“停走”型钟控序列概率模型信息论分析 [1]

刘传东　　吕述望　　范修斌

(中国科技大学研究生院信息安全国家重点实验室　北京　100039)

摘　要　给出了“停走”型钟控序列概率模型的信息论分析，得到了控制序列与输出序列之间互信息熵的简单计算公式，给出了输入与输出序列之间互信息熵的一个下界.

关键词　“停走”型钟控序列，信息论，互信息熵

中图号　TN911

1 引　言

由于钟控序列具有良好的密码学性质，因此它一度成为密码学研究的热点之一。关于钟控序列的研究文献一般可分为两类，一类为密码学基本性质的研究，主要包括其周期性、线性复杂度、平衡性等密码学参数的研究文献 [1−3]；另一类是对密码学攻击方面的研究文献 [4,5]．最近，文献 [6] 给出了 (1, 3) 型钟控序列的概率模型，得到了控制序列与输出序列互信息为零的结论。文献 [7] 给出了“停走”型钟控序列的概率模型，得到了此类生成器输出序列服从大数定律的结果. 本文利用信息论的原理对“停走”型钟控模型进行了熵漏分析，给出了控制序列与输出序列互信息熵的简单计算公式，证明了输入输出互信息是输出序列长度的严格单调增函数，得到了“停走”型钟控模型输入与输出互信息熵的一个下界，同时也证明了输出序列以其 Markov 性不同于其它钟控模型序列的结论. 以上结果不仅说明了信息论原理是研究钟控序列逻辑的重要工具和方法，同时对设计和分析钟控密钥流生成器也有一定的参考价值.

2 “停走”型钟控模型控制与输出互信息

定义 1[7]　设 $\tilde{a}=\{a_0,a_1,a_2,\cdots\}$ 和 $\tilde{b}=\{b_0,b_1,b_2,\cdots\}$ 都是概率空间 (Ω,F,p) 上的独立均匀分布的 0,1 随机变量序列，且 $\tilde{a}$ 与 $\tilde{b}$ 相互独立，记 $L(i)=\sum_{l<i}b_l(L(0)=0)$, $c_i=a_{L(i)}$, $i=0,1,2,\cdots$，则称密码学系统 $(\tilde{a},\tilde{b},\tilde{c})$ 为“停走”型钟控序列概率模型，其中，$\tilde{a}=\{a_0,a_1,a_2,\cdots\}$ 为钟控输入序列，$\tilde{b}=\{b_0,b_1,b_2,\cdots\}$ 为控制序列，$\tilde{c}=\{c_0,c_1,c_2,\cdots\}$ 为钟控输出序列.

为方便起见，$\{a_0=x_0,\cdots,a_n=x_n\}$, $\{c_0=y_0,\cdots,c_n=y_n\}$, $\{b_0=l_0,\cdots,b_n=l_n\}$ 分别简记为 $\tilde{a}_n=\tilde{x}_n$, $\tilde{c}_n=\tilde{y}_n$, $\tilde{b}_n=\tilde{l}_n$，其中 $x_i,y_i,l_i\in\{0,1\}$, $i=0,1,\cdots$, $\#\{\ \}$ 表示集合的势.

引理 1　任给 $\tilde{y}_n\in F_2^{n+1}$, $\tilde{l}_{n-1}\in F_2^n(n\geq 1)$, $p\{\tilde{c}_n=\tilde{y}_n,\tilde{b}_{n-1}=\tilde{l}_{n-1}\}\neq 0\Leftrightarrow$ 若 $y_j\neq y_{j+1}(0\leq j<n)$，则 $l_j=1$，此时若设 $\sum_{j=1}^{n}(y_{j-1}\oplus y_j)=i$, $\sum_{j=0}^{n-1}l_j=i+t(0\leq i\leq n,0\leq t\leq n-i)$，则 $p\{\tilde{c}_n=\tilde{y}_n,\tilde{b}_{n-1}=\tilde{l}_{n-1}\}=1/2^{n+i+t+1}$．

证明　设 $y_0=\cdots=y_{j_1}$, $y_{j_1+1}=\cdots=y_{j_2},\cdots,y_{j_i+1}=\cdots=y_n$, $y_{j_k}\neq y_{j_k+1}$, $k=1,2,\cdots,i$．

$\Rightarrow$ 若存在 $1\leq k\leq i$，使 $y_{j_k}\neq y_{j_k+1}$, $l_{j_k}=0$，由 $a_{L(j_k)}=a_{L(j_k+1)}$ 易知 $p\{\tilde{c}_n=\tilde{y}_n,\tilde{b}_{n-1}=\tilde{l}_{n-1}\}=p\{c_0=y_0,c_1=y_1,\cdots,c_n=y_n,\tilde{b}_{n-1}=\tilde{l}_{n-1}\}=p\{a_{L(0)}=y_0,\cdots,a_{L(j_1)}=y_{j_1},a_{L(j_1+1)}=y_{j_1+1},\cdots,a_{L(j_k)}=y_{j_k},a_{L(j_k+1)}=y_{j_k+1},\cdots,a_{L(j_i)}=y_{j_i},a_{L(j_i+1)}=y_{j_i+1},\cdots,a_{L(n)}=y_{j_i+1},\tilde{b}_{n-1}=\tilde{l}_{n-1}\}=0$．

[1] 2001-11-15 收到，2002-06-15 改回

$\Leftarrow$ 若 $\sum_{j=0}^{n-1} l_j = i+t$，且 $l_{j_1} = l_{j_2} = \cdots = l_{j_i} = 1$，由定义 1 可设 $L(0) = \cdots = L(t_0) < L(t_0+1) = \cdots = L(t_1) < \cdots < L(t_{i+t-1}+1) = \cdots = L(n)$，由 $y_0 = y_1 = \cdots = y_{t_0}$，$y_{t_0+1} = y_{t_0+2} = \cdots = y_{t_1}, \cdots, y_{t_{i+t-1}+1} = y_{t_{i+t-1}+2} = \cdots = y_n$、知:

$$\begin{aligned}
&p\{c_0 = y_0, c_1 = y_1, \cdots, c_n = y_n, \tilde{b}_{n-1} = \tilde{l}_{n-1}\} \\
&\quad = p\{a_0 = y_0, \cdots, a_0 = y_{t_0}, \cdots, a_{i+1} = y_{t_{i+t-1}+1}, \cdots, a_{i+t} = y_n, \tilde{b}_{n-1} = \tilde{l}_{n-1}\} \\
&\quad = p\{a_0 = y_{t_0}, a_1 = y_{t_1}, \cdots, a_{i+t-1} = y_{t_{i+t-1}}, a_{i+t} = y_n, \tilde{b}_{n-1} = \tilde{l}_{n-1}\} \\
&\quad = p\{a_0 = y_{t_0}, a_1 = y_{t_1}, \cdots, a_{i+t-1} = y_{t_{i+t-1}}, a_{i+t} = y_n\} \cdot p\{\tilde{b}_{n-1} = \tilde{l}_{n-1}\} \\
&\quad = 1/2^{n+i+t+1}
\end{aligned}$$

证毕

引理 2 输出 $\tilde{c} = \{c_0, c_1, c_2 \cdots\}$ 是概率空间 (Ω, F, p) 上均匀分布的 0,1 随机变量序列，且 $p\{\tilde{c}_n = \tilde{y}_n\} = 3^{n-i}/2^{2n+1}$，其中 $i = \sum_{l=1}^{n}(y_{l-1} \oplus y_l)$。

证明 由定义 1 易知，当 $n=0$ 时，$p\{c_0 = y_0\} = p\{a_0 = y_0\} = 1/2$。且当 $n \geq 1$ 时，a_j 与 $\sum_{i<n} b_i$ 相互独立，故 $p\{c_n = y_n\} = p\{a_{\sum_{i<n} b_i} = y_n\} = \sum_{j=0}^{n} p\{a_j = y_n, \sum_{i<n} b_i = j\}$ $= \sum_{j=0}^{n} p\{a_j = y_n\} p\left\{\sum_{i<n} b_i = j\right\} = \sum_{j=0}^{n}(1/2)(C_n^j/2^n) = 1/2$。

若 $\sum_{l=1}^{n}(y_{l-1} \oplus y_l) = i$，令 $y_{j_k} \neq y_{j_k+1}$, $k = 1, 2, \cdots, i$，由引理 1 得

$$\begin{aligned}
p\{\tilde{c}_n = \tilde{y}_n\} &= \sum_{\tilde{l}_{n-1} \in F_2^n} p\{c_0 = y_0, c_1 = y_1, \cdots, c_n = y_n, \tilde{b}_{n-1} = \tilde{l}_{n-1}\} \\
&= \sum_{k=0}^{n-i}\left(\#\{\tilde{l}_{n-1} | \tilde{l}_{n-1} \in F_2^n, l_{j_1} = l_{j_2} = \cdots = l_{j_i} = 1, \sum_{t=0}^{n-1} l_t = i+k\}\right) \cdot \frac{1}{2^{n+i+k+1}} \\
&= \sum_{k=0}^{n-i} \frac{C_{n-i}^k}{2^{n+i+k+1}} = \frac{1}{2^{n+i+1}}\left(1 + \frac{1}{2}\right)^{n-i} = \frac{3^{n-i}}{2^{2n+1}}
\end{aligned}$$

证毕

引理 3 对一切 $n \geq 0, k \geq 1, p\{c_{n+k} = c_n\} = \frac{2^k+1}{2^{k+1}} \stackrel{k\to\infty}{\longrightarrow} 1/2$。

证明 由 $\tilde{a}, \tilde{b}$ 的独立性知:

$$\begin{aligned}
p\{c_{n+k} = c_n\} &= \sum_{i=0}^{n}\sum_{j=0}^{k} p\left\{c_{n+k} = c_n, \sum_{l<n} b_l = i, \sum_{n \leq l < n+k} b_l = j\right\} \\
&= \sum_{i=0}^{n}\sum_{j=0}^{k} p\left\{a_{i+j} = a_i, \sum_{l<n} b_l = i, \sum_{n \leq l < n+k} b_l = j\right\} \\
&= \sum_{i=0}^{n}\sum_{j=0}^{k} p\{a_{i+j} = a_i\} \cdot p\left\{\sum_{l<n} b_l = i\right\} \cdot p\left\{\sum_{n \leq l < n+k} b_l = j\right\} \\
&= \sum_{i=0}^{n}\sum_{j=0}^{k} \frac{C_n^i}{2^n} \cdot \frac{C_k^j}{2^k} \cdot p\{a_{i+j} = a_i\} + \sum_{i=0}^{n} \frac{C_n^i}{2^n} \cdot \frac{1}{2^k} \cdot p\{a_i = a_i\} \\
&= \left(1 - \frac{1}{2^k}\right) \cdot \frac{1}{2} + \frac{1}{2^k} = \frac{2^k+1}{2^{k+1}} \stackrel{k\to\infty}{\longrightarrow} 1/2
\end{aligned}$$

证毕

文献 [6] 证明了 (1, 3) 型钟控模型控制序列与输出序列的互信息为零的结果，即通过输出序列得不到任何关于控制序列的信息。对于"停走"型钟控模型，控制序列与输出序列互信息如何？下面给出其分析结果。

定理 1　$H(\tilde{c}_n)=-\frac{3}{4}n\log_2 3+(2n+1)$，　$H(c_{n+1}|\tilde{c}_n)=2-\frac{3}{4}\log_2 3$.

证明　由 $\#\{\tilde{y}_n|\tilde{y}_n\in F_2^{n+1},\sum_{l=1}^{n}(y_{l-1}\oplus y_l)=i\}=2C_n^i$ 和引理 2 得：

$$
\begin{aligned}
H(\tilde{c}_n)&=-\sum_{\tilde{y}_n\in F_2^{n+1}}p\{\tilde{c}_n=\tilde{y}_n\}\log_2 p\{\tilde{c}_n=\tilde{y}_n\}\\
&=-\sum_{i=0}^{n}2C_n^i\frac{3^{n-i}}{2^{2n+1}}\log_2\frac{3^{n-i}}{2^{2n+1}}\\
&=-\sum_{i=0}^{n}C_n^i\frac{3^{n-i}}{2^{2n}}(n-i)\log_2 3+(2n+1)\sum_{i=0}^{n}C_n^i\frac{3^{n-i}}{2^{2n}}\\
&=-\frac{\log_2 3}{4^n}\sum_{i=0}^{n}iC_n^i\cdot 3^i+(2n+1)=-\frac{3}{4}n\log_2 3+(2n+1)
\end{aligned}
$$

由引理 2 和引理 3： $p\{c_{n+1}=y_{n+1}|\tilde{c}_n=\tilde{y}_n\}=\dfrac{p\{\tilde{c}_{n+1}=\tilde{y}_{n+1}\}}{p\{\tilde{c}_n=\tilde{y}_n\}}=\begin{cases}3/4, & y_{n+1}=y_n\\ 1/4, & y_{n+1}\neq y_n\end{cases}$
$=p\{c_{n+1}=y_{n+1}|c_n=y_n\}$ ，所以

$$
\begin{aligned}
&H(c_{n+1}|\tilde{c}_n)\\
&=-\sum_{\tilde{y}_n\in F_2^{n+1}}\sum_{y_{n+1}\in\{0,1\}}p\{\tilde{c}_n=\tilde{y}_n\}p\{c_{n+1}=y_{n+1}|\tilde{c}_n=\tilde{y}_n\}\log_2 p\{c_{n+1}=y_{n+1}|\tilde{c}_n=\tilde{y}_n\}\\
&=-\sum_{i=0}^{n}2C_n^i\frac{3^{n-i}}{2^{2n+1}}\left[\frac{3}{4}\log_2\frac{3}{4}+\frac{1}{4}\log_2\frac{1}{4}\right]=-\frac{3}{4}\log_2\frac{3}{4}-\frac{1}{4}\log_2\frac{1}{4}=2-\frac{3}{4}\log_2 3
\end{aligned}
$$

证毕

从此定理的证明过程我们易知， $\tilde{c}=\{c_0,c_1,\cdots\}$ 构成齐次马尔可夫链.

定理 2　$I(\tilde{b}_{n-1};\tilde{c}_n)=\frac{3}{2}n-\frac{3}{4}n\log_2 3\ \ (n\geq 1)$.

证明　令 $B_i=\{\tilde{y}_n|\tilde{y}_n\in F_2^{n+1},\sum_{l=1}^{n}(y_{l-1}\oplus y_l)=i\}$, $i=0,1,\cdots,n$ ，由引理 1:
$\#\left\{\tilde{l}_{n-1}|\tilde{l}_{n-1}\in F_2^n,\tilde{y}_n\in B_i,\ \ p\{\tilde{c}_n=\tilde{y}_n,\tilde{b}_{n-1}=\tilde{l}_{n-1}\}=1/2^{n+i+j+1}\right\}=C_{n-i}^j$, $j=0,1,\cdots,n-i$ ；而 $\#B_i=2C_n^i$ ，所以

$$
\begin{aligned}
H(\tilde{b}_{n-1}\tilde{c}_n)&=-\sum_{\tilde{l}_{n-1}\in F_2^n}\sum_{\tilde{y}_n\in F_2^{n+1}}p\{\tilde{b}_{n-1}=\tilde{l}_{n-1},\tilde{c}_n=\tilde{y}_n\}\log_2 p\{\tilde{b}_{n-1}=\tilde{l}_{n-1},\tilde{c}_n=\tilde{y}_n\}\\
&=-\sum_{i=0}^{n}2C_n^i\sum_{j=0}^{n-i}C_{n-i}^j\cdot\frac{1}{2^{n+i+j+1}}\log_2\frac{1}{2^{n+i+j+1}}\\
&=\frac{1}{2^n}\sum_{i=0}^{n}\frac{C_n^i}{2^i}\sum_{j=0}^{n-i}\frac{C_{n-i}^j}{2^j}[(n+i+1)+j]\\
&=\frac{1}{2^n}\sum_{i=0}^{n}\frac{C_n^i}{2^i}\left[(n+i+1)\frac{3^{n-i}}{2^{n-i}}+\frac{n-i}{2}\cdot\frac{3^{n-i-1}}{2^{n-i-1}}\right]=\frac{3^{n-1}}{2^{2n}}\sum_{i=0}^{n}\frac{C_n^i}{3^i}[(4n+3)+2i]\\
&=\frac{3^{n-1}}{2^{2n}}\left[(4n+3)\cdot\frac{4^n}{3^n}+2\cdot\frac{n}{3}\cdot\frac{4^{n-1}}{3^{n-1}}\right]=\frac{3n}{2}+1
\end{aligned}
$$

由定理 1 得 $I(\tilde{b}_{n-1};\tilde{c}_n)=H(\tilde{b}_{n-1})+H(\tilde{c}_n)-H(\tilde{b}_{n-1}\tilde{c}_n)=n+\left[-\frac{3}{4}n\log_2 3+(2n+1)\right]-\left(\frac{3n}{2}+1\right)$ $=\frac{3}{2}n-\frac{3}{4}n\log_2 3$.

由此可得：$I(\tilde{b}_n;\tilde{c}_{n+1})-I(\tilde{b}_{n-1};\tilde{c}_n)=\frac{3}{2}-\frac{3}{4}\log_2 3$. 证毕

3 “停走”型钟控序列输入与输出互信息

引理 4 若 $m\geq n\geq 1$ ，则 $p\{c_n=y_n|\tilde{a}_m=\tilde{x}_m,\ \tilde{c}_{n-1}=\tilde{y}_{n-1}\}=p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n,\ \tilde{c}_{n-1}=\tilde{y}_{n-1}\}$.

证明 由序列 $\tilde{a}=\{a_0,a_1,a_2,\cdots\}$ 的独立性与定义 1 得

$$p\{c_n=y_n|\tilde{a}_m=\tilde{x}_m,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}=\frac{p\{\tilde{a}_m=\tilde{x}_m,\tilde{c}_n=\tilde{y}_n\}}{p\{\tilde{a}_m=\tilde{x}_m,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}}$$

$$=\frac{2^{-(m-n)}p\{\tilde{a}_m=\tilde{x}_m,\tilde{c}_n=\tilde{y}_n|a_{n+1}=x_{n+1},a_{n+2}=x_{n+2},\cdots,a_m=x_m\}}{2^{-(m-n)}p\{\tilde{a}_m=\tilde{x}_m,\tilde{c}_{n-1}=\tilde{y}_{n-1}|a_{n+1}=x_{n+1},a_{n+2}=x_{n+2},\cdots,a_m=x_m\}}$$

$$=\frac{p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}}{p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}}=p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}$$ 证毕

引理 5 $p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}=\frac{1}{2^{n+1}}p\{c_0=y_0|a_0=x_0\}p\{c_1=y_1|\tilde{a}_1=\tilde{x}_1,c_0=y_0\}\cdots$ $p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}$.

证明 此引理利用概率论的乘法定理与引理 4 易得。

引理 6[8] 对输入随机变量 X 和输出随机变量 Y ，互信息量 $I(X;Y)\geq 0$ ，当且仅当 X 与 Y 统计独立时，才有 $I(X;Y)=0$ 。

定理 3 $I(\tilde{a}_n;\tilde{c}_n)<I(\tilde{a}_{n+1};\tilde{c}_{n+1})$ ，当 $n>0$ 时，$I(\tilde{a}_n;\tilde{c}_n)>0$ 。

证明

$$\begin{aligned}
I(\tilde{a}_n;\tilde{c}_n)&=H(\tilde{a}_n)+H(\tilde{c}_n)-H(\tilde{a}_n\tilde{c}_n)\\
&=H(\tilde{a}_n)+H(\tilde{c}_n)+\sum_{\tilde{x}_n,\tilde{y}_n\in F_2^{n+1}}p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}\log_2 p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}\\
&=H(\tilde{a}_n)+H(\tilde{c}_n)+\sum_{\tilde{x}_n,\tilde{y}_n\in F_2^{n+1}}p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}\log_2[\frac{1}{2^{n+1}}p\{c_0=y_0|a_0=x_0\}\\
&\quad\times p\{c_1=y_1|\tilde{a}_1=\tilde{x}_1,c_0=y_0\}\cdot\cdots\cdot p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}]\\
&=H(\tilde{c}_n)+\sum_{\tilde{x}_n,\tilde{y}_n\in F_2^{n+1}}p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}\log_2 p\{c_0=y_0|a_0=x_0\}\\
&\quad+\sum_{\tilde{x}_n,\tilde{y}_n\in F_2^{n+1}}p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}\log_2 p\{c_1=y_1|\tilde{a}_1=\tilde{x}_1,c_0=y_0\}+\cdots\\
&\quad+\sum_{\tilde{x}_n,\tilde{y}_n\in F_2^{n+1}}p\{\tilde{a}_n=\tilde{x}_n,\tilde{c}_n=\tilde{y}_n\}\log_2 p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n,\tilde{c}_{n-1}=\tilde{y}_{n-1}\}\\
&=H(\tilde{c}_n)-H(c_0|a_0)-H(c_1|a_0a_1c_0)-\cdots-H(c_n|a_0a_1\cdots a_nc_0c_1\cdots c_{n-1})\\
&=(H(c_0)-H(c_0|a_0))+(H(c_1|c_0)-H(c_1|a_0a_1c_0))+\cdots\\
&\quad+(H(c_n|c_0c_1\cdots c_{n-1})-H(c_n|a_0a_1\cdots a_nc_0c_1\cdots c_{n-1}))\\
&=I(a_0;c_0)+I(a_0a_1;c_1|c_0)+\cdots+I(a_0a_1\cdots a_n;c_n|c_0c_1\cdots c_{n-1})
\end{aligned}$$

由引理 6 和引理 2 、引理 3 可得定理结论.　　证毕

引理 7[9]　$\sum_{k=0}^{n}[C_n^k]^2=\frac{(2n)!}{(n!)^2}$.

引理 8[10]　$n!=n^ne^{-n}\sqrt{2n\pi}(1+O(1/n))$.

引理 9　$p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n\}=(1/2)(1+(-1)^{y_n}A(\tilde{x}_n))$,

其中 $A(\tilde{x}_n)=\frac{C_n^0(-1)^{x_0}+C_n^1(-1)^{x_1}+\cdots+C_n^n(-1)^{x_n}}{2^n}$.

证明

$$
\begin{aligned}
&p\{c_n=y_n|a_0=x_0,a_1=x_1,\cdots,a_n=x_n\}\\
&=2^{n+1}p\{c_n=y_n,a_0=x_0,a_1=x_1,\cdots,a_n=x_n\}\\
&=2^{n+1}\sum_{k=0}^{n}p\left\{a_k=y_n,a_0=x_0,a_1=x_1,\cdots,a_n=x_n,\sum_{l<n}b_l=k\right\}\\
&=2^{n+1}\sum_{k=0}^{n}p\left\{\sum_{l<n}b_l=k\right\}\cdot p\{a_k=y_n,a_0=x_0,a_1=x_1,\cdots,a_n=x_n\}\\
&=2\sum_{k=0}^{n}C_n^kp\{a_k=y_n,a_0=x_0,a_1=x_1,\cdots,a_n=x_n\}\\
&=\frac{1}{2^{n-1}}\sum_{k=0}^{n}C_n^kp\{a_k=x_k,a_k=y_n\}\\
&\quad\times\left[p\{a_k=x_k,a_k=y_n\}=\begin{cases}1/2, & (y_n=x_k)\\ 0, & (y_n\neq x_k)\end{cases}=(1/4)(1+(-1)^{y_n+x_k})\right]\\
&=\frac{1}{2^{n-1}}\sum_{k=0}^{n}C_n^k\frac{1}{4}(1+(-1)^{y_n+x_k})=\frac{1}{2}\left(1+(-1)^{y_n}\frac{1}{2^n}\sum_{k=0}^{n}C_n^k(-1)^{x_k}\right)\\
&=(1/2)(1+(-1)^{y_n}A(\tilde{x}_n))
\end{aligned}
$$

证毕

引理 10　$\sum_{\tilde{x}_n\in F_2^{n+1}}[A(\tilde{x}_n)]^2=\frac{2^{n+1}}{\sqrt{n\pi}}(1+O(1/n))$.

证明

$$
\begin{aligned}
&\sum_{\tilde{x}_n\in F_2^{n+1}}[A(\tilde{x}_n)]^2\ \underline{\underline{\text{引理 9}}}\ \frac{1}{2^{2n}}\sum_{\tilde{x}_n\in F_2^{n+1}}(C_n^0(-1)^{x_0}+C_n^1(-1)^{x_1}+\cdots+C_n^n(-1)^{x_n})^2\\
&=\frac{1}{2^{2n}}\cdot 2^{n+1}[(C_n^0)^2+(C_n^1)^2+\cdots+(C_n^n)^2]\ \underline{\underline{\text{引理 7}}}\ \frac{1}{2^{n-1}}\cdot\frac{(2n)!}{(n!)^2}\\
&\underline{\underline{\text{引理 8}}}\ \frac{1}{2^{n-1}}\cdot\frac{(2n)^{2n}e^{-2n}\sqrt{4n\pi}(1+O(1/n))}{(n^ne^{-n}\sqrt{2n\pi}(1+O(1/n)))^2}=\frac{2^{n+1}}{\sqrt{n\pi}}(1+O(1/n))
\end{aligned}
$$

证毕

引理 11[6]　$1-\frac{1}{\ln 2}+\frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{2^ii(i+1)}=0$.

定理 4　$I(\tilde{a}_n;c_n)\geq\frac{1}{2\sqrt{\pi}\ln 2}\frac{1}{\sqrt{n}}+O\left(\frac{1}{n^{1.5}}\right)$.

证明

$$
\begin{aligned}
I(\tilde{a}_n;c_n) &= H(c_n) - H(c_n|\tilde{a}_n) \\
&= 1 + \sum_{(\tilde{x}_n,y_n)\in F_2^{n+2}} p\{\tilde{a}_n=\tilde{x}_n\}p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n\}\log_2 p\{c_n=y_n|\tilde{a}_n=\tilde{x}_n\} \\
&\underline{\underline{\text{引理 9}}}\ 1 + \frac{1}{2^{n+1}} \sum_{(\tilde{x}_n,y_n)\in F_2^{n+2}} \left[1-\left(\frac{1}{2}-(-1)^{y_n}\frac{A(\tilde{x}_n)}{2}\right)\right] \log_2 \left[1-\left(\frac{1}{2}-(-1)^{y_n}\frac{A(\tilde{x}_n)}{2}\right)\right] \\
&= 1 - \frac{1}{2^{n+1}\ln 2} \sum_{(\tilde{x}_n,y_n)\in F_2^{n+2}} \left[1-\left(\frac{1}{2}-(-1)^{y_n}\frac{A(\tilde{x}_n)}{2}\right)\right] \sum_{i=1}^{\infty} \frac{(1/2-(-1)^{y_n}A(\tilde{x}_n)/2)^i}{i} \\
&= 1 - \frac{1}{2^{n+1}\ln 2} \sum_{(\tilde{x}_n,y_n)\in F_2^{n+2}} \left(\frac{1}{2}-(-1)^{y_n}\frac{A(\tilde{x}_n)}{2}\right) \\
&\quad + \frac{1}{2^{n+1}\ln 2} \sum_{(\tilde{x}_n,y_n)\in F_2^{n+2}} \sum_{i=1}^{\infty} \frac{1}{i(i+1)} \left(\frac{1}{2}-(-1)^{y_n}\frac{A(\tilde{x}_n)}{2}\right)^{i+1} \\
&= 1 - \frac{1}{\ln 2} + \frac{1}{2^{n+1}\ln 2} \sum_{\tilde{x}_n\in F_2^{n+1}} \sum_{i=1}^{\infty} \frac{1}{i(i+1)} \left[\left(\frac{1}{2}+\frac{A(\tilde{x}_n)}{2}\right)^{i+1} + \left(\frac{1}{2}-\frac{A(\tilde{x}_n)}{2}\right)^{i+1}\right] \\
&= 1 - \frac{1}{\ln 2} + \frac{1}{2^{n+1}\ln 2} \sum_{\tilde{x}_n\in F_2^{n+1}} \sum_{i=1}^{\infty} \frac{1}{2^i i(i+1)} [1 + C_{i+1}^2(A(\tilde{x}_n))^2 + C_{i+1}^4(A(\tilde{x}_n))^4 + \cdots] \\
&\underline{\underline{\text{引理 11}}}\ \frac{1}{2^{n+1}\ln 2} \sum_{\tilde{x}_n\in F_2^{n+1}} \sum_{i=1}^{\infty} \frac{1}{2^i i(i+1)} [C_{i+1}^2(A(\tilde{x}_n))^2 + C_{i+1}^4(A(\tilde{x}_n))^4 + \cdots] \\
&\geq \frac{1}{2^{n+1}\ln 2} \sum_{\tilde{x}_n\in F_2^{n+1}} \sum_{i=1}^{\infty} \frac{1}{2^i i(i+1)} C_{i+1}^2(A(\tilde{x}_n))^2 \\
&= \frac{1}{2^{n+1}\ln 2} \sum_{i=1}^{\infty} \frac{1}{2^{i+1}} \sum_{\tilde{x}_n\in F_2^{n+1}} (A(\tilde{x}_n))^2\ \underline{\underline{\text{引理 10}}}\ \frac{1}{2\ln 2\sqrt{n\pi}} + O\left(\frac{1}{n^{1.5}}\right)
\end{aligned}
$$

证毕

4 结束语

本文用信息论的方法讨论了“停走”型钟控模型，给出了控制序列与输出序列的互信息结果，同时对输入输出互信息作了一定的分析，从分析中可以看到“停走”型钟控密钥流生成器不但能从输出序列中获得控制序列、输入序列的部分信息，而且输出序列本身也存在信息泄露现象，这对使用“停走”型密钥生成器的密码体制构成了不同程度的威胁，在以后的工作中，将给出一般钟控序列的信息论分析结果。

参 考 文 献

[1] D. Gollmann, W. G. Chambers, Clock-controlled shift registers: A review, IEEE J. on Selected Areas in Communications, 1989, 7(4), 525–533.

[2] 丁存生，肖国镇，流密码学及其应用，北京，国防工业出版社， 1994, 189–190.

[3] 杨义先，两类钟控序列的研究，第三次全国密码学会议会议录，西安，西安电子科技大学情报资料室出版， 1988, 91–97.

[4] 郝长亮，一类自钟控序列的分析与破译，第三次全国密码学会议会议录，西安，西安电子科技大学情报资料室出版, 1988, 112–117.

[5] J. Golic, Towards fast correlation attacks on irregularly clocked shift registers, Advances in Cryptology-EUROCRTYPT'95(LNCS921), Berlin, Springer-Verlag, 1995, 248–262.

[6] Fan Xiubin, Li Shiqu, Analysis of the mutual information between input and output of a class of clock-controlled sequences, Journal of Electronics(China), 2000, 17(2), 185–192.

[7] 黄晓英，李世取，关于“停走”生成器输出序列的大数定律，信息工程大学学报， 2000, 6(1), 9–11.

[8] 姜　丹，钱玉美，信息理论与编码，合肥，中国科学技术大学出版社， 1992, 152–154.

[9] 数学手册，北京，人民教育出版社， 1979, 26.

[10] 潘承洞，于秀源，阶的估计，济南，山东科技出版社， 1983, 33, 136.

INFORMATION-THEORETIC ANALYSIS OF PROBABILITY MODEL FOR THE STOP-AND-GO CLOCK-CONTROLLED SEQUENCES

Liu Chuandong　　Lü Shuwang　　Fan Xiubin

(*State Key Lab. of Info. Security, Univ. of Sci. and Tech. of China, Beijing* 100039, *China*)

Abstract　An information-theoretic analysis of probability model for the stop-and-go sequences is proposed, the result of mutual information entropy between control sequence and output sequence is obtained and the lower bound of mutual information entropy between input sequence and output sequence is given.

Key words　The stop-and-go clock-controlled sequence, Information theory, Mutual information entropy

刘传东：　男， 1966 年生，硕士生，主要从事密码学和信息安全方面的研究.

吕述望：　男， 1941 年生，教授，博士生导师，国家 973 项目 (G1999035808) 负责人，主要从事密码理论的研究和芯片集成.

范修斌：　男， 1966 年生，副教授，博士后，主要从事概率论在信息安全中的应用.