[a,b]-自缩减生成器*)

白恩健 王 静 肖国镇

(西安电子科技大学ISN国家重点实验室 信息安全与保密研究所 西安710071)

摘 要 本文设计了一类新型的密钥流序列生成器—[a,b]-自缩减生成器,仅由一个线性反馈移位寄存器(LFSR)构成,利用相同的初始状态和反馈多项式可以产生一大类伪随机序列。生成序列具有良好的密码学性质:指数级周期,指数级线性复杂度和良好的统计特征。理论分析与局部随机性检验的实验数据都表明[a,b]-自缩减生成器适合于流密码系统的应用。

关键词 伪随机序列,自缩减生成器,周期,线性复杂度,局部随机性检测

The [a,b]-Self-Shrinking Generator

BAI En-Jian WANG Jing XIAO Guo-Zhen

(Nat. Key Lab. On ISN, Inst. of Info. Security and Privacy, Xidian Univ., Xi'an, 710071)

Abstract A new construction of a pseudorandom generator, called the [a,b]-self-shrinking generator, based on a single linear feedback shift register is investigated. The construction allows users to generate large family of sequences using the same initial states and the same characteristic feedback polynomials of the single LFSR. The construction has attractive properties such as exponential period, exponential linear complexity and good statistical properties. Both the theoretic analysis and the experimental results of local randomness tests show that the [a,b]-self-shrinking generator is suitable for practical implementation of efficient stream cipher cryptosystems.

Keywords Pseudo-random sequences, Self-shrinking generator, Period, Linear complexity, Local randomness tests

1 引言

设计性能良好的密钥序列始终是流密码学的一个研究热点。线性反馈移位寄存器(简记为LFSR)因其实现简单,速度快,有较为成熟的理论等优点而成为构造密钥流生成器的最重要的部件之一。目前比较成熟和实用的流密码系统都是基于LFSR构造的。我们可以把这些系统分为两大类:一类是LFSR和非线性布尔函数的组合[1],像非线性组合流密码和前馈流密码都属于此类;另一类是用一个LFSR去控制另一个LFSR。有两种控制模型:钟控型生成器[2]和缩减型生成器[3~6]。缩减生成器[3]由于结构简单而引人注目,有人猜想如此简单的构造也许不够安全,然而至今仍无成功的分析攻击文章发表。A. Kanso[4]构造了一类广义缩减生成器[a,b]-缩减生成器,生成序列具有指数级周期,指数级线性复杂度,良好的统计特征及抗相关分析能力。Meier等[5]受缩减生成器的启发,构造了一个由2元LFSR采用缩减生成器类似的方法构成的自缩生成器,但数据率缩减到原始序列的1/4。在文[6]中,作者构造了一类广义自缩减生成器,生成序列具有群结构、平衡性和良好的相关性质。

本文利用一个2元LFSR构造了另一类广义自缩减生成器,我们称之为[a,b]-自缩减生成器(简记为[a,b]-SSG),所产生的序列称之为[a,b]-自缩序列(简记为[a,b]-SSS)。[a,b]-SSS具有良好的性质:指数级周期、指数级线性复杂度和良好的统计特征。而且利用相同的LFSR初始状态和反馈多项式就可以产生一大类伪随机序列,由于a,b的引入使得采用以前对自缩减生成器的攻击方法分析[a,b]-SSG更为困难。

本文第2小节详细地描述[a,b]-SSG,讨论[a,b]-SSS的数据率,周期,线性复杂度和符号分布等性质;第3小节给出一些局部随机性检测的指标和[a,b]-自缩减m-序列的局部随机性检测结果;最后,以几类自缩减型生成器的比较作为本文的结束。

2 [a,b]-自缩减生成器

2.1 [a,b]-SSG的构造

[a,b]-SSG的基本组成部分是一个2元线性反馈移位寄存器(LFSR)。设LFSR A的级数为n,反馈多项式为$f(x)$,$a_0,a_1,\cdots,a_{n-1}$为A的非0初始状态,输出序列记为(a_t)。记$X_t=aa_t+b(a_t\oplus 1)$,这里$\oplus$为模2运算。定义累积函数:

$$G_A(t)=\sum_{i<t}X_i,(G_A(0)=0) \tag{1}$$

其中$\sum$是在实数域上求和。则[a,b]-SSG的输出比特Z_t按下面的规则对LFSR A的输出序列缩减而成:在任意时刻t,若$a_t=1$,则输出$a_{G_A}(t)$;否则,没有输出。等价地,定义

$$G_t:\{0,1,2\cdots\}\to\{0,1,2,\cdots\}$$

$$G_t(t-1)=G_A(t') \tag{2}$$

其中,$a_{t'}=1$并且t为$a_0,a_1,\cdots,a_{t'}$中1的个数。则[a,b]-SSG的输出比特Z_t为:

$$Z_t=a_{G_t(t)} \tag{3}$$

下面我们举例说明。设2级LFSR的反馈多项式为x^2+x+1,则输出序列为$(a_t)=(011)$。取$a=2,b=1$,则:$G_A(0)=0$,$G_A(1)=1$,$G_A(2)=3$,$G_A(3)=5$,$G_A(4)=6$,$G_A(5)=8$,$G_A(6)=10$,$G_A(7)=11$,$G_A(8)=13$,$G_A(9)=0$,$G_A(10)=1$,$G_A(11)=3$~因此,[2,1]-SSG的输出序列为:

*)基金项目:国家"十五"国防预研基金项目(41001040102);国家重点基础研究发展规划973资助项目(G1999035804)。白恩健 博士研究生。

$(a_{G_A(1)}a_{G_A(2)}a_{G_A(4)}a_{G_A(5)}a_{G_A(7)}a_{G_A(8)})=(a_1a_3a_6a_8a_{11}a_{13})$
$=(100111)$

2.2 $[a,b]$-SSS 的性质

$[a,b]$-SSG 可以应用于任意的2元 LFSR 序列。下面我们将讨论$[a,b]$-SSS 的数据率，周期，线性复杂度和符号分布等性质。

数据率 根据$[a,b]$-SSG 的缩减规则，考虑比特对$(a_i, a_{G_A(i)})$，当 $a_i=0$时没有输出；当 $a_i=1$时输出 $a_{G_A(i)}$。因此假如 LFSR 序列的周期为 N，元素1的个数为 N_1，则数据率为原始序列的 N_1/N。若 LFSR 的反馈多项式为 n 次本原多项式，即输出序列为 m-序列，则 $N=2^n-1, N_1=2^{n-1}$。所以此时数据率为 $N_1/N>1/2$。

周期 设LFSR A 的级数为 n，反馈多项式为 $f(x)$，其输出序列为(a_i)，周期为 N。记 N_1为(a_i)一个周期段中元素为1的个数，N_0为(a_i)一个周期段中元素为0的个数。根据累积函数 G_A 的定义，

$G_A(N^2)=NG_A(N)$，
$G_A(N^2+1)=NG_A(N)+X_0$，
$G_A(N^2+2)=NG_A(N)+X_0+X_1$，
……

因此，当(a_i)输出 N^2个比特后，$G_A(t)$开始重复，即序列(a_i)和$[a,b]$-SSG 输出序列同时回到初始状态。因此$[a,b]$-SSS 为周期序列。由于当 $a_i=1$时才有比特输出，因此(a_i)输出 N^2个比特后，$[a,b]$-SSG 输出 N_1N 个比特。因此$[a,b]$-SSG 的输出序列 $Z=(z_i)$的周期 P_Z 整除 N_1N。综上所述，有定理1：

定理1 设(a_i)为 LFSR 的输出序列，周期为 N。记 N_1为(a_i)一个周期段中元素为1的个数，Z 表示$[a,b]$-SSG 的输出序列，则 Z 为周期序列，它的周期 P_Z 整除 N_1N。

事实上，当满足一定的条件时，最大周期 N_1N 可以达到。

定理2 设 $c=\max(a,b)$，若 LFSR 的级数 $n<N/c$，并且 $(N,G_A(N))=1$，则 $P_Z=N_1N$。

证明：由定理1知 $P_Z|N_1N$，因此只需证明 $N_1N|P_Z$。由(3)式可得 $Z_i=a_{G_e(i)}$，根据$[a,b]$-SSS 的定义对任意 $j\geqslant 0$，

$$z_{i+jN_1}=a_{G_e(i)+jG_A(N)} \tag{4}$$

首先，证明下面的结论：

(*)若 $a_{k+jG_A(N)}=a_{k'+jG_A(N)}(\forall\ j\geqslant 0)$，则 $N|(k-k')$。

事实上，定义序列 $c_i=a_{iG_A(N)}(t\geqslant 0)$，则序列$(c_i)$为序列$(a_i)$的 $G_A(N)$-采样序列。由于$(N,G_A(N))=1$，因此序列(c_i)的周期为 N。若 $a_{k+jG_A(N)}=a_{k'+jG_A(N)}(\forall\ j\geqslant 0)$，定义 $k=hG_A(N) \bmod N, k'=h'G_A(N) \bmod N$，则 $c_{i+k}=c_{i+k'}$，因此 $N|(h-h')$。则 $N|(h-h')G_A(N)$，即 $N|k-k'$。所以结论(*)成立。

根据周期的定义，$z_i=z_{i+P_z}$。同样地，对$\forall\ i,j, z_{i+jN_1}=z_{i+jN_1+P_z}$。由(4)式可得 $a_{G_e(i)+jG_A(N)}=a_{G_e(i+P_z)+jG_A(N)}$，再由(*)结论可得：

$$N|G_e(i+P_z)-G_e(i) \tag{5}$$

其次证明(5)式成立当且仅当 $N_1|P_Z$。(5)式可以表示成：

$$G_e(i+P_Z)=G_e(i)+j_iN \tag{6}$$

同样地，设 $i=i+1$，则

$$G_e(i+1+P_Z)=G_e(i+1)+j_{i+1}N \tag{7}$$

(7)式减去(6)式得

$$G_e(i+1+P_Z)-G_e(i+P_Z)=G_e(i+1)-G_e(i)+(j_{i+1}-j_i)N \tag{8}$$

由于 n 级 LFSR 的输出序列不存在 n 长0-游程，因此 $G_e(i+1)-G_e(i)\leqslant nc$。由此可以断定 $j_{i+1}-j_i=0$。否则，$N\leqslant nc$，这与定理的条件 $n<N/c$ 相矛盾。因此，

$$G_e(i+1+P_Z)-G_e(i+P_Z)=G_e(i+1)-G_e(i) \tag{9}$$

(9)式表明在 LFSR 的输出序列(a_i)中，以 $a_{i'}$为起点的序列与以 $a_{(i+P_Z)'}$为起点的序列为相同序列(这里，$a_{i'}=a_{(i+P_Z)'}=1, G_e(i)=G_A((i'), G_e(i+P_Z)=G_A(i+P_Z)')$)，因此 $N|[(i+P_Z)'-i']$。同样地，在序列 $a_{i'}, a_{(i+1)'}, \cdots, a_{(i+P_Z-1)'}$中元素为1的个数为 N_1的倍数。同时，在序列 $a_{i'}, a_{(i+1)'}, \cdots, a_{(i+P_Z-1)'}$中元素为1的个数恰好为 P_Z，因此 $N_1|P_Z$。

不妨设 $P_Z=N_1u$，则对任意 $j, a_{G_e(0)}=z_0=z_{jP_Z}=Z_{jN_1u}=a_{G_e(0)+juG_A(N)}$，所以 $N|uG_A(N)$。又因为$(N,G_A(N))=1$，故 $N|u$，所以 $NN_1|uN_1=P_Z$。所以，序列(z_i)的周期 $P_Z=N_1N$。证毕

线性复杂度 是度量密钥流序列不可预测性的重要指标，定理3给出了$[a,b]$-SSS 的线性复杂度估计。

定理3 设 LFSR A 的输出序列为 n 级 m-序列，$c=\max(a,b)$。若 $n<2^n-1/c$，并且$(2^n-1, 2^{n-1}a+(2^{n-1}-1)b)=1$，则$[a,b]$-SSG 的输出序列$(z_i)$的线性复杂度 LC 满足：

$$n\cdot 2^{n-2}<LC\leqslant n\cdot 2^{n-1}$$

证明：因为 n 级 m-序列的周期为 $N=2^n-1$，一个周期段中1元素的个数为 $N_1=2^{n-1}$，0元素的个数为$2^{n-1}-1$，并且

$$\begin{aligned}G_A(N)&=G_A(N-1)+aa_{N-1}+b(a_{N-1}\oplus 1)=\cdots\cdots\\&=a[a_0+\cdots+a_{N-1}]+b[(a_0\oplus 1)+\cdots+(a_{N-1}\oplus 1)]'\\&=2^{n-1}a+(2^{n-1}-1)b\end{aligned}$$

所以由定理2可知序列(z_i)的周期为$2^{n-1}N$。

根据线性复杂度的定义，如果存在 d 次多项式 $p(x)$，满足 $\sum_{i=0}^{d}p_iz_{i+t}=0(\forall\ t\geqslant 0)$，则序列$(z_i)$的线性复杂度至多为 d。设对任意$0\leqslant k<N_1$，$(z_{k+t}^{N_1})$表示序列(z_i)的 N_1-采样序列。即 $z_{k+j}^{N_1}=z_{k+jN_1}, j=0,1,\cdots$。由(4)式 $z_{k+jN_1}=a_{G_e(k)+jG_A(N)}$，即$(z_{k+t}^{N_1})$为序列$(a_i)$的 $G_A(N)$-采样序列。由于$(N,G_A(N))=1$，并且序列(a_i)为 m-序列，因此$(z_{k+t}^{N_1})$为 m-序列并且其线性复杂度为 n。故存在 n 次多项式 $q(x)$，满足 $q(z_{k+t}^{N_1})=0$。不妨设 $q(x)=\sum_{i=0}^{n}q_ix^i$，则对 $k=0,1,\cdots,N_1-1$ 均满足 $\sum_{i=0}^{n}q_iz_{k+(i+t)N_1}=0$。因此序列 $z_{tN_1}, z_{1+tN_1}, \cdots, z_{N_1-1+tN_1}, \cdots z_{N_1-1+(i+n)N_1}$满足递归关系 $\sum_{j=0}^{nN_1}p_jz_{i+j}=0(i\geqslant 0)$，这里

$$\begin{cases}p_j=0, j \bmod N_1\neq 0\\ p_jN_1=q_j, j=0,1,\cdots,n\end{cases}$$

故存在多项式 $p(x)=[q(x)]^{N_1}$，满足 $p(z_i)=0$。又多项式 $p(x)$的次数为 $nN_1=n\cdot 2^{n-1}$，所以序列(z_i)的线性复杂度 $LC\leqslant n\cdot 2^{n-1}$。

设 $g(x)$为序列(z_i)的极小多项式，由上面的证明可知 $q(x)$为不可约多项式并且 $q^{N_1}(z_i)=0$，所以 $g(x)|[q(x)]^{N_1}$。又 $N_1=2^{n-1}$，所以 $g(x)$的表达式为 $g(x)=[q(x)]^r, r\leqslant 2^{n-1}$。如果 $r\leqslant 2^{n-2}$，则 $g(x)|[q(x)]^{2^{n-2}}$。由于 $q(x)|1-x^N$，因此 $g(x)|(1-x^N)^{2^{n-2}}=(1-x^{2^{n-2}N})$，这与序列$(z_i)$的周期为$2^{n-1}N$相矛盾，故 $r>2^{n-2}$。因此序列(z_i)的线性复杂度 $LC>n\cdot 2^{n-2}$。

综上所述，序列(z_i)的线性复杂度满足 $n\cdot 2^{n-2}<LC\leqslant n\cdot 2^{n-1}$。 证毕

线性复杂度具有不稳定现象[9]。良好的密钥流序列不仅应该具备非常大的线性复杂度，而且改变序列一个周期段中几个符号后不会引起线性复杂度的急剧下降。定理4讨论了$[a,b]$-SSS 的线性复杂度稳定性。

定理4 设 LFSR A 的输出序列为 n 级 m-序列，$c=\max$

(a,b)。若 $n<2^n-1/c$，并且$(2^n-1,2^{n-1}a+(2^{n-1}-1)b)=1$，记 $[a,b]$-SSG 的输出序列为 $Z=(z_t)$。则 Z 的1-重量复杂度 WC_1 满足：$WC_1(Z)\geqslant(2^n-n-1)\cdot 2^{n-1}$。

证明：由定理3的证明知在定理条件下，序列 $Z=(z_t)$ 的周期为 $P_Z=2^{n-1}(2^n-1)$。设 $f_z(x)$ 为 Z 的极小多项式，$Z^{P_Z}(x)=z_0+z_1x+\cdots+z_{P_Z-1}x^{P_Z-1}$。由文[9](p44，定理3.2.4)则：

$f_z(x)=1-x^{P_Z}/\gcd(1-x^{P_Z},Z^{P_Z}(x))$。

记 $g(x)=\gcd(1-x^{P_Z},Z^{P_Z}(x))$，则对$0\leqslant i\leqslant P_Z-1$，有

$$\begin{aligned}g_1(x)&=\gcd(1-x^{P_Z},Z^{P_Z}(x)+x^i)\\&=\gcd(f_zg(x),Z^{P_Z}(x)+x^i)\\&=\gcd(f_z,Z^{P_Z}(x)+x^i)。\end{aligned}$$

因此由文[9]（定理4.2.2）可得

$$\begin{aligned}WC_1(Z)&=\min_{0\leqslant i\leqslant P_Z-1}\{\deg[(1-x^{P_Z})/g_1(x)]\}\geqslant\deg[(1-x^{P_Z})/f_z(x)]=P_Z-LC(Z)\geqslant P_Z-n\cdot 2^{n-1}=\\&\quad 2^{n-1}\cdot(2^n-1)-n\cdot 2^{n-1}\\&=(2^n-n-1)\cdot 2^{n-1}。\end{aligned}$$

证毕

当 $n\geqslant 3$时，$WC_1(Z)\geqslant(2^n-n-1)\cdot 2^{n-1}>n\cdot 2^{n-1}\geqslant LC(Z)$。因此，序列$(z_t)$的线性复杂度是极不稳定的，但是这种不稳定表现在线性复杂度的急剧增大上。因而从稳定性的观点看$[a,b]$-SSS 作为密钥流序列是安全的。

符号分布(symbol distribution)　有定理5：

定理5　设 $c=\max(a,b)$，若 LFSR 的级数 $n<N/c$，输出序列(a_t)的周期为 N，并且$(N,G_A(N))=1$。记 N_1为(a_t)一个周期段中元素为1的个数，N_0为(a_t)一个周期段中元素为0的个数，则在$[a,b]$-SSS 的一个周期段中有 N_1^2个1，N_1N_0个0。

证明：当序列(a_t)输出 N^2个比特后，$[a,b]$-SSG 输出了 N_1N 个比特。显然 $G_A(i)\bmod N\in[0,N-1]$，$0\leqslant i\leqslant N^2-1$，并且在 N^2个值中取0，1，…，$N-1$均为 N 个，故在$[a,b]$-SSG 的输出序列中与 $a_t=1$相对应 $G_A(t)$取0，1，…，$N-1$的个数均为 N_1。而在(a_t)一个周期段中元素为1的个数为 N_1，元素为0的个数为 N_0，因此$[a,b]$-SSS 的一个周期段中有 N_1^2个1，N_1N_0个0。　证毕

3　局部随机性检测

周期，线性复杂度和符号分布是判断序列整体随机性的重要指标，必须考虑序列的一个全周期时才能获得这些结果。第2小节后半部分的数学分析结果表明当满足一定的条件时$[a,b]$-SSS 具有良好的整体随机性（指数级周期，指数级线性复杂度和基本平衡序列）。但是仅有整体随机性还是不够的，必须同时考虑序列的局部随机性质。当序列两个方面的随机性质都比较好时才能够以很大的概率断定伪随机序列“接近”真随机序列，适合于流密码系统的应用。本小节首先介绍几个2元序列局部随机性检测的指标[7,8]，然后给出$[a,b]$-SSS 的局部随机性检测结果。

3.1　局部随机性检测指标

用于检测序列局部随机性的指标有很多，我们只介绍其中最重要的5个，并利用这5个指标检测本文设计的$[a,b]$-SSG 的局部随机性。这里假设截取序列的长度为 N，其中0，1元素的个数分别为 N_0，N_1。为了判断2元序列是否通过局部随机性检测，需要假设一个决策门限值 α，本文取 $\alpha=5\%$。

Frequency Test　该指标用于检测 N 长序列中1元素的个数是否与均值 $N/2$相差很大。计算：

$$T=(N_0-N_1)^2/N \tag{10}$$

T 服从自由度为1的 χ^2分布，即 $T\sim\chi^2(1)$。当决策门限值 $\alpha=5\%$时，由 χ^2分布表知 $\chi^2=3.84$，因此若 $T<3.84$，则检测通过。

Serial Test　该指标用于检测 N 长序列中00，11，01，10出现的次数是否比较接近。计算：

$$T=[4/(N-1)]\sum_{i=0}^{1}\sum_{j=0}^{1}N_{ij}^2-(2/N)\sum_{i=0}^{1}N_i^2+1 \tag{11}$$

T 服从自由度为2的 χ^2分布，即 $T\sim\chi^2(2)$。这里 N_{00}，N_{11}，N_{10}，N_{01}分别表示00，11，10，01出现的次数。当决策门限值 $\alpha=5\%$时，由 χ^2分布表知 $\chi^2=5.99$，因此若 $T<5.99$，则检测通过。

Poker Test　该指标用于检测 N 长序列中2^m 个 $m(m>2)$长比特出现次数的接近程度。把 N 长序列分成 K 个组，$K=\lfloor N/m\rfloor$表示不超过 N/m 的最大整数。计算：

$$T=(2^m/K)\sum_{i=0}^{2^m-1}f_i^2-K \tag{12}$$

T 服从自由度为 m 的 χ^2分布，即 $T\sim\chi^2(m)$。设 $i=i_{m-1}2^{m-1}+\cdots+i_12+i_0$，则 f_i 表示$(i_{m-1},\cdots,i_1,i_0)$出现的次数。当决策门限值 $\alpha=5\%$，$m=3,4,5$时，相对应的 χ^2值分别为14.067，24.996，44.970。因此若 $T<\chi^2$，则检测通过。

Runs Test　该指标用于检测序列中各种长度的游程总数是否与真随机序列相似。当 Serial Test 通过时才进行 Runs Test。计算 $\text{Mean}=1+(2N_0N_1/N)$，$\text{Variance}=(\text{Mean}-1)(\text{Mean}-2)/(N-1)$以及

$$T=(\text{Runs}-\text{Mean})/\sqrt{\text{Variance}} \tag{13}$$

T 服从均值为0，方差为1的正态分布，即 $T\sim N(0,1)$。当决策门限值 $\alpha=5\%$时，若$|T|<1.96$，则检测通过。

Autocorrelation Test　该指标用于检测序列与其移位序列之间是否存在相关性。计算：

$$T(d)=\sum_{i=0}^{N-d-1}z_i\oplus z_{i+d}\quad(d>0) \tag{14}$$

若$\left|[T(d)-((N-d)/2)]/\sqrt{(N-d)/2}\right|<1.96$，则检测通过。

3.2　检测结果

我们对 m-序列的$[a,b]$-自缩减序列进行局部随机性检验。取 $N=5000$，为此 m-序列的极小多项式次数 $n>6$，并且同时满足 $n<(2^n-1)/\max(a,b)$，$(2^n-1,2^{n-1}a+(2^{n-1}-1)b)=1$，此时$[a,b]$-SSS 的周期为$2^{n-1}(2^n-1)>5000$。随机选取50条序列做检测，检测结果表明有86%的序列通过了全部检测。以7级 m-序列为例，其生成多项式为 $f(x)=x^7+x+1$，分别取 $a=3,b=4$和 $a=5,b=3$，此时均满足$(G_A(N),N)=1$。表1列出了[3,4]-SSS 和[5,3]-SSS 的局部随机性检测结果。

表1　决策门限值 $\alpha=5\%$的$[a,b]$-SSS 局部随机性检验

Tests	[3,4]-SSS	[5,3]-SSS
Frequency Test	1.479	0.001
Serial Test	3.137	0.522
Poker Test		
$m=3$	3.772	6.086
$m=4$	5.706	6.141
$m=5$	29.056	27.968
Runs Test	1.280	0.693
Autocorrelation Test		
$d=1$	0.940	0.540
$d=2$	0.440	0.520
…	…	…
$d=14$	0.661	2.103
…	…	…
$d=19$	1.824	0.160
$d=20$	1.683	0.321
Results	PASS	REJECT
Linear Complexity	413	420

（下转第158页）

出相应的诊断结果，以及为什么得出该结果的解释。

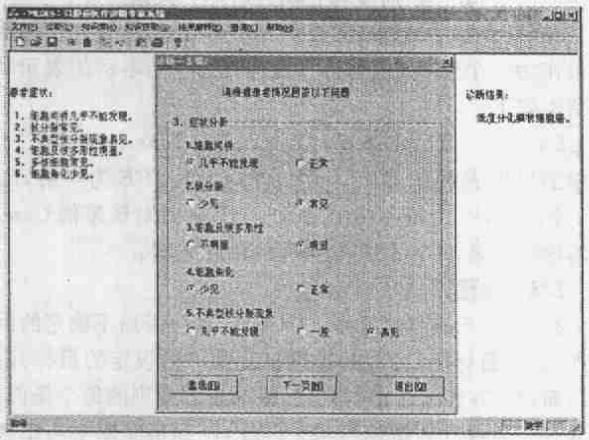

图2 OCDES 系统界面

我们设计了一种类似 V. L. Yu[6]等人提出的对 MYCIN 的“评价和测试方法的评价和测试”格式表，即“口腔癌诊断专家系统”性能评价测试表。

OCDES 系统性能评价测试方法是对某一患者的病症系统推理诊断之前，先由“口腔癌专家”根据该患者的病症进行专家级诊断，并详细记录专家的诊断意见和结论，然后运用 OCDES 诊断专家系统进行推理诊断，并逐项比较两者的诊断结果，找出两者的差异。该评价方法不仅能逐渐改进和完善 OCDES 系统，并能使该系统的诊断结果逐渐达到“口腔癌专家”的诊断水平，使系统达到实用化。

结束语 OCDES 系统采用模块化程序设计技术，按逻辑功能合理划分模块、编程、生成各自对应的目标模块，调试和维护十分灵活方便。另外系统还提供了图文并茂的输出信息，便于使用者的理解。目前系统还在不断地扩充口腔癌专家的知识和经验，在使用中将会逐渐地完善，以使该系统达到对口腔癌的辅助诊断和咨询的目标。

参 考 文 献

1 陈世福，潘金贵，等. 知识工程语言与应用. 南京大学出版社，1989
2 杭小树，张友华，等. 一个综合知识发现与知识求精系统—XFKDRS. 模式识别与人工智能，2002,15(4)：334～338
3 花蕾，杨育彬，等. 基于知识的肺癌早期细胞病理诊断专家系统. 计算机应用与研究，2000,17(2)：90～92
4 杨育彬，李宁，等. 肺癌分类识别中的神经网络集成技术研究. 计算机科学，2003,30(9)：39～42,53
5 于世风，汪说之，等. 口腔组织病理学. 人民卫生出版社(北京)，2003. 8
6 Shortliffe E H. Computer-based Medical Consultation：MYCIN. American Elsevier，Newyork，1976
7 金传伟. 缺陷诊断专家系统的知识与推理技术. 计算机工程与应用，2002,13：119～121
8 陈世福，等. 勘探地下水专家系统 NCGW 的设计与实现. 计算机学报，1989,12(6)：452～457

(上接第109页)

根据第2小节的理论分析以及本小节的实验结果可以得出结论[a,b]-SSG 适合于在流密码系统中应用。

4 几类自缩减型生成器的比较

Meier[5]将缩减生成器[3]简化为自缩减生成器，只用一个线性反馈移位寄存器得到一个隔位受控输出序列。Kanso[4]改变了自缩减生成器的输出规则：考虑比特对(a_i,a_{i+1})，若 $a_i=1$，则输出 a_{i+1}；否则，没有输出。Hu[6]进一步将自缩减生成器推广，得到了广义自缩减生成器。其输出规则为：设 $a=\cdots a_{-2}a_{-1}a_0a_1a_2\cdots$ 为 $GF(2)$上的 m-序列，周期为2^n-1，$G=(g_0,g_1,\cdots,g_{n-1})$。序列 v 满足

$$v_k=g_0a_k+g_1a_{k-1}+\cdots+g_{n-1}a_{k-n+1} \quad (15)$$

若 $a_k=1$，则输出 v_k；否则，没有输出。广义自缩减序列具有群结构和良好的相关性质。

表2列出了上述3种自缩减型生成器(分别称之为 Meier 生成器，Kanso 生成器和 Hu 生成器)与本文的[a,b]-自缩减生成器的性质比较。这里被缩减的序列均为 n-级 m-序列。

表2 几类自缩减型生成器的比较

	数据率	周期	线性复杂度	符号分布
Meier 生成器	1/4	$2^{\lfloor n/2\rfloor}<P\leqslant 2^{n-1}$	$2^{\lfloor n/2\rfloor-1}<LC\leqslant 2^{n-1}-n+2$	平衡序列
Kanso 生成器	1/2	$P=2^{n-1}$	$2^{n-2}<LC\leqslant 2^{n-1}-n+2$	平衡序列
Hu 生成器	一族序列	不少于3/4的序列周期为2^{n-1}，不少于7/8的序列周期$\geqslant 2^{n-3}$		平衡序列
[a,b]-自缩减生成器	>1/2	$2^{n-1}(2^n-1)$	$n\cdot 2^{n-2}<LC\leqslant n\cdot 2^{n-1}$	0,1符号的个数分别为2^{2n-2}和$2^{n-1}(2^{n-1}-1)$

从表2可以看出满足一定的条件下[a,b]-SSS 的周期与线性复杂度性质是最优的。而且对同一个反馈多项式和相同的初始状态，改变 a,b 的值就可以得到不同的输出序列。由于[a,b]-SSS 具有指数级线性复杂度，因此能够抵抗 B-M 综合算法的攻击。

关于[a,b]-SSG 的密码分析，需要做进一步的讨论，我们将在后续工作中解决这一问题。但有一点可以肯定的是由于 a,b 的引入，使得对[a,b]-SSG 的密码分析更为困难。

参 考 文 献

1 Rueppel R A. Stream ciphers, Contemporary, the Science of Information. IEEE Press, Gustovos J. Simmons, editor, 1992. 65～134
2 Gollman D, Chambers W G. Clock-controlled shift registers: a review. IEEE Journal on Selected Areas in Communications, 1989, 7(4):525～533
3 Coppersmith D, Krawczys H, Mansour Y. The shrinking generator, Advances in Cryptology-Crypt'93, LNCS, vol. 765. Berlin: Springer-Verlag, 1994. 22～39
4 Kanso A. Clock-controlled generators: [PhD thesis]. University of London ,1999. 132～185
5 Meier W, Staffelbach O. The self-shrinking generator, Advances in Cryptology-Eurocrypt'94, LNCS, vol. 950. Berlin: Springer-Verlag, 1995. 205～214
6 HU Yupu, XIAO Guozhen. The generalized self-shrinking generator. IEEE Trans. on Info. Theory, to appear
7 Beker H, Piper F. Cipher Systems: The protection of communications. New York: van Nostrand Reinhold, 1982
8 Erdemann E. Empirical tests of binary keystreams: [MPhil Thesis]. University of London, 1992
9 丁存生，肖国镇. 流密码学及其应用. 北京：国防工业出版社，1994