双侧停走生成器的概率模型

胡学先　刘文芬　李世取
(解放军信息工程大学信息工程学院　郑州　450002)

摘　要：该文首次建立了双侧停走生成器(Bilateral Stop/Go Generator)的概率模型，研究了模型中作为钟控函数输入的中间状态序列的马氏性、遍历性及严平稳性等概率性质，得到了生成器输出序列中 0, 1 分布是不平衡的结论，由此指出不能将这种生成器直接作为密钥流生成器；给出了生成器输出序列和相应的 LFSR 输出序列之间的符合率以及一阶差分序列之间的符合率；证明了生成器输出序列满足强大数定律和中心极限定理。

关键词：双侧停走生成器；钟控；马氏性；符合率
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2007)12-2974-04

A Probabilistic Model of the Bilateral Stop/Go Generator

Hu Xue-xian　Liu Wen-fen　Li Shi-qu
(*Institute of Information Engineering, PLA Information Engineering University, Zhengzhou* 450002, *China*)

Abstract: The probabilistic models for the bilateral stop/go generator are established. The properties such as Markov property, ergodic property and stationarity of the internal state sequence are studied. It is proved that the distributions of 0 and 1 in the output sequence are imbalanced, which implies that this generator can not be used as keystream generator directly. The rate of coincidence between the output sequence and corresponding LFSR sequences, together with their first derivatives are analyzed. The limit properties of the output sequence are also considered.

Key words: Bilateral stop/go generator; Clock-controlled; Markov property; Rate of coincidence

1　引言

钟控生成器被广泛地应用于密钥流生成器中以产生长周期、高线性复杂度和好的统计特性的序列[1]，其中钟控停走生成器在高速应用场合更受关注。分析还表明停走生成器产生的序列在一定程度上具有 m 序列和 M 序列的良好的伪随机性，同时克服了 m 序列在平移等价下相异序列的数量很少和 M 序列不易实现的缺陷。

双侧停走生成器是基于钟控停走生成器的密钥流生成器中的重要的一种，这种生成器由两个长为 L 的线性移位寄存器(LFSR)互钟控组成，用以产生周期为 $5\cdot 2^{L-2}-1$ 的序列[2]。文献[3]中指出这种生成器结构较级联停走等更为简单，且输出序列中不存在明显的密钥冗余。文献[4]中通过将常规钟控移存器的输出看成是独立同分布的序列，用输出序列和相应的LFSR序列之间的编辑概率作为相关性度量，对这种生成器进行了分别征服攻击。

本文在将LFSR输出的“伪随机”序列看成是“真随机”的随机性假设下，首次建立了双侧停走生成器的严格的概率模型，研究了模型中作为钟控函数输入的中间状态序列的马氏性、遍历性及严平稳性等概率性质，进而得到了钟控函数的输出序列和模型的输出序列的分布。所得结论表明这种生成器输出序列中的 0, 1 分布是不平衡的，因而不能将这种生成器直接作为密钥流生成器。本文还给出了生成器输出序列和相应的LFSR输出序列之间的符合率以及一阶差分序列之间的符合率，揭示了这些序列之间存在相关性，为对这种生成器的相关攻击甚至快速相关攻击提供了理论依据。本文最后证明了这种生成器的输出序列满足强大数定律和中心极限定理，这与关于钟控停走生成器的结论是一致的[5]。

2　双侧停走生成器的结构

双侧停走生成器由两个等长的线性移位寄存器(LFSR1、LFSR2)组成，这两个移存器通过互钟控的方式相连接(如图 1 所示)。具体地说，这两个生成器 $n+1$ 时刻的停走由一个二输出的钟控函数 $\big(c_1(n+1),c_2(n+1)\big)=h\big(s_{1,L}(n),s_{1,L-1}(n),s_{2,L}(n),s_{2,L-1}(n)\big)$ 来控制，其中 $\big(s_{1,L}(n),s_{1,L-1}(n)\big)$ 为 n 时刻移存器 LFSR1 的第 L 和第 $L-1$ 位，$\big(s_{2,L}(n),s_{2,L-1}(n)\big)$ 为 n 时刻移存器 LFSR2 的第 L 和第 $L-1$ 位。当 $c_i(n+1)$ 为 1 时，$n+1$ 时刻移存器 LFSRi 向前步进一步，否则不步进。其中，钟控函数 h 的定义如下，对任意 $a=(a_1,a_2,a_3,a_4)\in F_2^4$，

$$h(a_1,a_2,a_3,a_4)=\begin{cases}(1,0), & (a_1,a_2)=(0,1)\\ (0,1), & (a_1,a_2)\neq(0,1),(a_3,a_4)=(0,1)\\ (1,1), & (a_1,a_2)\neq(0,1),(a_3,a_4)\neq(0,1)\end{cases}\quad(1)$$

2006-05-22 收到，2006-12-29 改回
计算机网络与信息安全教育部重点实验室开放课题基金资助课题

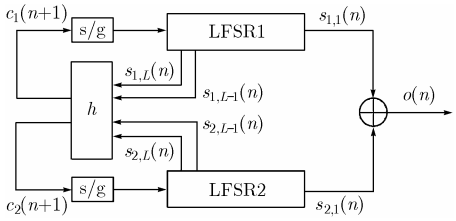

图 1　双侧停走生成器的结构图

3　概率模型

由于实用的线性移存器输出序列应具有良好的伪随机性，本文建立双侧停走生成器的如下概率模型：

随机性假设(1)　假设 $Y^{\infty}=\{Y_0,Y_1,Y_2,\cdots\}$ 和 $Z^{\infty}=\{Z_0,Z_1,Z_2,\cdots\}$ 是定义在同一概率空间上的独立同分布的随机变量序列，具有分布

$$\begin{aligned}P\{Y_n=0\}&=P\{Y_n=1\}=P\{Z_n=0\}\\&=P\{Z_n=1\}=\frac{1}{2},\quad n\ge 0\end{aligned}\tag{2}$$

分别称

$$\left.\begin{aligned}&U_0=Y_0,\quad U_n=Y_{\sum_{i=0}^{n-1}C_1(i)},\quad n\ge 1\\&V_0=Z_0,\quad V_n=Z_{\sum_{i=0}^{n-1}C_2(i)},\quad n\ge 1\end{aligned}\right\}\tag{3}$$

为双侧停走生成器的概率模型中 LFSR1 和 LFSR2 的输出序列。其中钟控序列 $\{C(n)=(C_1(n),C_2(n))\}_{n=0}^{\infty}$ 和作为钟控函数输入的中间状态序列 $(\xi(n))_{n=0}^{\infty}$ 定义如下：

$$\left.\begin{aligned}&\xi(0)=(Y_1,Y_0,Z_1,Z_0),\quad (C_1(0),C_2(0))=h(\xi(0))\\&\xi(n)=\left(Y_{1+\sum_{i=0}^{n-1}C_1(i)},Y_{\sum_{i=0}^{n-1}C_1(i)},Z_{1+\sum_{i=0}^{n-1}C_2(i)},Z_{\sum_{i=0}^{n-1}C_2(i)}\right),\\&(C_1(n),C_2(n))=h(\xi(n)),\quad n\ge 1\end{aligned}\right\}\tag{4}$$

称 $X_n=U_n\oplus V_n, n\ge 0$ 为双侧停走生成器概率模型的输出序列。

注：为了记号简单，上述概率模型中忽略了 LFSR 的长度 L。事实上，若进一步考虑 LFSR 的长度 L，只需在上述概率模型的定义中将相应的序列平移 L 位即可。

4　性质分析

在不涉及运算的时候，本文以下部分记 F_2^4 中的元素为 $s_0,s_1,\cdots,s_{15}$，其中 $a=(a_1,a_2,a_3,a_4)\in F_2^4$ 对应于 s_k，$k=\sum_{i=1}^{4}a_i\cdot 2^{4-i}$。

首先根据所给概率模型的定义可得到中间状态序列的如下性质。

定理 1　状态序列 $(\xi(n))_{n=0}^{\infty}$ 是齐次马氏链，状态空间为 F_2^4，一步转移概率矩阵为 $\boldsymbol{P}=(p_{i,j})$，其中 $p_{i,j}$ 表示由状态 s_i 转移到状态 s_j 的概率，$i,j=0,1,\cdots,15$。

$$\boldsymbol{P}=\begin{bmatrix}
1/4&0&1/4&0&0&0&0&0&1/4&0&1/4&0&0&0&0&0\\
1/2&0&1/2&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4&0&0&0&0\\
0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4&0&0&0&0\\
1/2&0&0&0&0&0&0&0&1/2&0&0&0&0&0&0&0\\
0&1/2&0&0&0&0&0&0&0&1/2&0&0&0&0&0&0\\
0&0&1/2&0&0&0&0&0&0&0&1/2&0&0&0&0&0\\
0&0&0&1/2&0&0&0&0&0&0&0&1/2&0&0&0&0\\
0&0&0&0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4&0\\
0&0&0&0&0&0&0&0&1/2&0&1/2&0&0&0&0&0\\
0&0&0&0&0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4\\
0&0&0&0&0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4\\
0&0&0&0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1/2&0&1/2&0\\
0&0&0&0&0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4\\
0&0&0&0&0&1/4&0&1/4&0&0&0&0&0&1/4&0&1/4
\end{bmatrix}\tag{5}$$

证明　首先由生成器的驱动方式和概率模型中的随机性假设易知序列 $(\xi(n))_{n=0}^{\infty}$ 是状态空间为 F_2^4 的齐次马氏链。

其次，若

$$\begin{aligned}\xi(n)&=\left(Y_{1+\sum_{i=0}^{n-1}C_1(i)},Y_{\sum_{i=0}^{n-1}C_1(i)},Z_{1+\sum_{i=0}^{n-1}C_2(i)},Z_{\sum_{i=0}^{n-1}C_2(i)}\right)\\&=(0,0,0,0)\end{aligned}\tag{6}$$

则据钟控函数的定义可知 $h(0,0,0,0)=(1,1)$，此时钟控生成器 LFSR1 和 LFSR2 均向前步进一步，所以可以得到

$$\begin{aligned}\xi(n+1)&=\left(Y_{1+\sum_{i=0}^{n}C_1(i)},Y_{\sum_{i=0}^{n}C_1(i)},Z_{1+\sum_{i=0}^{n}C_2(i)},Z_{\sum_{i=0}^{n}C_2(i)}\right)\\&=\left(Y_{2+\sum_{i=0}^{n-1}C_1(i)},0,Z_{2+\sum_{i=0}^{n-1}C_2(i)},0\right)\end{aligned}\tag{7}$$

根据概率模型的随机性假设，状态 $\xi(n)=(0,0,0,0)$ 分别以 $1/4$ 的概率转移到状态 $(0,0,0,0)$，$(0,0,1,0)$，$(1,0,0,0)$，$(1,0,1,0)$ 中的每一个，而转移到其它状态的概率是 0。

按照上述方法可以得到所有状态的转移概率，这样就可以得到状态之间的转移矩阵 $\boldsymbol{P}=(p_{i,j})$。　证毕

结合上述转移矩阵，可以分析得到齐次马氏链 $(\xi(n))_{n=0}^{\infty}$ 的下述性质。

定理 2　齐次马氏链 $(\xi(n))_{n=0}^{\infty}$ 是不可分的遍历链，即 F_2^4 中的所有状态都是互通的，且都是非周期的正常返状态。

证明　由于 $\boldsymbol{P}^4$ 中的元素全部不为 0，根据互通的定义可以得到所有状态全是互通的，所以该齐次马氏链不可分。进一步根据 $\boldsymbol{P}^5$ 中的元素全部不为 0，可知所有状态全是非周期的。由于不可分的有限马氏链的状态都是正常返状态[6]，所以 F_2^4 中所有状态都是正常返的。　证毕

定理 3　齐次马氏链 $(\xi(n))_{n=0}^{\infty}$ 有唯一的平稳分布

$$\pi=\left(\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{30},\frac{1}{15},\frac{1}{30},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15},\frac{1}{15}\right)\tag{8}$$

证明　由齐次马氏链 $(\xi(n))_{n=0}^{\infty}$ 是不可分的遍历链，可得平稳分布的唯一性[6]。又由于平稳分布是方程组

$$(\pi_0,\pi_1,\cdots,\pi_{15})=(\pi_0,\pi_1,\cdots,\pi_{15})\cdot\boldsymbol{P}\tag{9}$$

满足条件 $\sum_{k=0}^{15}\pi_k=1$，$\pi_k\ge 0$，$k=1,2,\cdots,15$ 的唯一解。解方程组即可证得定理结论。　证毕

在模型的随机性假设下，上述马氏链的初始分布为 F_2^4 上的均匀分布，不同于平稳分布，因而该马氏链不具有严平稳性，但可以验证此时该马氏链以很快的速度收敛到上述平稳分布。因此不失一般性，进一步假设马氏链初始分布为平稳分布，即为如下随机性假设。

随机性假设(2) 假设 $\{Y_2,Y_3,Y_4,\cdots\}$ 和 $\{Z_2,Z_3,Z_4,\cdots\}$ 是定义在同一概率空间上的独立同分布的随机变量序列，具有分布

$$\begin{aligned}P\{Y_n=0\}&=P\{Y_n=1\}=P\{Z_n=0\}\\&=P\{Z_n=1\}=1/2,\quad n\geq 2\end{aligned}\tag{10}$$

而 (Y_1,Y_0,Z_1,Z_0) 是和 $\{Y_2,Y_3,Y_4,\cdots\}$，$\{Z_2,Z_3,Z_4,\cdots\}$ 均独立的随机向量，且具有分布

$$P\{(Y_1,Y_0,Z_1,Z_0)=s_i\}=\pi_i,\ \ i\in\{0,1,2,\cdots,15\}\tag{11}$$

在此假设下，前面给出的结论仍然成立。本文以下部分的分析将在“随机性假设(2)”下进行，此时将得到关于状态序列 $(\xi(n))_{n=0}^{\infty}$ 的更强的结论。

命题 1 齐次马氏链 $(\xi(n))_{n=0}^{\infty}$ 是严平稳的，且具有分布

$$P(\xi(n)=s_i)=\pi_i,\ \ i\in\{0,1,2,\cdots,15\}\tag{12}$$

关于钟控序列 $\{C(n)=(C_1(n),C_2(n))\}_{n=0}^{\infty}$ 的分布，我们有如下性质。

定理 4 序列 $\{C(n)=(C_1(n),C_2(n))\}_{n=0}^{\infty}$ 是状态空间为 F_2^2 的严平稳序列，且随机变量 $C(n)$ 具有分布

$$\left.\begin{aligned}&P(C(n)=(0,0))=0,P(C(n)=(1,1))=3/5\\&P(C(n)=(0,1))=P(C(n)=(1,0))=1/5\end{aligned}\right\}\tag{13}$$

证明 由于 $(C_1(n),C_2(n))=h(\xi(n))$，$n\geq 0$，根据序列 $(\xi(n))_{n=0}^{\infty}$ 的严平稳性可知序列 $\{C(n)\}_{n=0}^{\infty}$ 是严平稳的，进一步根据 $\xi(n)$ 的分布可求得 $C(n)$ 的分布为

$$\left.\begin{aligned}&P(C(n)=(0,1))=P(\xi(n)\\&\qquad\in\{(0,0,0,1),(1,0,0,1),(1,1,0,1)\})=1/5\\&P(C(n)=(1,0))=P(\xi(n)\\&\qquad\in\{(0,1,0,0),(0,1,0,1),(0,1,1,0),(0,1,1,1)\})=1/5\\&P(C(n)=(1,1))=1-P(C=(0,1))-P(C=(1,0))=3/5\end{aligned}\right\}\tag{14}$$

证毕

注：上述结论说明了在双侧停走生成器中，以 $1/5$ 的概率只是 LFSR1 向前步进一步，以 $1/5$ 的概率只是 LFSR2 向前步进一步，以 $3/5$ 的概率两个移存器同时都向前步进一步。

关于移位寄存器 LFSR1、LFSR2 及双侧停走生成器的输出序列分布，根据序列 $(\xi(n))_{n=0}^{\infty}$ 的严平稳性和 $\xi(n)$ 的分布，可以得到下述结论。

定理 5 双侧停走生成器的概率模型中 LFSR1 的输出序列 $\{U_0,U_1,U_2,\cdots\}$ 及 LFSR2 的输出序列 $\{V_0,V_1,V_2,\cdots\}$ 均是 F_2 上的严平稳序列，且具有分布

$$\left.\begin{aligned}&P(U_n=0)=8/15,\quad P(U_n=1)=7/15\\&P(V_n=0)=7/15,\quad P(V_n=1)=8/15\end{aligned}\right\}\tag{15}$$

命题 2 若记 $\eta(n)=\left(Y_{1+\sum_{i=0}^{n}C_1(i)}\oplus Z_{1+\sum_{i=0}^{n}C_2(i)},Y_{\sum_{i=0}^{n}C_1(i)}\oplus Z_{\sum_{i=0}^{n}C_2(i)}\right)$，则序列 $(\eta(n))_{n=0}^{\infty}$ 是状态空间为 F_2^2 的严平稳序列，且具有分布

$$\left.\begin{aligned}&P(\eta(n)=(0,0))=P(\eta(n)=(1,0))=4/15\\&P(\eta(n)=(0,1))=P(\eta(n)=(1,1))=7/30\end{aligned}\right\}\tag{16}$$

定理 6 双侧停走生成器概率模型的输出序列 $\{X_0,X_1,X_2,\cdots\}$ 是 F_2 上的严平稳序列，且具有分布

$$P(X_n=0)=8/15,\quad P(X_n=1)=7/15\tag{17}$$

证明 由于 $X_n=Y_{\sum_{i=0}^{n}C_1(i)}\oplus Z_{\sum_{i=0}^{n}C_2(i)}$，根据序列 $(\eta(n))_{n=0}^{\infty}$ 的严平稳性可知序列 $\{X_0,X_1,X_2,\cdots\}$ 是严平稳的。由命题 2 的结论可知

$$\left.\begin{aligned}&P(X_n=0)=P(\eta(n)=(0,0))+P(\eta(n)=(1,0))=8/15\\&P(X_n=1)=P(\eta(n)=(0,1))+P(\eta(n)=(1,1))=7/15\end{aligned}\right\}\tag{18}$$

证毕

定理 6 的结论表明，双侧停走生成器的输出序列不是 0, 1 平衡的序列，这与仿真实验所得的实际结果是一致的。考虑到实际应用中所需的密钥流序列应该满足较好的伪随机性，因此不能将这种生成器直接作为密钥流生成器。

5 概率模型输出序列和相应的 LFSR 序列之间的符合率

文献[7]指出考察钟控停走生成器的输出序列和相应的LFSR序列之间的符合率是一个重要的研究问题。对于双侧停走生成器，考察输出序列和相应的LFSR序列之间的符合率，分析其相关性，同样也是很重要的。

定理 7 设 $\{U_0,U_1,U_2,\cdots\}$，$\{V_0,V_1,V_2,\cdots\}$ 和 $\{X_0,X_1,X_2,\cdots\}$ 的定义如上，则

$$\left.\begin{aligned}&P(X_n=U_n)=7/15,\quad P(X_n\neq U_n)=8/15\\&P(X_n=V_n)=8/15,\quad P(X_n\neq V_n)=7/15\end{aligned}\right\}\tag{19}$$

定理8 设 $\{U_0,U_1,U_2,\cdots\}$，$\{V_0,V_1,V_2,\cdots\}$ 和 $\{X_0,X_1,X_2,\cdots\}$ 的定义如上。记一条序列 $\{A_0,A_1,A_2,\cdots\}$ 的一阶差分序列为 $\{\dot{A}_0,\dot{A}_1,\dot{A}_2,\cdots\}$，其中 $\dot{A}_n=A_n\oplus A_{n+1}$。则关于一阶差分序列 $\{\dot{U}_0,\dot{U}_1,\dot{U}_2,\cdots\}$，$\{\dot{V}_0,\dot{V}_1,\dot{V}_2,\cdots\}$ 和 $\{\dot{X}_0,\dot{X}_1,\dot{X}_2,\cdots\}$ 之间的符合率，有

$$\left.\begin{aligned}&P(\dot{X}_n=\dot{U}_n)=P(\dot{X}_n=\dot{V}_n)=3/5\\&P(\dot{X}_n\neq\dot{U}_n)=P(\dot{X}_n\neq\dot{V}_n)=2/5\end{aligned}\right\}\tag{20}$$

证明 根据全概率公式，有

$$\begin{aligned}P(\dot{X}_n=\dot{U}_n)&=\sum_{i,j\in E}P(\dot{X}_n=\dot{U}_n,\xi(n)=i,\xi(n+1)=j)\\&=\sum_{i,j\in E}P(\xi(n)=i,\xi(n+1)=j)\cdot I\{g_4(i)=g_4(j)\}\end{aligned}$$

$$= \sum_{i,j\in E} P\big(\xi(n)=i\big)\cdot P\big(\xi(n+1)=j \mid \xi(n)=i\big) \cdot I\big\{g_4(i)=g_4(j)\big\} \tag{21}$$

其中 $g_4\big((a_1,a_2,a_3,a_4)\big)=a_4$。再结合 $\xi(t)$ 的分布和定理 1 中给出的转移概率矩阵 $\boldsymbol{P}$ 计算可得 $P\big(\dot{X}_n=\dot{U}_n\big)=3/5$。其它概率可以类似地计算得到。　　证毕

6　输出序列的大数性质

将双侧停走生成器概率模型的输出序列 $\{X_0,X_1,X_2,\cdots\}$ 看成是实值的 0, 1 随机变量序列，则可以进一步考虑输出序列的大数性质。前面已证，$(\xi(t))_{t=0}^{\infty}$ 是有限状态的严平稳齐次马氏链，且是不可分的遍历链。根据马尔可夫链的泛函的极限定理[8]可得

定理 9　双侧停走生成器的概率模型的输出序列 $\{X_0,X_1,X_2,\cdots\}$ 服从强大数定律。

定理 10　双侧停走生成器的概率模型的输出序列 $\{X_0,X_1,X_2,\cdots\}$ 服从中心极限定理。

7　结束语

本文建立了生成器的严格的概率模型，讨论了钟控函数的输出序列、作为钟控函数输入的中间状态序列及生成器输出序列的概率性质，给出了输出序列的分布，得到了输出序列和相应的LFSR序列之间的符合率以及一阶差分序列之间的符合率，证明了输出序列符合强大数定律和中心极限定理。所得结论表明，尽管这种生成器输出序列具有较长的周期，但是由于序列中 0，1 分布是不平衡的，故不能将这种生成器直接作为密钥流生成器；生成器输出序列和相应的移存器输出序列之间存在相关性，说明可以据此对这种生成器实施相关攻击甚至快速相关攻击，关于这部分结果，我们将在以后的工作中给出。

参 考 文 献

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

[2] Zeng K C, Yang C H and Rao T R N. Large primes in stream-cipher cryptography. Advances in Cryptology-AUSCRYPT 90(LNCS 453), Berlin, Springer-Verlag, 1990: 194–205.

[3] Zeng K C, Yang C H, Wey D Y and Rao T R N. Pseudorandom bit generators in stream-cipher cryptography. *IEEE Computer*, 1991, 24(2): 8–17.

[4] Golic J Dj and Menicocci R. Edit probability correlation attacks on stop-go clocked keystream generators. *Journal of Cryptology*, 2002, 15(16): 41–68.

[5] 李世取, 黄晓英, 刘文芬, 等. 密码学中的有关概率模型. 北京: 电子工业出版社, 2005: 169–173.

[6] 林元杰. 应用随机过程. 北京: 清华大学出版社, 2002: 78–116.

[7] 丁存生, 肖国镇. 流密码学及其应用. 北京: 国防工业出版社, 1994: 181–202.

[8] 胡迪鹤. 随机过程：基础、理论、应用(第二版). 武汉: 武汉大学出版社, 2005: 248–252.

胡学先：　男，1982 年生，硕士生，研究方向为概率统计在密码学中的应用.

刘文芬：　女，1965 年生，教授，硕士生导师，主要研究方向为概率统计在密码学中的应用.

李世取：　男，1945 年生，教授，博士生导师，主要研究方向为概率统计在密码学中的应用.