对 Py 的一种改进的区分攻击

胡学先,那 键,刘文芬
HU Xue-xian,NA Jian,LIU Wen-fen

信息工程大学 信息工程学院,郑州 450002
Institute of Information Engineering,Information Engineering University,Zhengzhou 450002,China
E-mail:xuexian_hu@yahoo.com.cn

HU Xue-xian,NA Jian,LIU Wen-fen.Improved distinguishing attack on Py.Computer Engineering and Applications, 2007,43(16):152-155.

Abstract: A method for efficiently computing the conditional probability of the output sequence of Py is given, which is based on the theory of hidden Markov model, and from this a distinguisher optimal for this model is built. For the same advantage as that of the best known distinguisher,this attack results in a reduction in the samples needed by a factor of approximately 3.2.
Key words: stream cipher;distinguishing attack;Hidden Markov Model

摘 要:提出了对流密码算法的一种改进的区分攻击方法。首先利用隐 Markov 模型给出了有效计算的输出序列在一个特定的事件发生的情况下的条件分布的公式,并由此构造了一个"最优"区分器,在区分优势和目前最有效的区分攻击相同的情况下,所需密钥流长度缩短为原来的 1/3.2。
关键词:流密码;区分攻击;隐 Markov 模型
文章编号:1002-8331(2007)16-0152-04 **文献标识码**:A **中图分类号**:TP309.7

1 引言

Py 是由 Biham 和 Seberry[1]提交给 ECRYPT 计划的一个面向软件实现的候选算法, 在 2006 年 3 月公布的第二轮选拔结果中被选为面向软件实现的最有希望的 7 个候选算法之一。该算法用两个大的滚动数组(Rolling Array)作为其主要部件,内部状态共有 1 300 个字节, 每次状态更新后输出两个 32 bit 的字作为密钥流,实现速度比 RC4 快 2.5 倍。

在文献[2]中,Souradyuti 等定义了一个关于内部状态的事件 L,并证明了在 L 发生的条件下,输出密钥流中某两个字 $O_{1,1}$、$O_{2,3}$ 的最低有效位 $[O_{1,1}]_0$、$[O_{2,3}]_0$ 必定以概率 1 相等。文献[3]同样在发生的条件下,利用隐 Markov 模型,给出了有效计算 $O_{1,1}$、$O_{2,3}$ 的联合分布的方法,并由此构造了一个更为有效的区分器,在区分效果与文献[2]相同的情况下所需的密钥流长度缩减为原来的 1/60 552。

Souradyuti 等还定义了另外一个事件 L',并指出事件 L' 和事件 L 发生的概率是一样的,且当事件 $L\cup L'$ 不发生时,$O_{1,1}$ 和 $O_{2,3}$ 是相互独立且均匀分布的字[2]。本文中,我们综合利用事件 L 和事件 L' 发生的条件下 $O_{1,1}$、$O_{2,3}$ 的联合分布信息, 通过隐 Markov 模型给出 L' 发生的条件下其条件概率的一个有效的计算公式,并由此建立了一个更为有效的区分器。在区分效果与文献[2]相同的情况下所需的密钥流长度降低为文献[2]中的 1/191 203,为文献[3]中的 1/3.2。

2 Py 简介

Py 的内部状态主要包括两个滚动数组 P、Y 及一个字 s,P 是一个 256 个字节长的数组,分别记为 $P[0],P[1],\cdots,P[255]$。P 中元素的取值总是{0,1,2,…,255}的一个置换。Y 是包含 260 个字的数组,分别记为 $Y[-3],Y[-2],\cdots,Y[256]$。分别记时刻时的 P、Y 及 s 为 P_i,Y_i 及 s_i。对任意字(或字节)C,记从最低有效位起的第比特为 $[C]_j$。类似于文献[2],记 Py 的每一轮如下:

算法 1 Py 的一轮更新

$$O_{1,i}=(\mathrm{ROTL32}(s_i,25)\oplus Y_i[256])+Y_i[P_i[26]]$$

$$O_{2,i}=(s_i\oplus Y_i[-1])+Y_i[P_i[208]]$$

$$Y_{i+1}=Y_i[-2\cdots 256]\,\|\,((\mathrm{ROTL32}(s_i,14)\oplus Y_i[-3])+Y_i[P_i[153]])$$

$$P_{i+1}=\begin{cases}P_i[1\cdots k-1]\,\|\,P_i[0]\,\|\,P_i[k+1\cdots 255]P_i[k] & k\neq 0\\ P_i[1\cdots 255]\,\|\,P_i[0] & k=0\end{cases}$$

$$s_{i+1}=\mathrm{ROTL32}(s_i+Y_{i+1}[P_{i+1}[72]]-Y_{i+1}[P_{i+1}[239]],(P_{i+1}[116]+18)\&31)$$

其中 $k=Y_{i+1}[185]\bmod 256$,"‖"代表字符串的串联,$O_{1,i}$、$O_{2,i}$ 为 i 轮输出的密钥流。

假设密钥建立过程之后得到的 P_1,Y_1 及 s_1 是完全随机的,即 P_1 在所有可能的置换上均匀分布,Y_1、s_1 分别在 $F_2^{260\times 32}$、F_2^{32} 上均匀分布,且还假设 P_1、Y_1、s_1 相互独立。

3 隐 Markov 模型

称一个取值于字符集 $\Psi=\{s_1,s_2,\cdots,s_N\}$ 的随机序列 Q_1,

作者简介:胡学先(1982-),男,硕士研究生,主要研究方向为概率论及其在密码学中的应用;那键(1981-),男,硕士研究生,主要研究方向为概率论及其在密码学中的应用;刘文芬(1965-),女,博士,教授,硕士生导师,主要研究方向为概率论及其在密码学中的应用。

$Q_2,\cdots,Q_n$为一个一阶 Markov 链,若对任意的 $0\leqslant i\leqslant n-1$,对任意的 $q_0,q_1,\cdots,q_{i+1}\in\Psi$

$$\Pr\{Q_{i+1}=q_{i+1}|Q_i=q_i,Q_{i-1}=q_{i-1},\cdots,Q_0=q_0\}=\Pr\{Q_{i+1}=q_{i+1}|Q_i=q_i\}$$

记其初始分布向量为 $\boldsymbol{\pi}$,其中 $\pi_i=\Pr\{Q_0=s_i\}$。记时刻 i 时的转移矩阵为 $\boldsymbol{M}^i$,其中第 k 行第 j 列的元素 $m^i_{kj}=\Pr\{Q_{i+1}=s_k|Q_i=s_j\}$。

一个隐 Markov 模型[4,5]由一列形成一阶 Markov 链的隐状态和对应于隐状态转移的可见状态组成。记可见状态的取值字符集为 y,对任意的 $y\in y$,定义隐 Markov 模型时刻 i 的转移矩阵为 $\boldsymbol{M}^i_y$,其中第 k 行第 j 列的元素 $m^i_{y,kj}=\Pr\{Y_i=y,Q_{i+1}=s_k|Q_i=s_j\}$。

转移矩阵已知时,对任意给定的可见状态序列$(y_0,y_1,\cdots,y_{n-1})$,其出现的概率可由"前向算法"计算:

$$\Pr\{(Y_0,Y_1,\cdots,Y_{n-1})=(y_0,y_1,\cdots,y_{n-1})\}=$$
$$(1,1,\cdots,1)M^{n-1}_{y_{n-1}}\cdots M^0_{y_0}\pi$$

4　条件概率的计算

为综合利用文献[2]中定义的事件 L 和 L',以构造比只利用一个事件 L 的情况下更为有效的区分器,本节首先给出有效的计算条件概率 $\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)|L'\}$的方法。事件 L'定义为如下 6 个事件的交:

$P_2[116]\equiv -18(\mathrm{mod}\ 32)$

$P_3[116]\equiv 7(\mathrm{mod}\ 32)$

$P_2[72]\equiv P_3[72]+1(\mathrm{mod}\ 32)$

$P_2[239]\equiv P_3[239]+1(\mathrm{mod}\ 32)$

$P_1[26]=1$

$P_3[208]=254$

Souradyuti 指出 $\Pr(L)=\Pr(L')$,且当事件 L'发生的时候,有

$O_{1,1}=(\mathrm{ROTL32}(S,25)\oplus B)+A$

$O_{2,3}=(\mathrm{ROTL32}(S+2K,25)\oplus A)+B$

其中 S、K、A、B 是 4 个相互独立且均匀分布的字。

若记 $S_1=\mathrm{ROTL32}(S,25)$,$S_2=\mathrm{ROTL32}(S+2K,25)$,则根据 S 和 K 的随机性可知,除了必须满足$[S_1]_{25}=[S_2]_{25}$外,S_1 和 S_2 的所有 bit 均可以看成是 F_2 上的相互独立且均匀分布的随机变量。

引理1[6]　对任意两个 32 bit 长的整数 x、y,若记

$$z=\mathrm{carry}(x,y)=(x+y)\oplus x\oplus y$$

则$[z]_0=0$ 且$[z]_{i+1}=\mathrm{maj}([x]_i,[y]_i,[z]_i)$,$i=0,1,\cdots,30$,其中 maj(·)为择多函数。

令 $c_1=\mathrm{carry}(S_1\oplus B,A)$,$c_2=\mathrm{carry}(S_2\oplus A,B)$。则易知序列$\{([c_1]_i,[c_3]_i)\}_{i=0}^{31}$构成了一个 Markov 链,初始分布满足 $\Pr\{([c_1]_0,[c_3]_0)=(0,0)\}=1$。此时,隐 Markov 模型的可见状态序列为$\{([O_{1,1}]_i,[O_{2,3}]_i)\}_{i=0}^{31}$。

这个模型的每次内部状态转移及输出取决于模型的当前状态以及 4 bit 随机输入$[A]_i$,$[B]_i$,$[S_1]_i$,$[S_2]_i$,因此除时刻 25 以外,其它时刻的输入均是相互独立且均匀分布的 0、1 随机变量,故这些时刻模型的转移矩阵是相同的。

定理 1　当 $0\leqslant i\leqslant 31$ 且 $i\neq 25$ 时,上述隐 Markov 模型的转移矩阵为:

$$\boldsymbol{M}^i_{(0,0)}=\begin{pmatrix}1/16&0&0&0\\1/16&1/8&0&0\\1/16&0&1/8&0\\1/16&1/8&1/8&1/4\end{pmatrix}\quad \boldsymbol{M}^i_{(0,1)}=\begin{pmatrix}1/8&1/16&0&0\\0&1/16&0&0\\1/8&1/16&1/4&1/8\\0&1/16&0&1/8\end{pmatrix}$$

$$\boldsymbol{M}^i_{(1,0)}=\begin{pmatrix}1/8&0&1/16&0\\1/8&1/4&1/16&1/8\\0&0&1/16&0\\0&0&1/16&1/8\end{pmatrix}\quad \boldsymbol{M}^i_{(1,1)}=\begin{pmatrix}1/4&1/8&1/8&1/16\\0&1/8&0&1/16\\0&0&1/8&1/16\\0&0&0&1/16\end{pmatrix}$$

证明　对任意 $0\leqslant i\leqslant 24$ 或 $26\leqslant i\leqslant 31$,上述隐 Markov 模型中转移概率计算如下:

$$\Pr\{([O_{1,1}]_i,[O_{2,3}]_i)=(w_1,w_3),([c_1]_{i+1},[c_3]_{i+1})=(v_1,v_3)|([c_1]_i,[c_3]_i)=(u_1,u_3),L'\}=$$
$$\frac{\left|\left\{(a,b,s_1,s_3)\in\{0,1\}^4\ \middle|\ w_1=s_1\oplus b\oplus a\oplus u_1,w_3=s_3\oplus b\oplus a\oplus u_3,v_1=\mathrm{maj}(s_1\oplus b,a,u_1),v_3=\mathrm{maj}(s_3\oplus a,b,u_3)\right\}\right|}{16}=$$
$$\frac{\left|\left\{(a,b,s_1',s_3')\in\{0,1\}^4\ \middle|\ w_1=s_1'\oplus u_1,w_3=s_3'\oplus u_3,v_1=\mathrm{maj}(s_1'\oplus a,a,u_1),v_3=\mathrm{maj}(s_3'\oplus b,b,u_3)\right\}\right|}{16}=$$
$$\frac{\left|\left\{(a,b,s',s_3')\in\{0,1\}^4\ \middle|\ w_1=s_1'\oplus u_1,w_3=s_3'\oplus u_3,v_1=\mathrm{IF}(s_1',a,u_1),v_3=\mathrm{IF}(s_3',b,u_3)\right\}\right|}{16}=$$

$$\begin{cases}1/4 & \text{if } v_1=u_1=\bar{w}_1,v_3=u_3=\bar{w}_3\\1/8 & \text{if } v_1=u_1=\bar{w}_1,u_3=w_3\\1/8 & \text{if } u_1=w_1,v_3=u_3=\bar{w}_3\\1/16 & \text{if } u_1=w_1,u_3=w_3\\0 & \text{otherwise}\end{cases}$$

其中

$$\mathrm{IF}(x,y,z)=\begin{cases}y & \text{if } x=0\\z & \text{if } x=1\end{cases}$$

由此并根据转移矩阵的定义即可得定理结论。

定理 2　当 $i=25$ 时,上述隐 Markov 模型的转移矩阵为

$$\boldsymbol{M}^{25}_{(0,0)}=\begin{pmatrix}1/8&0&0&0\\1/8&0&0&0\\1/8&0&0&0\\1/8&0&0&1/2\end{pmatrix}\quad \boldsymbol{M}^{25}_{(0,1)}=\begin{pmatrix}0&1/8&0&0\\0&1/8&0&0\\0&1/8&1/2&0\\0&1/8&0&0\end{pmatrix}$$

$$\boldsymbol{M}^{25}_{(1,0)}=\begin{pmatrix}0&0&1/8&0\\0&1/2&1/8&0\\0&0&1/8&0\\0&0&1/8&0\end{pmatrix}\quad \boldsymbol{M}^{25}_{(1,1)}=\begin{pmatrix}1/2&0&0&1/8\\0&0&0&1/8\\0&0&0&1/8\\0&0&0&1/8\end{pmatrix}$$

证明 当 i=25 的情况，上述隐 Markov 模型中转移概率计算如下：

$$\Pr\{([O_{1,1}]_{25},[O_{2,3}]_{25})=(w_1,w_3),([c_1]_{26},[c_3]_{26})=(v_1,v_3)\mid([c_1]_{25},[c_3]_{25})=(u_1,u_3),L'\}=$$

$$\frac{\left|\left\{(a,b,s_1)\in\{0,1\}^3\mid w_1=s_1\oplus b\oplus a\oplus u_1,w_3=s_1\oplus b\oplus a\oplus u_3,v_1=\mathrm{maj}(s_1\oplus b,a,u_1),v_3=\mathrm{maj}(s_1\oplus a,b,u_3)\right\}\right|}{8}=$$

$$\frac{\left|\left\{(a,b,s_1')\in\{0,1\}^3\mid w_1=s_1'\oplus u_1,w_3=s_1'\oplus u_3,v_1=\mathrm{maj}(s_1'\oplus a,a,u_1),v_3=\mathrm{maj}(s_1'\oplus b,b,u_3)\right\}\right|}{8}=$$

$$\frac{\left|\left\{(a,b,s_1')\in\{0,1\}^3\mid w_1=s_1'\oplus u_1,w_3=s_1'\oplus u_3,v_1=\mathrm{IF}(s_1',a,u_1),v_3=\mathrm{IF}(s_1',b,u_3)\right\}\right|}{8}=$$

$$\begin{cases}1/2 & \text{if } (u_1,u_3)=(v_1,v_3)=(\overline{w}_1,\overline{w}_3)\\1/8 & \text{if } (u_1,u_3)=(w_1,w_3)\\0 & \text{otherwise}\end{cases}$$

再根据转移矩阵的定义即可得定理结论。

于是，根据隐 Markov 模型的前向算法可以给出概率 $\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L'\}$的如下计算公式：

$$\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L'\}=$$

$$(1,1,1,1)\boldsymbol{M}^{31}_{([o_1]_{31},[o_3]_{31})}\cdots\boldsymbol{M}^{0}_{([o_1]_0,[o_3]_0)}(1,0,0,0)^{\mathrm{T}}\qquad(1)$$

5 区分器的设计与分析

前一章中给出了概率 $\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L'\}$的计算公式。文献[3]中给出了概率 $\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L\}$的如下计算公式：

$$\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L\}=$$

$$(1,1,1,1)\boldsymbol{M}_{([o_1]_{31},[o_3]_{31})}\cdots\boldsymbol{M}_{([o_1]_0,[o_3]_0)}(1,0,0,0)^{\mathrm{T}}\qquad(2)$$

其中 $\boldsymbol{M}_y=\boldsymbol{M}^{25}_y$，$y\in F_2^2$。本章中按照文献[7]的方法，利用上述概率计算公式，构造出一个有效的区分器。

考虑一个信源按照某种分布 D 产生了 n 个取值于字符集 Z 的独立同分布的随机变量序列 Z^n，D 只可能取值是 D_1 或 D_0。对任意事件 X，记 $\Pr_{D_j}\{X\}=\Pr\{X\mid D=D_j\}$。一个区分器 A 是定义在字符集 Z^n 上的取值为 0 或 1 的函数，其效率由如下区分优势度量

$$\mathrm{Adv}(A)=\sum_{z^n\in Z^n}[\Pr_{D_1}\{A(z^n)=1\}-\Pr_{D_0}\{A(z^n)=1\}]$$

文献[7]指出“最优区”分器为

$$A_{\mathrm{opt}}(z^n)=\begin{cases}1 & \text{if } \mathrm{LLR}(z^n)>0\\0 & \text{otherwise}\end{cases}$$

其中 $\mathrm{LLR}(z^n)=\log\left(\dfrac{\Pr_{D_1}\{Z^n=z^n\}}{\Pr_{D_0}\{Z^n=z^n\}}\right)$。若分布 D_1 和 D_0 很接近的时候，即对任意的 $z\in Z$，$\varepsilon_z=\Pr_{D_1}\{Z=z\}-\Pr_{D_0}\{Z=z\}<<\Pr_{D_0}\{Z=z\}$时，可以得到

$$\mathrm{Adv}(A_{\mathrm{opt}})=\sum_{z^n\in Z^n}[\Pr_{D_1}\{A(z^n)=1\}-\Pr_{D_0}\{A(z^n)=1\}]\approx$$

$$1-2\Phi\left(-\frac{\sqrt{n\beta}}{2}\right)$$

其中 $\beta=\sum_{z\in Z}\dfrac{\varepsilon_z^2}{P_0(z)}$。

按照上述方法构造相应的最优区分器以区分 Py 的输出序列和真随机的序列。即区分取值为 $Z=F_2^{64}$ 上的分布 $P_1(z)=\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L\}\Pr(L)+\Pr\{(O_{1,1},O_{2,3})=(o_1,o_3)\mid L'\}\Pr(L')+P_0(z)\Pr(L^c)$和 $Z=F_2^{64}$ 上的均匀分布 $P_0(z)$。

为了求得区分优势和相应的所需密钥流长度，计算 β 如下：

$$\beta=\sum_{z\in Z}\frac{(P_1(z)-P_0(z))^2}{P_0(z)}=|Z|\sum_{z\in Z}\left(P_1(z)-\frac{1}{|Z|}\right)^2=$$

$$|Z|\sum_{z\in Z}\begin{pmatrix}\Pr\{(O_{1,1},O_{2,3})=z\mid L\}\Pr(L)+\\\Pr\{(O_{1,1},O_{2,3})=z\mid L'\}\Pr(L')+\\P_0(z)\Pr((L\cup L')^c)-\dfrac{1}{|Z|}\end{pmatrix}^2=$$

$$|Z|\Pr(L)^2\sum_{z\in Z}\begin{pmatrix}\Pr\{(O_{1,1},O_{2,3})=z\mid L\}+\\\Pr\{(O_{1,1},O_{2,3})=z\mid L'\}-\dfrac{2}{|Z|}\end{pmatrix}^2$$

鉴于 Z 中的元素个数为 2^{64}，即使能够有效的计算两个条件概率，直接累加以计算 β 的值是不合算的。定义如下函数族：

$$f_k(x)=\sum_{\substack{y_1\in y\\0\leqslant k\leqslant 31}}\left((1,1,1,1,1,1,1,1)\begin{pmatrix}\boldsymbol{M}_{y_0}&0\\0&\boldsymbol{M}^{31}_{y_0}\end{pmatrix}\begin{pmatrix}\boldsymbol{M}_{y_1}&0\\0&\boldsymbol{M}^{30}_{y_1}\end{pmatrix}\cdots\begin{pmatrix}\boldsymbol{M}_{y_{k-1}}&0\\0&\boldsymbol{M}^{30-(k-1)}_{y_{k-1}}\end{pmatrix}x-\frac{2}{|Z|}\right)^2$$

其中 k=0,1,…,32。则根据条件概率计算公式(1)、(2)可知

$$\beta=|Z|\Pr(L)^2 f_{32}((1,0,0,0,1,0,0,0)^{\mathrm{T}})$$

函数族 $f_k(x)$的值可按如下方法递归计算：

$$f_0(x)=\left((1,1,1,1,1,1,1,1)x-\frac{2}{|Z|}\right)^2=$$

$$\begin{pmatrix}x\\-\dfrac{2}{|Z|}\end{pmatrix}^{\mathrm{T}}\boldsymbol{A}_0\begin{pmatrix}x\\-\dfrac{2}{|Z|}\end{pmatrix}$$

其中 $\boldsymbol{A}_0$ 为 q 阶全 1 方阵。当 $0\leqslant k\leqslant 31$ 时，

$$f_{k+1}(x)=\sum_{y_k\in y}f_k\left(\begin{pmatrix}\boldsymbol{M}_{y_k}&0\\0&\boldsymbol{M}^{31-k}_{y_k}\end{pmatrix}x\right)=$$

$$\sum_{y_k\in y}\left(\begin{pmatrix}\boldsymbol{M}_{y_k} & 0\\ 0 & \boldsymbol{M}_{y_k}^{31-k}\end{pmatrix}\boldsymbol{x}\right)^{\mathrm{T}}\boldsymbol{A}_k\left(\begin{pmatrix}\boldsymbol{M}_{y_k} & 0\\ 0 & \boldsymbol{M}_{y_k}^{31-k}\end{pmatrix}\boldsymbol{x}\right)=\begin{pmatrix}x\\ -\frac{2}{|Z|}\end{pmatrix}^{\mathrm{T}}$$

$$\left(\sum_{y_k\in y}\begin{pmatrix}\begin{pmatrix}\boldsymbol{M}_{y_k} & 0\\ 0 & \boldsymbol{M}_{y_k}^{31-k}\end{pmatrix} & 0\\ 0 & 1\end{pmatrix}^{\mathrm{T}}\boldsymbol{A}_k\begin{pmatrix}\begin{pmatrix}\boldsymbol{M}_{y_k} & 0\\ 0 & \boldsymbol{M}_{y_k}^{31-k}\end{pmatrix} & 0\\ 0 & 1\end{pmatrix}\right)\begin{pmatrix}x\\ -\frac{2}{|Z|}\end{pmatrix}=$$

$$\begin{pmatrix}x\\ -\frac{2}{|Z|}\end{pmatrix}^{\mathrm{T}}\boldsymbol{A}_{k+1}\begin{pmatrix}x\\ -\frac{2}{|Z|}\end{pmatrix}$$

其中：

$$\boldsymbol{A}_{k+1}=\sum_{y_k\in y}\begin{pmatrix}\begin{pmatrix}\boldsymbol{M}_{y_k} & 0\\ 0 & \boldsymbol{M}_{y_k}^{31-k}\end{pmatrix} & 0\\ 0 & 1\end{pmatrix}^{\mathrm{T}}\boldsymbol{A}_k\begin{pmatrix}\begin{pmatrix}\boldsymbol{M}_{y_k} & 0\\ 0 & \boldsymbol{M}_{y_k}^{31-k}\end{pmatrix} & 0\\ 0 & 1\end{pmatrix}$$

利用上式可以有效地递归计算 $\boldsymbol{A}_{32}$，从而可以计算得 $\beta\approx 191\,203\Pr(L)^2$。因此，在区分效果和文献[2]等同的情况下，所需的密钥流长度只需约为文献[2]的 1/191 203，约为文献[3]的 60 552/191 203≈1/3.2。

值得注意的是，Py 的设计目标之一是使得没有区分器能在密钥长度低于 2^{64} 字节时以较穷搜索更快的方法对输出密钥流实施区分攻击。按照此方法，在密钥流长度为 2^{64} 字节时，所得的区分优势约为 0.064。

6　结束语

本文讨论了对最近提出并入选 ECRYPT 第二轮选拔的一个候选算法 Py 的区分攻击。首先利用隐 Markov 模型给出了有效计算在事件 L' 发生的条件下输出密钥流中两个字 $O_{1,1}$、$O_{2,3}$ 的联合分布的计算公式，由此构造了一个区分器。在区分效果和目前最有效的区分攻击的效果相同的情况下，所需密钥流长度缩短为原来的 1/3.2。即使在密钥流长度限制为 2^{64} 字节，仍能以约为 0.064 的优势区分密钥流和真随机的序列。

(收稿日期：2006 年 9 月)

参考文献：

[1] Biham E，Seberry J.Py(Roo)：a fast and secure stream cipher using rolling arrays Report 2005/023[R].eSTREAM，ECRYPT Stream Cipher Project，2005.

[2] Gautham Sekar，Souradyuti Paul，Bart Preneel.Distinguishing attacks on the stream cipher Py Report 2005/081[R].eSTREAM，ECRYPT Stream Cipher Project，2005.

[3] Crowley P.Improved cryptanalysis of Py[C]//Workshop Record of SASC 2006-Stream Ciphers Revisited.Belgium：Leuven，2006：52-60.

[4] Rabiner L R.A tutorial on hidden Markov models and selected applications in speech recognition[J].Proceedings of the IEEE，1990，7(2)：267-296.

[5] Yariv Ephraim，Neri Merhav.Hidden Markov processes[J].IEEE Trans Infor Theory，2002，48(6)：1518-1569.

[6] Helger Lipmaa，Shiho Moriai.Efficient algorithms for computing differential properties of addition[C]//LNCS 2335：Fast Software Encryption 2001.Berlin：Springer-Verlag，2001：336-350.

[7] Thomas Baigneres，Pascal Junod，Serge Vaudenay.How far can we go beyond linear cryptanalysis?[C]//LNCS 3329：Advances in Cryptography-ASIACRYPT 2004.Berlin：Springer-Verlag，2004：432-450.

(上接 115 页)

从结果可以看出，由于需求的随机性，每周期的生产量在均值附近波动；随着变质率不断增大，库存损耗的成本增加，当变质率大到一定程度(本例中为大于 0.03)时，库存损耗成本已经大于生产准备成本，因此计划表现为在每个周期都安排生产而不持有库存。

5　结论

本文针对能力约束的生产计划问题，在需求随机和库存产品有保质期的情况下给出了生产计划优化模型，并给出了由随机模拟、遗传算法和启发式算法构成的混合求解算法。与确定型模型相比，随机模型更符合实际情况。通过对需求符合正态分布的数值实例计算，该算法可以对有效地求出最优解，且当变质率增大时，成本的变化符合实际情况。通过修改修改随机模拟算法，本模型可适用于需求为其他概率分布的情况。

(收稿日期：2006 年 9 月)

参考文献：

[1] Wee Huiming，Shum Yusu.Model development for deteriorating inventory in material requirement planning systems[J].Computers & Industrial Engineering，1999，36(1)：219-225.

[2] Yang Pochung，Wee Huiming.An integrated multi-lot-size production inventory model for deteriorating item[J].Computers & Operations Research，2003，30(5)：671-682.

[3] Wee Huiming，Law S T.Replenishment and pricing policy for deteriorating items taking into account the time-value of money[J].Intertional Journal of Production Economics，2001，71(1)：213-220.

[4] Yao Ming-jong，Huang Jian-xiong.Solving the economic lot scheduling problem with deteriorating items using genetic algorithms[J].Journal of Food Engineering，2005，70(3)：309-322.

[5] Castro E L，Tabucanon M T，Nagarur N N.A production order quantity model with stochastic demand for a chocolate milk manufacturer[J].Int J Production Economics，1997，49(1)：145-156.

[6] Sox C R.Dynamic lot sizing with random demand and non-stationary costs[J].Operations Research Leatters，1997，20(4)：155-164.

[7] Zhou Jian，Liu Bao-ding.New stochastic models for capacitated location-allocation problem[J].Computers & Industrial Engineering，2003，45(1)：111-125.

[8] Dixon P S，Poh C L.Heuristic procedures for multi-item inventory planning with limited storage[J].IIE Transactions，1990，22(2)：112-123.

[9] Karni R，Roll Y.A heuristic algorithm for the multi-item lot-sizing problem with capacity constraints[J].IIE Transactions，1982，14(4)：249-256.