Hans Journal of Data Mining 数据挖掘, 2018, 8(3), 104-111
Published Online July 2018 in Hans. http://www.hanspub.org/journal/hjdm
https://doi.org/10.12677/hjdm.2018.83012

Hans汉斯

Algorithm of Generating S-Box Based on Uniform Chaotic System

Huifang Huang

School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou Fujian
Email: 13661363592@163.com

Received: Jun 15th, 2018; accepted: Jul. 10th, 2018; published: Jul. 17th, 2018

Abstract

In this paper, a new quadratic polynomial chaotic system is given and homogenized based on its probability density function. Then, based on the homogenized chaotic systems, an S-box generation algorithm is constructed. The security of S-box is tested by numerical simulation including differential probability analysis and linear probability analysis. The statistical results show that the uniform chaotic system can produce better performance of S-boxes.

Keywords

Chaotic System, Homogenization, S-Box, Differential Probability, Linear Probability

基于均匀化混沌系统的S-Box生成算法

黄慧芳

厦门大学嘉庚学院，信息科学与技术学院，福建 漳州
Email: 13661363592@163.com

收稿日期：2018年6月15日；录用日期：2018年7月10日；发布日期：2018年7月17日

摘 要

该文给出了一个新的二次多项式混沌系统，并基于系统的概率密度函数对其进行均匀化处理。基于均匀化后的混沌系统构造了新的S-Box生成算法。对生成的S-Box进行性能检测，包括双射特性，非线性度，差分概率(DP)和线性概率(LP)分析，结果表明本文均匀化后混沌系统产生的S-Box具有较好的密码特性，适合用于加密系统。

文章引用: 黄慧芳. 基于均匀化混沌系统的 S-Box 生成算法[J]. 数据挖掘, 2018, 8(3): 104-111.
DOI: 10.12677/hjdm.2018.83012

关键词

混沌系统，均匀化，S-Box，差分概率，线性概率

Copyright © 2018 by author and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

混沌是非线性动力学系统特有的一种无周期的有序运动。文献[1]中首次用数学定义描述了混沌一词。混沌系统具有高度的初值敏感性、伪随机性和不可预测性，使其在混沌密码学的研究中成为热点。自 20 世纪 80 年代以来，密码学家不断挖掘出了混沌在密码学领域中的应用潜力[2] [3] [4]。除此之外，混沌还在各个领域中得到广泛关注与应用。

为满足安全保密通信的要求，科学家往往希望得到均匀性随机性良好的随机数源。混沌系统作为重要的随机数源，在构造伪随机数发生器时，大部分系统不能满足均匀性要求。因此，找到有效的混沌系统均匀化方法有着重要的学术意义。文献[5]把混沌系统生成的序列通过反正切和反余弦函数变换成服从均匀分布的伪随机序列，文献[6]基于计算机浮点数表示，给出了将混沌序列变换成均匀伪随机序列的 bit 位操作方法，文献[7]曹光辉等人给出了一个基于概率原理将 Logistic 混沌系统产生的非均匀分布随机变量转化为服从均匀分布的随机变量的方法。

通过混沌映射的概率密度函数可以发现大部分混沌序列不服从均匀分布。混沌系统具有各态历经的特性，利用混沌映射的概率密度可以描述系统长期的统计特征。由于大多数混沌系统的复杂性，其概率密度函数并不容易获得。何振亚等人[8]通过证明 Logistic 映射与 Tent 映射的拓扑共轭关系以及 Chebyshev 映射与 Tent 映射的拓扑共轭关系，得到了 Logistic 映射和 Chebyshev 映射的概率密度。

一个 $n\times m$ 的 S-Box 是将 n 位输入映射到 m 位输出的非线性映射，由于 S-Box 是 AES 等分组密码中唯一的非线性部件，设计好的分组密码算法就很大程度上依赖于 S-Box 的性能。密码学研究者提出了很多构造动态 S-Box 的方法[9]，其中，将具有良好伪随机性的混沌系统用于构造动态 S-Box 便是一种重要方法[10]。

本文基于已有定理提出了一个新的二次多项式混沌系统，并基于拓扑共轭理论推出了混沌系统的概率密度函数，从而对系统进行修正，使其能够产生均匀化的随机序列；利用均匀化的混沌序列构造 S-Box，对 S-Box 的性能指标进行统计分析，结论是均匀化后系统产生的 S-Box 密码性能良好。

本文其余部分安排如下：在第 2 节中提出了一个新的混沌系统，并基于概率密度函数对系统进行了均匀化处理。在第 3 节中，设计了一个动态 S-Box 的生成方法，利用均匀化后的混沌系统生成 S-Box，并进行了 S-Box 性能分析。第 4 节总结全文。

2. 二次多项式混沌系统的均匀化处理

纸型

文献[11]提出了一般非线性二次多项式 3-周期点存在的充分必要条件，表述为如下引理：

引理 1 [11]：二次多项式 $f(x)=ax^2+bx+c$ 有实的 3-周期点的充要条件是

$$b^2-4ac-2b\geq 7$$

基于引理 1，本文构造了新的一维混沌系统为：

$$f(x)=1.28x^2+0.56x-1.72, x\in\left[-\frac{57}{32},\frac{43}{32}\right] \tag{1}$$

将系统表示为

$$x(n+1)=ax^2(n)+bx(n)+c \tag{2}$$

其中

$$a=1.28, b=0.56, c=-1.72.$$

图 1(a)为混沌系统(2)随参数 $a\in[0.28,1.28]$ 变化的分岔图，其中参数 $b=0.56, c=-1.72$，图 1(b)，图 1(c)分别为混沌系统(2)随参数 b,c 变化的分岔图，其中 $b\in[0.56,1.4]$，$c\in[-1.72,-0.72]$。

根据文献[12]中拓扑共轭的定义，如果存在一个可逆映射 $h: X\to Y$，使得 $h(g(x))=f(h(x))$ 成立，则称映射 $g(x)$ 和 $f(y)$ 是拓扑共轭的。以下证明混沌系统

$$f(x)=1.28x^2+0.56x-1.72, x\in\left[-\frac{57}{32},\frac{43}{32}\right]$$

与 Tent 映射是拓扑共轭的。

此处，Tent 映射为

$$g(x)=\begin{cases}2x, & 0\le x\le\dfrac{1}{2}\\ 2-2x, & \dfrac{1}{2}\le x\le 1\end{cases}$$

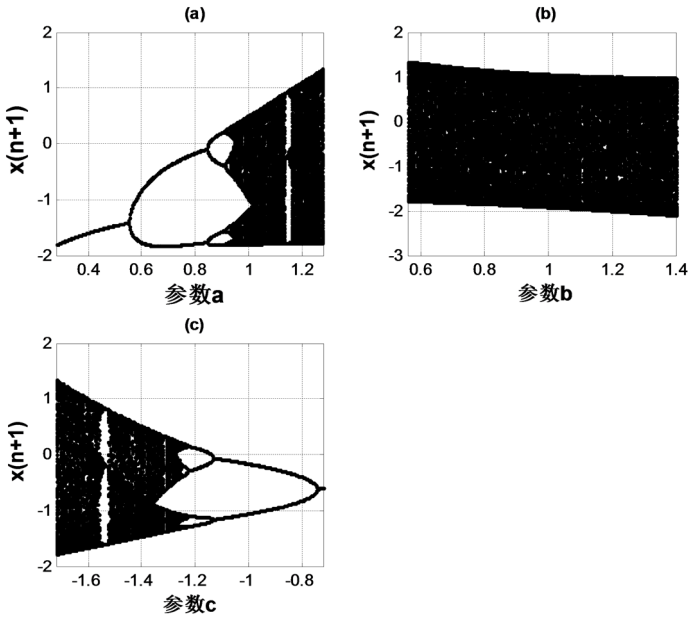

Figure 1. (a) The bifurcation diagram of parameter a in system (2); (b) The bifurcation diagram of parameter b in system (2); (c) The bifurcation diagram of parameter c in system (2)

图 1. (a) 系统(2)关于参数 a 的分岔图；(b) 系统(2)关于参数 b 的分岔图；(c) 系统(2)关于参数 c 的分岔图

令连续可逆函数

$$h(x)=\frac{25}{16}\cos\pi x-\frac{7}{32},\ x\in[0,1]$$

则有

$$\begin{aligned}h\circ g(x)&=\begin{cases}\frac{25}{16}\cos 2\pi x-\frac{7}{32}, & 0\le x\le\frac{1}{2}\\ \frac{25}{16}\cos\pi(2-2x)-\frac{7}{32}, & \frac{1}{2}\le x\le 1\end{cases}\\&=\frac{25}{16}\cos 2\pi x-\frac{7}{32}\\&=h(2x)\end{aligned}$$

且

$$\begin{aligned}f\circ h(x)&=\frac{32}{25}h^2(x)+\frac{14}{25}h(x)-\frac{43}{25}\\&=\frac{32}{25}\left(h(x)+\frac{7}{32}\right)^2-\frac{57}{32}\\&=\frac{32}{25}\left(\frac{25}{16}\cos\pi x\right)^2-\frac{57}{32}\\&=\frac{25}{16}\cos 2\pi x-\frac{7}{32}\\&=h(2x)\end{aligned}$$

即 $h(g(x))=f(h(x))$， $f(x)$ 与 Tent 映射关于 $h(x)$ 拓扑共轭。

基于函数的共轭关系，可以证明混沌系统

$$f(x)=1.28x^2+0.56x-1.72,\ x\in\left[-\frac{57}{32},\frac{43}{32}\right]$$

的概率密度函数为

$$\rho(x)=\begin{cases}\frac{1}{\pi}\frac{32}{\sqrt{2451-448x-1024x^2}}, & x\in\left[-\frac{57}{32},\frac{43}{32}\right]\\ 0, & \text{其他}\end{cases}$$

证明：已知 Tent 映射的概率密度函数为

$$\rho_T(x)=1,\ x\in(0,1).$$

根据上述证明过程， $f(x)=1.28x^2+0.56x-1.72$ 与 Tent 映射关于 $h(x)=\frac{25}{16}\cos\pi x-\frac{7}{32}$ 拓扑共轭，因此有

$$\begin{aligned}\rho_f(x)&=\rho_T\left(h^{-1}(x)\right)\left|\frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x}\right|\\&=\frac{1}{\pi}\frac{32}{\sqrt{2451-448x-1024x^2}}\end{aligned}$$

显然，系统(1)的概率密度函数表明该系统会生成不均匀的序列，容易具有明显的统计特性，不适合作为伪随机数发生器，不利于推广应用。以下基于概率密度函数，提出一个以系统(1)函数值为变量的反正弦函数，并证明该函数能够产生服从均匀分布的混沌序列。

定理 1：已知随机变量 X 服从概率密度函数

$$\rho(x)=\begin{cases}\dfrac{1}{\pi}\dfrac{32}{\sqrt{2451-448x-1024x^2}}, & x\in\left[-\dfrac{57}{32},\dfrac{43}{32}\right]\\ 0, & \text{其他}\end{cases}$$

则随机变量

$$Z=\frac{1}{\pi}\arcsin\left(-\frac{16}{25}X-\frac{7}{50}\right) \tag{3}$$

在区间 $\left[-\frac{1}{2},\frac{1}{2}\right]$ 上服从均匀分布。

证明：随机变量 Z 的分布函数

$$\begin{aligned}F_Z(z)&=P(Z\le z)=P\left(\frac{1}{\pi}\arcsin\left(-\frac{16}{25}X-\frac{7}{50}\right)\le z\right)\\&=\int_{-\infty}^{-\frac{25}{16}\sin\pi z-\frac{7}{32}}\rho_X(x)\mathrm{d}x\end{aligned} \tag{4}$$

对式(4)求导，得到 Z 的概率密度

$$\rho_Z(z)=\begin{cases}1, & -\dfrac{1}{2}\le z\le\dfrac{1}{2};\\ 0, & \text{其它.}\end{cases}$$

综上，随机变量 $Z=\frac{1}{\pi}\arcsin\left(-\frac{16}{25}X-\frac{7}{50}\right)$ 在区间 $\left[-\frac{1}{2},\frac{1}{2}\right]$ 上服从均匀分布，由于随机变量 Z 与随机变量 X 为一一对应关系，因此生成序列为混沌序列。

以上定理提出了利用概率密度函数对混沌系统进行均匀化处理的方法。由证明过程可知，经由(3)式把原二次多项式混沌系统(1)转换为服从均匀分布的随机变量。本文把式(2) (3)合称为修正的混沌映射，表示为

$$\begin{cases}x(n+1)=1.28x(n)^2+0.56x(n)-1.72\\ z(n+1)=\dfrac{1}{\pi}\arcsin\left(-\dfrac{16}{25}x(n+1)-\dfrac{7}{50}\right)\end{cases} \tag{5}$$

针对均匀化前混沌系统式(1)和均匀化后系统式(5)产生的序列进行直方图统计，验证均匀化方法的有效性。图 2(a)是原二次多项式系统生成混沌序列的频率直方图，图 2(b)是修正混沌映射生成的具有均匀分布随机序列的频率直方图。由模拟结果对比可见，处理后的混沌序列均匀性明显增强。

3. 基于均匀化混沌系统构造 S-Box

3.1. S-Box 算法构造

S-Box 作为分组密码中的非线性部件，主要起到置换的功能。为了达到更好的置乱效果，增加加密方案的抵抗攻击能力，本文利用混沌系统进行迭代，并基于混沌系统的不同的初始值动态生成 8×8 的 S-Box，因而，S-Box 的密钥由混沌系统的参数，迭代次数，初值等构成。具体的算法步骤为：

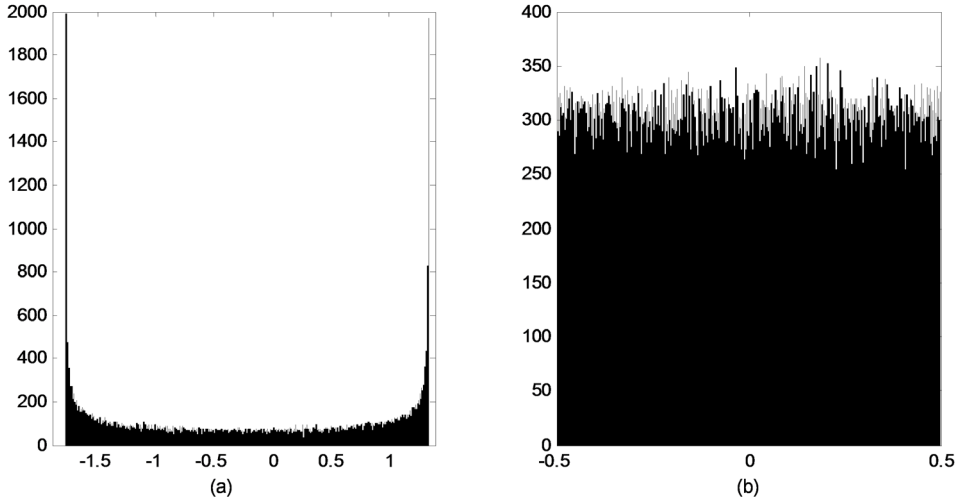

Figure 2. Histogram: (a) Histogram of the sequence before uniformity; (b) Histogram of the sequence after uniformity
图 2. 统计直方图：(a) 均匀化前序列；(b) 均匀化后序列

1) 将相空间$[-0.5,0.5]$进行 n 等分，分别为每个小区间标号为$i=0,1,\cdots,n$；

2) 取初值 x_0，利用混沌系统(5)式迭代 n 次，得到一个 n 维混沌序列；

3) 将序列值对应到相空间$[-0.5,0.5]$中的相应小区间，用区间标号$i(\mathrm{mod}\,256)$，得到一个 n 维位置序列；

4) 位置序列中前 256 个不相等的值依次构成 S-Box 序列。

当混沌迭代的初始值 x_0 或迭代次数发生改变时，由于混沌系统的初值敏感性和不可预测性，算法相当于一个一次一密的加密部件。

3.2. S-Box 性能分析

下面从动态生成的 S-Box 中选取出一个样本分析密码学性能指标，与现有混沌 S-Box 作比较分析，证明本文构造的由均匀化混沌系统生成的 S-Box 适用于设计分组密码方案。表 1 为选取的 S-Box 序列样本。

首先对双射特性进行检测，表 1 中 S-Box 样本的 8 个分量布尔函数记为 $S(x)=(f_1(x),\cdots,f_8(x)):GF(2^8)\to GF(2^8)$，线性运算之和都为 128，与理想值相同，满足双射特性，输出函数的比特平衡性很好。

S-Box 的非线性度为 $N_s=\min\limits_{\substack{l\in L_n\\ 0\neq u\in F_2^m}} d_H(u\cdot S(x),l(x))$。式中：$u\cdot S(x)$表示 u 与 $S(x)$的点积。L_n 表示全体 n 元线性和仿射函数之集；$d_H(x,y)$表示 x 和 y 的汉明距离。函数的非线性度越大，意味着抵抗线性攻击的能力越强。表 2 给出了 S-Box 的 8 个布尔函数的非线性度，对比可见，表 1 的 S-Box 样本非线性度处在较高水平，表明更能够抵抗最佳线性逼近攻击。

S-Box 的差分概率(DP)用来评价其抵抗差分密码攻击的能力，DP 值越小，抵抗能力越强。而线性概率(LP)评价了 S-box 抵抗线性密码攻击的能力，LP 指标越小，抵抗效果越好。离散混沌 S-Box 的 Lyapunov 指数[13]可以用来衡量双射映射中自变量改变一比特时，映射值变化比特的情况。Lyapunov 指数越大，说明自变量能够引起状态值的变成程度越高，意味着系统混沌性越好。本文构造 S-Box 的 DP，LP 及其 Lyapunov 指数结果与文献中 S-Box 的对比见表 3。由对比结果可见，本文 S-box 的 DP 值和 LP 值均小于

Table 1. S-box sequence sample
表 1. S-box 序列样本

250	174	41	79	177	63	35	91	117	16	163	85	247	180	57	155
118	182	191	116	43	75	183	5	206	187	248	36	160	55	20	148
121	175	39	83	251	171	11	139	204	10	141	136	145	81	0	101
215	243	54	4	154	110	23	185	197	196	72	102	213	153	112	232
67	28	105	29	104	66	30	47	216	242	214	130	157	103	211	252
190	38	52	194	88	125	167	71	122	241	32	98	221	217	239	195
254	166	86	181	129	159	99	60	3	80	1	97	224	225	192	33
95	212	249	133	151	37	78	140	150	15	240	244	40	27	12	137
143	131	64	93	231	18	51	21	120	2	124	170	218	123	25	111
165	189	46	59	135	44	49	173	199	255	164	128	228	193	87	108
113	222	230	74	14	58	246	149	142	76	9	106	169	109	161	96
100	237	146	134	132	24	186	69	114	176	22	138	73	226	172	8
31	227	127	209	89	156	70	188	42	17	56	168	65	158	119	19
92	48	61	210	220	233	207	203	126	115	6	45	219	236	202	13
200	77	184	82	253	84	144	162	235	107	178	62	50	205	179	147
245	201	152	234	26	94	208	198	90	238	34	7	223	229	68	53

Table 2. Comparison of the nonlinearity of S-boxes
表 2. S-Boxes 的非线性度对比

S-Box	非线性度								均值
本文构造的 S-Box	108	106	108	108	108	104	108	104	106.75
文献[14]的 S-Box	103	109	104	105	105	106	104	103	104.88
文献[15]的 S-Box	104	100	106	102	104	102	104	104	103.25
文献[16]的 S-Box	106	106	108	108	108	108	108	110	107.75

Table 3. Comparison of the DP, LP, Lyapunov exponent of S-boxes
表 3. S-Boxes 的 DP，LP，Lyapunov 指数对比

S-Box	DP	LP	Lyapunov
本文构造的 S-Box	0.03906250	0.05493164	1.75545713
文献[14]的 S-Box	0.06250000	0.12915039	1.60528688
文献[15]的 S-Box	0.03906250	0.05493164	1.76551996
文献[16]的 S-Box	0.04687500	0.08813476	1.84638726

文献[14] [15]中 S-boxes 的相应指标值，说明有均匀化系统构造的 S-box 可以更好地抵抗差分密码攻击和线性密码攻击。而 Lyapunov 指数比文献[15] [16]中 S-boxes 的 Lyapunov 指数来得小，说明本文 S-box 的混沌程度还有待提高。

4. 结论

本文提出了一个新的二次多项式混沌系统，结合拓扑共轭理论和 tent 映射的概率密度函数推出了系

统的概率密度函数，并基于概率原理提出了一个满足均匀化分布的随机变量。利用均匀化前后系统生成的混沌序列的直方图统计直观地说明了均匀化效果良好。基于均匀化后混沌系统设计了一个新的构造S-Box的算法，对S-Box样本进行各项指标分析对比可见，该算法能够产生密码性良好的S-Box，对差分密码攻击和线性密码攻击的抵抗能力较强。但是，由均匀化系统构造出来的S-box在混沌程度上稍逊一筹，具体原因可能有两方面，一方面是由于均匀化方法导致混沌系统的混沌性受到影响，另一方面是S-box生成算法的不足，未来的研究将从这两方面进行改进，致力于为进一步设计分组密码算法提供良好的非线性资源。

参考文献

[1] Li, Tienyien. and Yorke, J.A. (1975) Period Three Implies Chaos. *American Mathematical Monthly*, **82**, 985-992. https://doi.org/10.1080/00029890.1975.11994008

[2] Matthews, R. (1989) On the Serivation of a "Chaotic" Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[3] Gotz, M., Kelber, K. and Schwarz, W. (1997) Discrete-Time Chaotic Coders for Information Encryption—Part 1: Systematic Structural Design. Workshop on Nonlinear Dynamics of Electronic Systems, Moscow, Russia, 21-26.

[4] Kocarev, L., Jakimoski, G., Stojanovski, T., *et al.* (1998) From Chaotic Maps to Encryption Schemes. P*roceedings of the* 1998 *IEEE International Symposium on Circuits and Systems*, Monterey, CA, USA, 31 May-3 June 1998, 514-517. https://doi.org/10.1109/ISCAS.1998.698968

[5] 盛利元, 曹莉凌, 孙克辉, 等. 基于TD-ERCS混沌系统的伪随机数发生器及其统计特性分析[J]. 物理学报, 2005, 54(9): 4031-4037.

[6] 盛利元, 肖燕予, 盛喆. 将混沌序列变换成均匀伪随机序列的普适算法[J]. 物理学报, 2008, 57(7): 4007-4013.

[7] 曹光辉, 胡凯, 佟维. 基于Logistic均匀分布图像置乱方法[J]. 物理学报, 2011, 60(11): 125-132.

[8] 何振亚, 李克, 杨绿溪. 具有良好安全性能的混沌映射二进制序列[J]. 电子与信息学报, 1999, 21(5): 646-651.

[9] Terry, R. (1990) Substitution Cipher with Pseudo-Random Shuffling: The Dynamic Substitution Combiner. *Cryptologia*, **14**, 289-303. https://doi.org/10.1080/0161-119091864986

[10] Wong, K.W., Ho, S.W. and Yung, C.K. (2003) A Chaotic Cryptography Scheme for Generating Short Cipher Text. *Physics Letters A*, **310**, 67-73. https://doi.org/10.1016/S0375-9601(03)00259-7

[11] 周海玲, 宋恩彬. 二次多项式映射的3-周期点判定[J]. 四川大学学报(自然科学版), 2009, 46(3): 561-564.

[12] 郝柏林. 从抛物线谈起—混沌动力学引论[M]. 北京: 北京大学出版社, 2013: 114-118.

[13] 臧鸿雁, 范修斌, 闵乐泉, 等. S-Box的Lyapunov指数研究[J]. 物理学报, 2012, 61(20): 200508.

[14] Han, M., Shah, T. and Batool, S.I. (2016) Construction of S-Box Based on Chaotic Boolean Functions and Its Application in Image Encryption. *Neural Computing & Applications*, **27**, 677-685. https://doi.org/10.1007/s00521-015-1887-y

[15] 韩丹丹, 闵乐泉, 赵耿, 等. 一维鲁棒混沌映射及S-Box的设计[J]. 电子学报, 2015(9): 1770-1775.

[16] Razaq, A., Yousaf, A., Shuaib, U., *et al*. (2017) A Novel Construction of Substitution Box Involving Coset Diagram and a Bijective Map. *Security & Communication Networks*, **2017**, Article ID: 5101934. https://doi.org/10.1155/2017/5101934

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2163-145X，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：hjdm@hanspub.org