密码学控选逻辑控制序列与输出序列的互信息 [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 给出了密码学控选逻辑的概率模型，得到了密码学控选逻辑控制序列与输出序列互信息为零的充要条件，同时利用控制序列在输出序列上的信息泄漏，给出了分析密码学控选逻辑的一种方法。

关键词 密码学控选逻辑，互信息，“停走”型钟控序列

中图号 TN918

1 引 言

在序列密码的编码过程中，经常利用控选逻辑技术实现其密码算法。迄今为止，人们使用的控选逻辑技术主要有 $(l_0,l_1,\cdots,l_{m-1})$ 型钟控序列， $1/m$ 型选择序列， m 型控选 ROM 序列等。最近，文献 [1] 在上面几种常见的控选逻辑的基础上给出了一种密码学控选逻辑的概率模型，得到了密码学控选逻辑控制序列与输出序列互信息为零的一个充分条件。本文对文献 [1] 中的定义进行修正，给出了密码学控选逻辑的概率模型更为合理的定义，得到了密码学控选逻辑控制序列与输出序列互信息为零的充要条件；鉴于“停走”型钟控密钥流生成器在社会实践中的应用，且目前没有有效的相关分析方法 [2,3] ，本文利用控制序列在输出序列上的信息泄漏，给出了分析该密码学控选逻辑的一种方法，该方法能够非常容易地攻破该密码体制。另外，本文的结果对设计和分析密钥流生成器都有一定的参考价值。

2 密码学控选逻辑控制序列与输出序列互信息为零的充要条件

定义 1 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) 上独立均匀分布的随机变量序列， $\tilde{a}$ 和 $\tilde{b}$ 也相互独立，且 $a_i\in\{0,1,\cdots,n-1\}$, $b_i\in\{0,1,\cdots,m-1\}$, $i=0,1,\cdots$。

记 $c_j=\chi_{g_j(b_0,b_1,\cdots,b_{j-1})}(a_{f_0^{(j)}(b_0,b_1,\cdots,b_{j-1})},a_{f_1^{(j)}(b_0,b_1,\cdots,b_{j-1})},\cdots,a_{f_{k-1}^{(j)}(b_0,b_1,\cdots,b_{j-1})})$ ，其中 $k\in N$, $f_l^{(j)}$, $l=0,1,\cdots,k-1$ 为随机向量 $(b_0,b_1,\cdots,b_{j-1})$ 到 $Z^+\bigcup\{0\}$ 的可测变换，且变换对 b_{j-1} 是非退化的， g_j 为随机向量 $(b_0,b_1,\cdots,b_{j-1})$ 到 $\{0,1,\cdots,k-1\}$ 的可测变换，$\chi_{g_j(b_0,b_1,\cdots,b_{j-1})}$ 即为 $c_j=a_{f^{(j)}_{g_j(b_0,b_1,\cdots,b_{j-1})}(b_0,b_1,\cdots,b_{j-1})}$, $j=1,2,\cdots$ ，则 c_j 亦为 (Ω,F,p) 上且取值于 $\{0,1,\cdots,n-1\}$ 上的随机变量，记为 $\tilde{c}=\{c_1,c_2,c_3,\cdots\}$ 满足上述关系的系统 $(\tilde{a},\tilde{b},\tilde{c})$ 称之为密码学控选逻辑序列概率模型。其中， $\tilde{a}=\{a_0,a_1,a_2,\cdots,\}$ 为控选逻辑输入序列，$\tilde{b}=\{b_0,b_1,b_2,\cdots,\}$ 为控选逻辑控制序列， $\tilde{c}=\{c_1,c_2,c_3,\cdots,\}$ 为控选逻辑输出序列。

从上面可以看出，定义 1 在文献 [1] 的基础上附加了可测变换 $f^{(i)}_{g_i(b_0,\cdots,b_{i-1})}(b_0,\cdots,b_{i-1})$ 对变元 b_{i-1} 是非退化的条件。在密码编码学中，这一定义显然是具有实际意义的。参照文献 [1] ，我们可类似地证明，文献 [1] 定义的 $(l_0,l_1,\cdots,l_{m-1})$ 型钟控序列概率模型， $1/m$ 型选择序列概率模型， m 型控选 ROM 序列概率模型均满足定义 1 。下面我们研究密码学控选逻辑控制序列与输出序列互信息为零的充要条件。

[1] 2002-05-29 收到， 2002-11-14 改回

为方便起见，$(c_1,c_2,\cdots,c_t)$, $(x_1,x_2,\cdots,x_t)$, $(b_0,b_1,\cdots,b_t)$, $(y_0,y_1,\cdots,y_t)$ 分别简记作 $\bar{c}_t$, $\bar{x}_t$, $\tilde{b}_t$, $\tilde{y}_t$，其中 $x_i\in\{0,1,\cdots,n-1\}$, $y_j\in\{0,1,\cdots,m-1\}$, $i=1,2,\cdots$, $j=0,1,\cdots$。

引理 1　$c_1,c_2,\cdots,c_t$ 相互独立的充要条件是 $\forall\tilde{y}_{t-1}\in F_m^t$, $f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1})$, $i=1,2,\cdots,t$ 中没有相等者。

证明　(1) *必要性*　若 $c_1,c_2,\cdots,c_t$ 相互独立，由定义 1 可得：

$\chi_{g_i(b_0,b_1,\cdots,b_{i-1})}(a_{f_1^{(i)}(b_0,b_1,\cdots,b_{i-1})},a_{f_2^{(i)}(b_0,b_1,\cdots,b_{i-1})},\cdots,a_{f_k^{(i)}(b_0,b_1,\cdots,b_{i-1})}),i=1,2,\cdots,t$ 相互独立，即 $a_{f^{(1)}_{g_1(b_0)}(b_0)},a_{f^{(2)}_{g_2(b_0,b_1)}(b_0,b_1)},\cdots,a_{f^{(t)}_{g_t(b_0,b_1,\cdots,b_{t-1})}(b_0,b_1,\cdots,b_{t-1})}$ 相互独立。又 $\tilde{a}=\{a_0,a_1,a_2,\cdots\}$ 是概率空间 (Ω,F,p) 上的独立均匀分布的随机变量序列，故 $\forall\tilde{y}_{t-1}\in F_m^t$, $f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1})$, $i=1,2,\cdots,t$ 中没有相等者；

(2) *充分性*　若 $\forall\tilde{y}_{t-1}\in F_m^t$, $f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1})$, $i=1,2,\cdots,t$ 中没有相等者，则由定义 1 中 $\tilde{a}$ 的条件可知：$a_{f^{(1)}_{g_1(y_0)}(y_0)},a_{f^{(2)}_{g_2(\tilde{y}_1)}(\tilde{y}_1)},\cdots,a_{f^{(t)}_{g_t(\tilde{y}_{t-1})}(\tilde{y}_{t-1})}$ 相互独立，故 $c_1,c_2,\cdots,c_t$ 相互独立。

引理 2[4]　对输入随机变量 X 和输出随机变量 Y，互信息量 $I(X;Y)\geq 0$，且当 X 与 Y 统计独立时，才有 $I(X;Y)=0$。

引理 3　$I(\tilde{b}_t;\bar{c}_{t+1})=I(\tilde{b}_{t-1};\bar{c}_t)+I(\tilde{b}_t;c_{t+1}|\bar{c}_t)$。

证明　$p\{\tilde{b}_i=\tilde{y}_i,\bar{c}_{i+1}=\bar{x}_{i+1}\}$, $p\{\tilde{b}_i=\tilde{y}_i\}$, $p\{\bar{c}_i=\bar{x}_i\}$ 分别简记作 $p\{\tilde{b}_i,\bar{c}_{i+1}\}$, $p\{\tilde{b}_i\}$, $p\{\bar{c}_i\}$，则有

$$
\begin{aligned}
I(\tilde{b}_t;\bar{c}_{t+1}) &= \sum_{\tilde{b}_t\in F_m^{t+1}}\sum_{\bar{c}_{t+1}\in F_n^{t+1}} p\{\tilde{b}_t,\bar{c}_{t+1}\}\log_2\frac{p\{\tilde{b}_t,\bar{c}_{t+1}\}}{p\{\tilde{b}_t\}\cdot p\{\bar{c}_{t+1}\}}\\
&= \sum_{\tilde{b}_t\in F_m^{t+1}}\sum_{\bar{c}_{t+1}\in F_n^{t+1}} p\{\tilde{b}_t,\bar{c}_{t+1}\}\log_2\left[\frac{p\{\tilde{b}_{t-1},\bar{c}_t\}}{p\{\tilde{b}_{t-1}\}\cdot p\{\bar{c}_t\}}\frac{p\{(b_t,c_{t+1})|(\tilde{b}_{t-1},\bar{c}_t)\}}{p\{b_t|\tilde{b}_{t-1}\}\cdot p\{c_{t+1}|\bar{c}_t\}}\right]\\
&= I(\tilde{b}_{t-1};\bar{c}_t)+\sum_{\tilde{b}_t\in F_m^{t+1}}\sum_{\bar{c}_{t+1}\in F_n^{t+1}} p\{\tilde{b}_t,\bar{c}_{t+1}\}\log_2\frac{p\{(b_t,c_{t+1})|(\tilde{b}_{t-1},\bar{c}_t)\}}{p\{b_t\}\cdot p\{c_{t+1}|\bar{c}_t\}}\\
&= I(\tilde{b}_{t-1};\bar{c}_t)+\sum_{\tilde{b}_t\in F_m^{t+1}}\sum_{\bar{c}_{t+1}\in F_n^{t+1}} p\{\tilde{b}_t,\bar{c}_{t+1}\}\log_2\frac{p\{c_{t+1}|(\tilde{b}_t,\bar{c}_t)\}}{p\{c_{t+1}|\bar{c}_t\}}\\
&= I(\tilde{b}_{t-1};\bar{c}_t)+I(\tilde{b}_t;c_{t+1}|\bar{c}_t)
\end{aligned}
$$

定理 1　$I(\tilde{b}_{t-1};\bar{c}_t)=0$ 的充要条件是 $\forall\tilde{y}_{t-1}\in F_m^t$, $f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1})$, $i=1,2,\cdots,t$ 中没有相等者。

证明　由引理 2：若 $I(\tilde{b}_{t-1};\bar{c}_t)=0$，则 $\tilde{b}_{t-1}$, $\bar{c}_t$ 相互独立，即对任意的 $\tilde{y}_{t-1}\in F_m^t$, $\bar{x}_t\in F_n^t$，均有 $p\{\tilde{b}_{t-1}=\tilde{y}_{t-1},\bar{c}_t=\bar{x}_t\}=p\{\tilde{b}_{t-1}=\tilde{y}_{t-1}\}\cdot p\{\bar{c}_t=\bar{x}_t\}$。

(1) *必要性*　令 $p\{b_i=y\}=p$, $p\{a_i=x\}=q$，用归纳法证之。

当 $t=2$ 时，若存在 $\tilde{y}_1\in F_m^2$，使得 $f^{(1)}_{g_1(y_0)}(y_0)=f^{(2)}_{g_2(y_0,y_1)}(y_0,y_1)$，令 $I_1=\{\tilde{y}_1|f^{(1)}_{g_1(y_0)}(y_0)=f^{(2)}_{g_2(y_0,y_1)}(\tilde{y}_1),\tilde{y}_1\in F_m^2\}$, $I_2=\{\tilde{y}_1|f^{(1)}_{g_1(y_0)}(y_0)\neq f^{(2)}_{g_2(y_0,y_1)}(\tilde{y}_1),\tilde{y}_1\in F_m^2\}$，则 $I_1\neq\phi$, $I_2\neq\phi$，任取 $(y_0,y_1)\in I_1$, $(x_1,x_2)\in F_n^2$，且 $x_1\neq x_2$，则 $p\{\tilde{b}_1=\tilde{y}_1,\bar{c}_2=\bar{x}_2\}=0$，而由 $\tilde{b}_t$, $\tilde{a}_t$ 的独立性知：$p\{\tilde{b}_1=\tilde{y}_1\}=p^2\neq 0$, $p\{\bar{c}_2=\bar{x}_2\}=\sum_{\tilde{v}_1\in I_2}p\{\tilde{b}_1=\tilde{v}_1,\bar{c}_2=\bar{x}_2\}=\sum_{\tilde{v}_1\in I_2}p\{\tilde{b}_1=$

$\tilde{v}_1, a_{f^{(1)}_{g_1(v_0)}(v_0)} = x_1, a_{f^{(2)}_{g_2(v_0,v_1)}(v_0,v_1)} = x_2\} = p^2q^2|I_2| \neq 0$. 这与 $I(\tilde{b}_1;\bar{c}_2) = 0$, $\tilde{b}_1$ 与 $\bar{c}_2$ 相互独立矛盾，所以 $t = 2$ 时，结论成立；

假设 $t = k$ 时，若 $I(\tilde{b}_{k-1};\bar{c}_k) = 0$, 则 $\forall \tilde{y}_{k-1} \in F_m^k, a_{f^{(1)}_{g_1(y_0)}(y_0)}, a_{f^{(2)}_{g_2(\tilde{y}_1)}(\tilde{y}_1)}, \cdots, f^{(k)}_{g_k(\tilde{y}_{k-1})}(\tilde{y}_{k-1})$ 没有相等者，下证 $t = k+1$ 时的情况：

当 $t = k+1$ 时，由引理 3 与假设：

$I(\tilde{b}_k;\bar{c}_{k+1}) = 0 \Rightarrow I(\tilde{b}_{k-1};\bar{c}_k) = 0 \Rightarrow f^{(i)}_{g_i(b_1,\cdots,b_{i-1})}(b_0,\cdots,b_{i-1}),\quad i = 1,2,\cdots,k$

没有相等者。若存在 $1 \le j < k+1$, $\tilde{y}_k \in F_m^{k+1}$, 使得 $f^{(j)}_{g_j(\tilde{y}_{j-1})}(\tilde{y}_{j-1}) = f^{(k+1)}_{g_{k+1}(\tilde{y}_k)}(\tilde{y}_k)$, 令

$$I_1 = \{\tilde{y}_k | f^{(j)}_{g_j(\tilde{y}_{j-1})}(\tilde{y}_{j-1}) = f^{(k+1)}_{g_{k+1}(\tilde{y}_k)}(\tilde{y}_k), \tilde{y}_k \in F_m^{k+1}\};$$

$$I_2 = \{\tilde{y}_k | f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1}) = f^{(k+1)}_{g_{k+1}(\tilde{y}_k)}(\tilde{y}_k), \tilde{y}_k \in F_m^{k+1}, 1 \le i < k+1 \text{且} i \neq j\};$$

$$I_2' = \{i | \exists \tilde{y}_k \in F_m^{k+1}, f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1}) = f^{(k+1)}_{g_{k+1}(\tilde{y}_k)}(\tilde{y}_k), 1 \le i \neq j < k+1\};$$

$$I_3 = \{\tilde{y}_k | f^{(i)}_{g_i(\tilde{y}_{i-1})}(\tilde{y}_{i-1}) \neq f^{(k+1)}_{g_{k+1}(\tilde{y}_k)}(\tilde{y}_k), 1 \le i < k+1, \tilde{y}_k \in F_m^{k+1}\};$$

由定义 1， I_2, I_3 不同时为空集（否则， $f^{(k+1)}_{g_{k+1}(\tilde{b}_k)}(\tilde{b}_k)$ 对变元 b_k 为退化的情况），对任意的 $\tilde{y}_k \in I_1$, 取 $\bar{x}_{k+1} \in F_n^{k+1}$, $x_j \neq x_{k+1}$, 且 $\forall i \in I_2'$, $x_i = x_{k+1}$, 则 $p\{\tilde{b}_k = \tilde{y}_k, \bar{c}_{k+1} = \bar{x}_{k+1}\} = 0$, 而由 $\tilde{b}_t$, $\tilde{a}_t$ 的独立性知：

$$p\{\tilde{b}_k = \tilde{y}_k\} = p^{k+1} \neq 0,$$

$$p\{\bar{c}_{k+1} = \bar{x}_{k+1}\} = \sum_{\tilde{v}_k \in I_2} p\{\tilde{b}_k = \tilde{v}_k, \bar{c}_{k+1} = \bar{x}_{k+1}\} + \sum_{\tilde{v}_k \in I_3} p\{\tilde{b}_k = \tilde{v}_k, \bar{c}_{k+1} = \bar{x}_{k+1}\}$$

$$= \sum_{\tilde{v}_k \in I_2} p\{\tilde{b}_k = \tilde{v}_k, a_{f^{(1)}_{g_1(v_0)}(v_0)} = x_1, \cdots, a_{f^{(i)}_{g_i(\tilde{v}_{i-1})}(\tilde{v}_{i-1})} = x_i, \cdots, a_{f^{(k+1)}_{g_{k+1}(\tilde{v}_k)}(\tilde{v}_k)} = x_{k+1}\}$$

$$+ \sum_{\tilde{v}_k \in I_3} p\{\tilde{b}_k = \tilde{v}_k, a_{f^{(1)}_{g_1(v_0)}(v_0)} = x_1, \cdots, a_{f^{(k+1)}_{g_{k+1}(\tilde{v}_k)}(\tilde{v}_k)} = x_{k+1}\} = p^{k+1}q^k|I_2| + p^{k+1}q^{k+1}|I_3| \neq 0$$

这与 $I(\tilde{b}_k;\bar{c}_{k+1}) = 0$, $\tilde{b}_k$ 与 $\bar{c}_{k+1}$ 相互独立矛盾，所以 $t = k+1$ 时，结论成立；

(2) 充分性 由定义 1 及引理 1： $a_{f^{(1)}_{g_1(v_0)}(y_0)}, a_{f^{(2)}_{g_2(\tilde{y}_1)}(\tilde{y}_1)}, \cdots, a_{f^{(t)}_{g_t(\tilde{y}_{t-1})}(\tilde{y}_{t-1})}, b_0, \cdots, b_{t-1}$ 相互独立，从而 $\tilde{b}_{t-1}, \bar{c}_t$ 相互独立，故 $I(\tilde{b}_{t-1};\bar{c}_t) = 0$ 。 证毕

3 密码学控选逻辑控制序列在输出序列上的熵漏分析

从信息论的观点出发，若控选逻辑控制序列与输出序列的互信息不为零，那么分析者不但能从输出序列中获得输入序列的信息，而且能从输出序列中获得控制序列的部分信息，这有时会给整个密码体制带来灾难性的后果。由于“停走”型密钥流生成器在密码学中有广泛的应用，下面以此研究控选逻辑控制序列的信息泄露问题。

“停走”型密钥流生成器由两个移存器组成，一个移存器用于控制另一个的步进，文献 [3] 给出了其钟控序列的概率模型：

定义 2 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。

显然，若令 $k=1, f_0^{(i)}(b_0,b_2,\cdots,b_{i-1})=\sum_{j<i}b_j, g_i(b_0,b_2,\cdots,b_{i-1})\equiv 0, c_0=a_0$，则定义 2 满足定义 1。由定理 1 可得下面结论：

推论 1　“停走”型钟控序列控制序列与输出序列的互信息 $I(\tilde{b}_{n-1},\tilde{c}_n)>0$。

引理 4[5]　$\forall \tilde{x}_n\in F_2^{n+1}, \tilde{y}_{n-1}\in F_2^n (n\geq 1), p\{\tilde{c}_n=\tilde{x}_n,\tilde{b}_{n-1}=\tilde{y}_{n-1}\}\neq 0$ 的充要条件是若 $x_j\neq x_{j+1}(0\leq j<n)$，则 $y_j=1$，此时若设 $\sum_{j=1}^{n}(x_{j-1}\oplus x_j)=i, \sum_{j=0}^{n-1}y_j=i+t(0\leq i\leq n,$ $0\leq t\leq n-i)$，则 $p\{\tilde{c}_n=\tilde{x}_n,\tilde{b}_{n-1}=\tilde{y}_{n-1}\}=1/2^{n+i+t+1}$。

引理 5[5]　$p\{\tilde{c}_n=\tilde{x}_n\}=3^{n-i}/2^{2n+1}$，其中 $i=\sum_{l=1}^{n}(x_{l-1}\oplus x_l)$。

定理 2　若令 $\xi=\sum_{j=1}^{n}(c_{j-1}\oplus c_j)$，则 $E\xi=\frac{n}{4}, D\xi=\frac{3}{16}n$。

证明　由引理 5：$E\xi=\sum_{i=0}^{n}\left(2C_n^i\cdot i\cdot\frac{3^{n-i}}{2^{2n+1}}\right)=\frac{3^n\cdot n}{4^n}\sum_{i=1}^{n}\frac{C_{n-1}^{i-1}}{3^i}=\frac{n}{4}$；因为

$$E\xi^2=\sum_{i=0}^{n}\left(2C_n^i\cdot i^2\cdot\frac{3^{n-i}}{2^{2n+1}}\right)=\sum_{i=0}^{n}\left[C_n^i\cdot i\cdot(i-1)\cdot\frac{3^{n-i}}{4^n}\right]+E\xi$$

$$=\frac{3^n}{4^n}\sum_{i=2}^{n}\frac{C_{n-2}^{i-2}}{3^i}+E\xi=\frac{1}{16}n(n-1)+E\xi$$

所以 $D\xi=E\xi^2-(E\xi)^2=\frac{1}{16}n(n-1)+\frac{n}{4}-\frac{n^2}{16}=\frac{3}{16}n$。　　证毕

由于移存器在任意位置的输出为其初始状态的线性表达式，因此只要获得移存器在若干位置的输出，就可求出移存器的初始状态。引理 4 给出了从输出序列中获取控制移存器输出的方法，定理 2 给出了获取控制移存器秘密密钥所需输出序列长度的期望值。假设用于控制的移存器和源序列寄存器的级数分别为 N, M，且反馈多项式已知，由移存器的理论可知，分析者只要获得 $\max\{4N,M\}$ 长度的密钥流，用分别征服的方法就可攻破该密码体制。

4 结束语

由以上分析可以看到，密码学控选逻辑中可测变换 $f_{g_i(b_0,\cdots,b_{i-1})}^{(i)}(b_0,\cdots,b_{i-1})$ 的设计是非常重要的。“停走”型钟控序列虽然在周期性、线性复杂度、平衡性、相关免疫性等方面具有良好的密码学性质[2]，但它无法掩盖控制序列在输出序列的信息泄露给整个密码体制造成的影响。在基于 LFSR 序列密码的编码过程中，可测变换 $f_{g_i(b_0,\cdots,b_{i-1})}^{(i)}(b_0,\cdots,b_{i-1})$ 的构造是非常方便的，我们可借助控选逻辑函数的设计或满足某些密码学性质的由低阶变元到高阶变元的设计方法来实现。

参　考　文　献

[1] 范修斌，吕述望，刘传东，密码学控选逻辑控制序列与输出序列互信息为零的一个充分条件，通信学报，2002, 23(8), 14–18.

[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] 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.

[4] 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.

[5] 刘传东，吕述望，范修斌，“停走”型钟控序列概率模型信息论分析，电子与信息学报，2003, 25(1), 67–73.

THE MUTUAL INFORMATION BETWEEN CONTROL AND OUTPUT SEQUENCES OF THE CONTROL-CHOICE CRYPTOGRAPHIC LOGIC

Liu Chuandong Lü Shuwang Fan Xiubin

(*State Key Lab. of Info. Security, Graduate School of USTC, Beijing* 100039, *China*)

Abstract This paper presents the probability model of the control-choice cryptographic logic. A necessery and sufficient condition is gained which satisfies that the mutual information is zero between control and output sequences of the control-choice cryptographic logic. By using the information leak between control and output sequences, a method of analysing the control-choice cryptographic logic is given.

Key words Control-choice cryptographic logic, Mutual information, Stop-and-go clock-controlled sequence

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.