$ 解密的语音及其频谱图



c) 错误密钥 $\boldsymbol{AA}' = 24$ 解密的语音及其频谱图

图 2 密钥敏感度测试

从图 2 可以看出,密钥只作很细微的改变,加密语音就无法被解密. 同样可以看到,使用错误密码对加密语音进行解密,错误解密后的语音频谱近似服从均匀分布. 因此,该加密算法具有很高的密钥敏感度.

3.3 抵抗统计分析

为了抵抗统计分析,“信息论之父”香农建议任何加密系统都应该引入扩散和混乱. 本文提出的加密算法使用了渐进确定性随机产生的密钥对明文进行扩散,然后使用离散耦合映像格子进行迭代处理. 图 3 为原始语音与加密语音频谱分析. 由图 1b)和图 3b)可知,加密语音的波形及频谱近似于均匀分布,这就使得基于统计的攻击变得很困难.

除此之外,对原始语音和加密语音的相关性,以及使用不同密钥加密的加密语音之间的相关性进行测试. 原始语音和使用不同密钥 $x_0 \in [0.12, 0.13]$ 加密的加密语音之间的相关性如图 4a)所示,对 $x_0 = 0.125$ 的加密语音和 $x_0 \in [0.12, 0.13]$ 的加密语音进行相关性测试,测试结果如图 4b)所示. 由图 4a)可知,明文和密文的相关曲线近似于一条等于 0 的曲线,表明明文和密文几乎是不相关的;由图 4b)可知,使用 $x_0 = 0.125$ 的加密语音和使用 $x_0 \in [0.12, 0.13]$ 的加密语音的相关曲线仅在 $x_0 = 0.125$ 处表现为一个冲击,其他各点近似等于 0,原因是区间 $x_0 \in [0.12, 0.13]$ 包含了 $x_0 = 0.125$,由此表明使用不同密钥加密的密文是互相独立的. 以上分析表明,原始语音与加密语音之间没有可探测的相关性,即明文与密文之间的相关性非常小. 因此,该加密方案能够很好地抵抗基于统计的攻击.

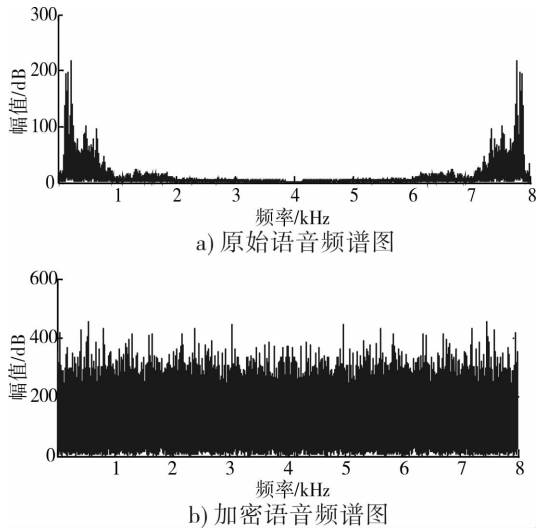
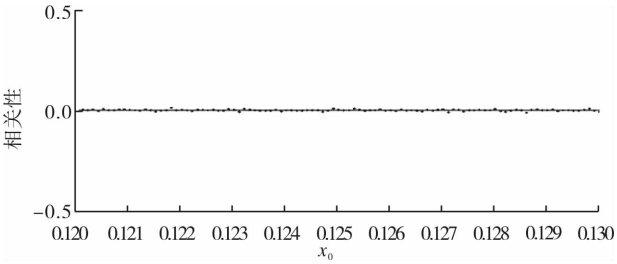
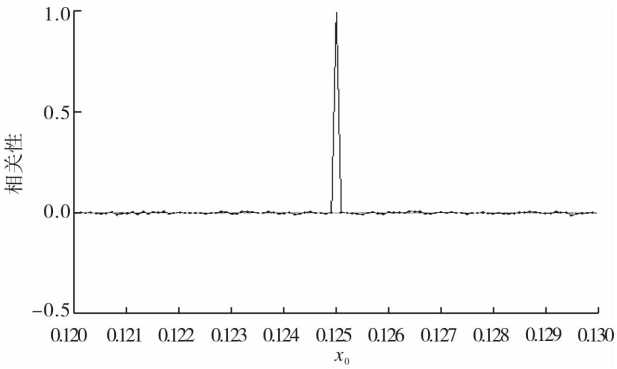


图 3 原始语音与加密语音频谱分析



a)明文与密文之间的相关性



b)不同密文之间的相关性

图 4　加密相关性测试

4　结论

本文基于对混沌理论和密码学的研究和分析,提出一种基于离散耦合映像格子和渐进确定性随机的混沌块加密算法. 该算法利用渐进确定性随机产生密钥序列,并通过离散耦合映像格子对明文进行迭代得到密文. 仿真实验及安全性能分析表明,该算法在安全性上有突出的特点,能够为学界提供有益的参考和借鉴.

参考文献:

[1] 盛苏英,吴新华. 基于耦合映象格子的混沌图像加密算法研究[J]. 微电子学与计算机,2014(1):32.

[2] Kinzel W, Englert A, Kanter I. On chaos synchronization and secure communication[J]. Phil Trans R Soc(A), 2010,368(1911):379.

[3] Olivares F, Plastino A, Rosso O A, Contrasting chaos with noise via local versus global information quantiers[J]. Phys Lett(A),2012,376:1577.

[4] Kocarev L, Lian S G. Chaos-based Cryptography: Theory, Algorithms and Applications[M]. Berlin: Springer, 2011.

[5] Lozi R. Emergence of randomness from chaos[J]. International Journal of Bifurcation and Chaos, 2012, 22(2):15.

[6] Pareek N K, Patidar V, Sud K K. A random bit generator using chaotic maps[J]. International Journal of Network Security, 2010, 10(1):32.

[7] Wang K, Pei W J, Zou L H, et al. The asymptotic deterministic randomness[J]. Phys Lett(A), 2007, 368:38.

[8] Kaneko K. Period-doubling of kink-antikink patterns, quasi-periodicity in antiferro-like structures and spatial intermittency in coupled logistic lattice[J]. Progress of Theoretical Physics, 1984, 72 (3):480.

[9] Wang K, Pei W J, Xia H S, et al. Pseudo-random number generator based on asymptotic deterministic randomness [J]. Phys Lett(A), 2008, 372:4388.

[10] Wang K, Pei W J, Gonzalez J A, et al. Statistical independence in nonlinear maps coupled to non-invertible transformations[J]. Phys Lett(A), 2008, 372:6593.

[11] Wang K, Pei W J, Hou X B, et al. Discrete asymptotic deterministic randomness for the generation of pseudorandom bits[J]. Phys Lett(A), 2009, 373:653.