国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第10卷第4期 1988年12月 Vol.10.No.4

具有最佳汉明相关性能的跳频序列族

梅文华 陈先福
（空军航空工程研究所） （国防科技大学）

摘 要

在非正交跳频扩展频谱多址通信系统中用作跳频图样的P^k进制序列族要求具有小的汉明互相关。文[1]中得到了给定长度和字母表大小的序列的异相自相关及互相关的下限，并构造了具有最佳汉明相关性能的序列族。本文中提出一种更一般的构造方法，文[1]的构造是它的一个特例。构造出的序列族具有最佳汉明相关性能，并且可部分解决Hop—and—Stay问题。

关键词：通信，跳频，序列

1 引 言

跳频通信技术具有抗干扰防窃听和选址多址组网等优点，在战术无线通信方面得到重视和应用。跳频通信的实现是用伪随机码（称跳频码）控制信号载波频率在一定频率范围内跳变来完成的，频率跳变的规律称为跳频图样。寻求和设计比较理想的跳频码是研究跳频通信技术的重要课题之一。国内外应用于扩频系统的跳频图样设计技术，主要基于m序列、M序列、R-S码、本原序列及一般Bent函数序列等。文[1]中考虑了基于m序列进行跳频图样设计的一般模型。即使用有限域GF(p)上的n级最大长度线性反馈移位寄存器，并且以寄存器的k个相邻级控制频率合成器而不用全部n级，如图1所示。这种序列具有最佳的汉明相关性能，但是每当在移存器里出现n重$\times\times\cdots\times$，$\times\neq 0$时，则输入到频合的是连续$n-k+1$次跳变的k重$\times\times\cdots\times$。当$0\ 0\cdots 0X$出现在移存器时类似情况也会发生。这样信号将停留在一个频隙上相当长时间，易于被非法接收机检测，这称为Hop—and—Stay问题。

本文提出一个改进的构造方法，论证其产生的序列族具有最佳的汉明相关性能，该方法可部分解决Hop—and—Stay问题具具有更大的密钥量。改进的方法是：使用k个非相邻级而不是相邻级去控制频率合成器，如图2所示。

首先给出汉明相关的定义及最佳性判据。

给定字母表A上的长为q的两个序列$X=\{x(j)\}$和$Y=\{y(j)\}$之间的汉明相关如下定义：

$$H_{XY}(\tau)=\sum_{j=0}^{q-1}h[x(j),y(j+\tau)],\quad 0\leqslant\tau<q \tag{1}$$

1987年12月10日收稿

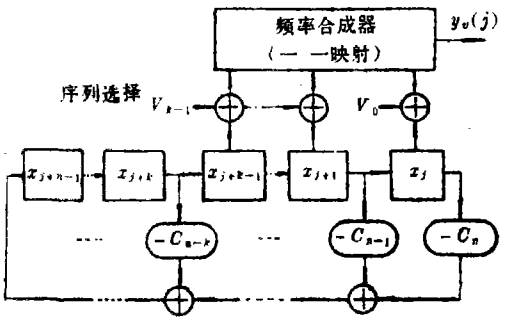

图 1 Lempel—Greenberger模型

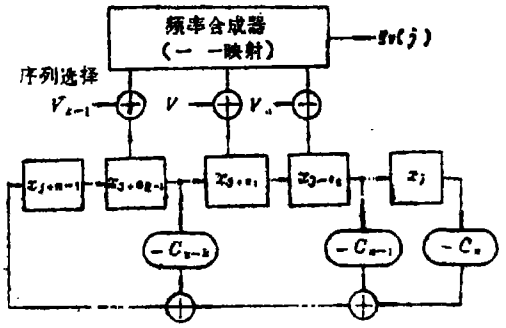

图 2 改进的一般模型

其中

$$h[x,y]=\begin{cases}1, & \text{如果}x=y\\ 0, & \text{如果}x\neq y\end{cases} \tag{2}$$

而且本文中所有相位标志以模 q 运算。

设 S 表示给定字母表 A 上的长为 q 的所有序列的集合。对 X、$Y\in S$，取

$$H(X)=\max_{0<\tau<q}\{H_{XX}(\tau)\} \tag{3}$$

$$H(X,Y)=\max_{0\leqslant\tau<q}\{H_{XY}(\tau)\} \tag{4}$$

$$M(X,Y)=\max\{H(X),H(Y),H(X,Y)\} \tag{5}$$

为探讨序列族的性能，提出如下最佳性判据：

（1）$X\in S$是最佳序列，如果对于所有$X'\in S$有$H(X)\leqslant H(X')$；

（2）X、$Y\in S$是最佳序列对，如果对于所有$X',Y'\in S$有$M(X,Y)\leqslant M(X',Y')$；

（3）一子集$F\subset S$是最佳序列族，如果F中每一对不同的序列是最佳序列对。

2 最佳序列及最佳序列族的构造

在这一节我们将证明图 2 结构得到的p^k进制序列具有最佳的汉明相关性能。图 1 结构是图 2 结构的一个特例。A.Lempel和H.Greenberger已证明：由图 1 结构所得到的序列具有最佳的汉明相关性能。

给定一素数 p 和一正整数 k，设

$$P=\{0,1,2,\cdots,p-1\}$$

$$P_k=\{0,1,2,\cdots p^k-1\}$$

$$P^k=\{(w_0w_1\cdots w_{k-1})\mid w_i\in P\}$$

P^k表示 P 上的 k 重字集。

存在一个从P^k到P_k的一一映射 σ，对于所有的 $w=(w_0w_1\cdots w_{k-1})\in P^k$对应有

$$w\sigma=\sum_{i=0}^{k-1}w_i\cdot p^i\in P_k \tag{6}$$

Lempel和Greenberger已经证明了如下定理：

定理 1 对于字母表 A 上的长为 q 的任何序列$Y=\{y(j)\}$有

$$H(Y)\geqslant\frac{(q-b)(q+b-m)}{m(q-1)} \tag{7}$$

其中m是字母表A的大小$|A|=m$，b是q模m的最小非负余数，而$H(Y)$如定义(3)。

定理 2　对于P_k上长为$q=p^n-1\geqslant 2$的任意一对序列X和Y，有

$$M(X,Y)\geqslant p^{n-k},\quad 1\leqslant k\leqslant n \tag{8}$$

由定理 1 和定理 2 知：如果序列的自相关以等式满足(7)式，则该序列为最佳序列；如果序列对的互相关以等式满足 (8) 式，则该序列对为最佳序列对；如果序列族F中任何一对不同序列都以等式满足(8)式，则F就是最佳序列族。

现在考虑一个P上长为q的序列$X=\{x(j)\}$，设$X(j,k)$表示X中第j个相继或非相继的k重：

$$[x(j+e_0)x(j+e_1)\cdots x(j+e_{k-1})]$$

这里$e_i<e_{i+1}$，且$0\leqslant e_i\leqslant n-1$(对任何$i$)。对于每一$w\in P^k$，设$u_X(w)$表示$X$中不同相位$j$的数目。这里$0\leqslant j\leqslant q$，满足$w=X(j,k)$。$u_X(w)$被称为$X$中$w$的重根数。应用映射$\sigma$于$X$中相继或非相继的$k$重，可得到$P_k$上长为$q$的序列$Y=\{y(j)\}$，而

$$y(j)=X(j,k)\sigma=\sum_{i=0}^{k-1}x(j+e_i)p^i,\quad 0\leqslant j<q \tag{9}$$

将X和Y间的关系(9)表示成$Y=X\sigma_k$，称序列Y为X的σ_k变换。例如二进制序列

$$\begin{aligned}X=\ &0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\\ &0\,1\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\\ &0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\end{aligned} \tag{10}$$

如果$y(j)=x(j)+x(j+1)\cdot 2+x(j+2)\cdot 4$，则$X$的$\sigma_3$变换为：

$$\begin{aligned}Y=\ &2\,5\,2\,5\,6\,3\,1\,4\,6\,3\,5\,6\,7\,3\,5\,6\,3\,5\,2\,1\,4\\ &2\,1\,4\,6\,7\,3\,1\,0\,4\,2\,5\,6\,7\,7\,3\,1\,4\,2\,5\,2\,1\\ &0\,4\,6\,3\,1\,0\,0\,4\,2\,1\underline{\,0\,0\,0\,}4\,6\underline{\,7\,7\,7\,}3\,5\end{aligned} \tag{11}$$

如果$y(j)=x(j)+x(j+2)\cdot 2+x(j+4)\cdot 4$，则$X$的$\sigma_3$变换为：

$$\begin{aligned}Y=\ &0\,7\,4\,3\,2\,5\,5\,2\,6\,5\,7\,2\,7\,5\,3\,6\,1\,3\,4\,1\,2\\ &4\,5\,6\,2\,3\,1\,5\,0\,6\,4\,7\,6\,3\,3\,5\,1\,6\,0\,3\,0\,5\\ &4\,2\,2\,1\,1\,4\,0\,2\,0\,1\,0\,4\,4\,6\,6\underline{\,7\,7\,}3\underline{\,7\,}1\,7\end{aligned} \tag{12}$$

为简单起见，并不失一般性，我们在例题中均假定$p=2$。

所提出的最佳序列的构造方法基于下述定理。

定理 3　设X为$GF(p)$上长为$q=p^n-1$的一个m序列，那么对所有k，$1\leqslant k\leqslant n$，X的σ_k变换是P_k上长为q的最佳序列。

证明　设$Y=\{y(j)\}$是一长为$q=p^n-1$的m序列$X=\{x(j)\}$的σ_k变换，这里$1\leqslant k\leqslant n$。设γ^τ表示循环移位运算，如下定义：

$$X\gamma^\tau=\{x(j)\}\gamma^\tau=\{x(j+\tau)\}$$

则有

$$Y\gamma^\tau=(X\sigma_k)\gamma^\tau=(X\gamma^\tau)\sigma_k$$

而

$$H_{YY}(\tau)=\sum_{j=0}^{q-1}h[y(j),y(j+\tau)],\quad 0\leqslant\tau<q$$

当$\tau=0$时，

$$H_{YY}(0)=\sum_{j=0}^{q-1}h[y(j),y(j)]=q$$

当$\tau\neq 0$时，

$$H_{YY}(\tau)=\sum_{j=0}^{q-1}h[X(j,k)\sigma,X(j+\tau,k)\sigma]$$

$X(j,k)\sigma=X(j+\tau,k)\sigma$，当且仅当$X(j,k)=X(j+\tau,k)$。定义$Z=X-X\gamma^{r}$，则$Z(j,k)=X(j,k)-X(j+\tau,k)$。因此$X(j,k)\sigma=X(j+\tau,k)\sigma$，当且仅当$Z(j,k)=0^{k}$。所以$H_{YY}(\tau)=u_{Z}(0^{k})$。

$\tau\neq0$时$Z=X-X\gamma^{r}$是m序列X的某一个位移序列，由m序列的性质知：

$$H_{YY}(\tau)=u_{Z}(0^{k})=u_{X}(0^{k})$$
$$=p^{n-k}-1,\quad \tau\neq0 \tag{13}$$

现回到定理1，如果$q=p^{n}-1$，$A=P_{k}$，$1\leqslant k\leqslant n$，则$m=p^{k}$且知$b=p^{k}-1$，代入(7)式得

$$H(Y)\geqslant\frac{(p^{n}-p^{k})(p^{n}-2)}{p^{k}(p^{n}-2)}=p^{n-k}-1 \tag{14}$$

由上面推导知，若X是一长$p^{n}-1$的m序列，则X的σ_{k}变换$Y=X\sigma_{k}$的异相自相关$H_{YY}(\tau)$恒为$p^{n-k}-1$。所以$H(X\sigma_{k})=\max\limits_{0<\tau<q}\{H_{YY}(\tau)\}=p^{n-k}-1$，即$X\sigma_{k}$以等式满足(14)式。由最佳性判据知$X$的$\sigma_{k}$变换是$P_{k}$上长为$q$的最佳序列。（证毕）

现在证明图2结构的序列族是最佳序列族。先用数学语言表述图2的构造方法：

设$X=\{x(j)\}$为GF(p)上长为$q=p^{n}-1$的一个m序列。对任意$j\in P_{n}$及$v\in P_{k}$，$1\leqslant k\leqslant n$，用$X_{v}(j,k)$代表X的第j个k重$X(j,k)$和k重$v\sigma^{-1}\in P^{k}$的逐项模p之和，即：

$$X_{v}(j,k)=X(j,k)+v\sigma^{-1} \tag{15}$$

对任何$v\in P_{k}$，$Y_{v}=\{y_{v}(j)\}$是P_{k}上长为$q=p^{n}-1$的序列，该序列的第j项由下定义：

$$y_{v}(j)=X_{v}(j,k)\sigma \tag{16}$$

从X到Y_{v}的复合变换可用$Y_{v}=X\sigma_{k}(v)$表示。

定理4 设$X=\{x(j)\}$是GF(p)上长为$q=p^{n}-1\geqslant2$的一个m序列，对每一k，$1\leqslant k\leqslant n$，p^{k}个序列$Y_{v}=X\sigma_{k}(v)$，$v\in P_{k}$的集合是一个最佳序列族，而且F中每一序列本身也是最佳的。

证明 考虑一对序列Y_{r}，$Y_{s}\in F$，有

$$H_{Y_{r}Y_{s}}(\tau)=\sum_{j=0}^{q-1}h[y_{r}(j),y_{s}(j+\tau)]$$

因为映射σ是一一对应的，$y_{r}(j)=y_{s}(j+\tau)$当且仅当$X_{r}(j,k)=X_{s}(j+\tau,k)$，或等效地，当且仅当$X(j,k)-X(j+\tau,k)=s\sigma^{-1}-r\sigma^{-1}$，取$Z=X-X\gamma^{r}$和$w=s\sigma^{-1}-r\sigma^{-1}$，上式等效为

$$Z(j,k)=w$$

由此得到

$$H_{Y_{r}Y_{s}}(\tau)=u_{Z}(w)$$

若$r=s$，则$w=0^{k}$。情况和定理3完全一样。故知每一序列$Y_{r}\in F$本身是最佳的。

假设$r\neq s$，则$w\neq0^{k}$。若$\tau=0$，则Z是长为q的全0序列，显然Z中w的重根数为0，即

$$H_{Y_{r}Y_{s}}(0)=0,\quad r\neq s \tag{17}$$

若$\tau\neq0$，则$Z=X-X\gamma^{r}=X\gamma^{\theta}$，而$X\gamma^{\theta}$中$w$的重根数与$X$中的一样，为$p^{n-k}$：

$$H_{Y_{r}Y_{s}}(\tau)=u_{X}(w)=p^{n-k},\quad r\neq s,\ 0<\tau<q \tag{18}$$

由(17)式和(18)式知，对于F中任何一对不同的序列有

$$H(Y_r,Y_s)=p^{n-k} \tag{19}$$

已经证明，每一 $Y_v\in F$ 本身是最佳序列，且 $H(Y_r)=H(Y_s)=p^{n-k}-1$。因此 $M(Y_r,Y_s)=p^{n-k}$。由定理 2 知序列族 F 是最佳的。

作为一个例子，考虑(10)式的二进制 m 序列的 $\sigma_3(v)$ 变换的 8 个序列的集合 F，取 $y(j)=x(j)+x(j+2)\cdot 2+x(j+4)\cdot 4$，8 个序列如下：

Y_0：如(12)式

$Y_1=$ 1 6 5 2 3 4 4 3 7 4 6 3 6 4 2 7 0 2 5 0 3
5 4 7 3 2 0 4 1 7 5 6 7 2 2 4 0 7 1 2 1 4
5 3 3 0 0 5 1 3 1 0 1 5 5 7 7 6 6 2 6 0 6

$Y_2=$ 2 5 6 1 0 7 7 0 4 7 5 0 5 7 1 4 3 1 6 3 0
6 7 4 0 1 3 7 2 4 6 5 4 1 1 7 3 4 2 1 2 7
6 0 0 3 3 6 2 0 2 3 2 6 6 4 4 5 5 1 5 3 5

……

$Y_7=$ 7 0 3 4 5 2 2 5 1 2 0 5 0 2 4 1 6 4 3 6 5
3 2 1 5 4 6 2 7 1 3 0 1 4 4 2 6 1 7 4 7 2
3 5 5 6 6 3 7 5 7 6 7 3 3 1 1 0 0 4 0 6 0

容易验证，$H(Y_v)=7$，$0\leqslant v\leqslant 7$；且有 $M(Y_r,Y_s)=8$，对所有 $r,s\in\{0,1,2,\cdots,7\}$，$r\neq s$。

3　序列的游程：Hop-and-Stay问题

序列的最长游程对应于跳频图样在某个频隙上的最长停留时间。为了抗截获和转发式干扰，总希望跳频序列的最长游程越小越好。

定理 5　设 X 为GF(p)上长为 $q=p^n-1$ 的一个 m 序列，X 的 $\sigma_k(v)$ 变换 Y_v 的最长游程的极大值为 $n-k+1$。

证明　X 的 $\sigma_k(v)$ 变换 Y_v 的最长游程等于 X 的 σ_k 变换 Y 的最长游程，只要证明 Y 的最长游程的极值为 $n-k+1$ 即可。用反证法。

已经知道：当 $X(j,k)$ 表示 X 中第 j 个相继的 k 重时，即是说以寄存器的 k 个相邻级控制频合时，X 的 σ_k 变换 Y 的最长游程达到 $n-k+1$。假设最长游程的极大值不是 $n-k+1$，即大于 $n-k+1$，不妨假定为 $n-k+2$。考虑连续 $n-k+2$ 个码元所对应的矢量 $X(j,k)$，$1\leqslant j\leqslant n-k+2$，作如下矩阵：

$$\begin{bmatrix} x(1+e_0) & \cdots & x(1+e_{i-1}) & x(1+e_i) & \cdots & x(1+e_{k-1}) \\ x(2+e_0) & \cdots & x(2+e_{i-1}) & x(2+e_i) & \cdots & x(2+e_{k-1}) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x(n-k+2+e_0) & \cdots & x(n-k+2+e_{i-1}) & x(n-k+2+e_i) & \cdots & x(n-k+2+e_{k-1}) \end{bmatrix}$$

其中行矢量即为 $X(j,k)$，$1\leqslant j\leqslant n-k+2$.

若 $X(1,k)=X(2,k)=\cdots=X(n-k+2,k)$，对应跳频序列 Y 中存在长为 $n-k+2$ 的游程，则矩阵中每列的元相等，即 $x(1+e_i)=x(2+e_i)=\cdots=x(n-k+2+e_i)$，$0\leqslant i\leqslant k-1$。如果证明相邻两列元素中存在相位标志相同的码元，则这两列元素相等。任取相邻两列，如第 i 列和第 $i+1$ 列，比较第 i 列最后的元 $x(n-k+2+e_{i-1})$ 和第 $i+1$ 列的第一个元 $x(1+e_i)$ 的位标：

因 $e_i \leqslant e_{i-1}+n-k+1$

故 $1+e_i \leqslant n-k+2+e_{i-1}$

这说明第 i 列和第 $i+1$ 列有相位相同的元，推知这两列所有元均相等。因为这相邻两列的选取是任意的，最终得出上述矩阵中所有的元均相等，即 $x(l)=$常数，$1+e_0 \leqslant l \leqslant n-k+2+e_{k-1}$，而 $e_{k-1} \geqslant k-1+e_0$，所以 $n-k+2+e_{k-1} \geqslant n+1+e_0$，推出在 n 级 m 序列中存在长为 $n+1$ 以上的游程。显然，这与 m 序列的游程特性相矛盾。故知假设是错误的。定理得证。

定理 6 设 X 为 GF(p) 上长为 $q=p^n-1$ 的一个 m 序列，$X(j,k)$ 表示 X 中第 j 个相继或非相继的 k 重：$[x(j+e_0)\ x(j+e_1)\ \cdots x(j+e_{k-2})\ x(j+e_{k-1})]$。仅当如下情况时，$X$ 的 $\sigma_k(v)$ 变换 Y_v 的最长游程才可能达到极大值 $n-k+1$：

1) 当 $e_i=i+e_0$，$0 \leqslant i \leqslant t-1$ 而 $e_i=n-(k-i)+e_0$，$t \leqslant i \leqslant k-1$ 时，序列 Y_v 可能出现长为 $n-k+1$ 的游程。是否出现与 m 序列 X 有关；

2) 当 $e_i=i+e_0$，$0 \leqslant i \leqslant k-1$ 时，序列 Y_v 一定会出现长为 $n-k+1$ 的游程 $p-1$ 个。

证明 考虑如下矩阵

$$\begin{bmatrix} x(1+e_0) & \cdots & x(1+e_{t-1}) & x(1+e_t) & \cdots & x(1+e_{k-1}) \\ x(2+e_0) & \cdots & x(2+e_{t-1}) & x(2+e_t) & \cdots & x(2+e_{k-1}) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x(n-k+1+e_0) & \cdots & x(n-k+1+e_{t-1}) & x(n-k+1+e_t) & \cdots & x(n-k+1+e_{k-1}) \end{bmatrix}$$

假设上述 $n-k+1$ 个码矢 $X(j,k)$ 相等，则矩阵中每列的元相等。比较任意相邻两列中前列的最后一元与后列的最前一元的位标，如比较 $x(n-k+1+e_{t-1})$ 和 $x(1+e_t)$ 的位标。

因 $e_t \leqslant e_{t-1}+n-k+1$，分两种情况考虑：

1) $e_t=e_{t-1}+n-k+1$

由 $e_{t-1} \geqslant t-1+e_0$，推出 $e_t \geqslant n-(k-t)+e_0$

由定义有 $e_t \leqslant n-(k-t)+e_0$

故得出

$$e_t=n-(k-t)+e_0$$

$$e_{t-1}=t-1+e_0$$

这意味着：$e_i=i+e_0$，$0 \leqslant i \leqslant t-1$；

$e_t=n-(k-i)+e_0$，$t \leqslant i \leqslant k-1$

由此继续推得矩阵中前 t 列中所有元相等，后 $k-t$ 列中所有元为另一常元：

$$x(l)=\text{元}1,\quad 1+e_0 \leqslant l \leqslant n-k+t+e_0$$

$$x(l)=\text{元}2,\quad n-k+t+1+e_0 \leqslant l \leqslant 2n-k+e_0$$

这种情况在 n 级 m 序列中可能出现也可能不出现。定理6.1得证。

2) $e_t < e_{t-1}+n-k+1$

这时有 $e_t \leqslant e_{t-1}+n-k$，得 $1+e_t \leqslant n-k+1+e_{t-1}$。由此推得第 t 列元素等于第 $t+1$ 列元素。继续比较任意其它两列元素时，如果不相等，则归入上述1)中的情况。直到比较完所有的相邻列，得到矩阵中所有的元均相等；

$$x(l)=\text{常元},\quad 1+e_0\leqslant l\leqslant n-k+1+e_{k-1}$$

由$e_{k-1}\geqslant k-1+e_0$，推得$n-k+1+e_{k-1}\geqslant n+e_0$。由$m$序列的游程特性知，$e_{k-1}$的值只能取$k-1+e_0$，这意味着　$e_i=i+e_0$，$0\leqslant i\leqslant k-1$。

因为m序列中一定会出现长为n的游程$p-1$个，所以当$e_i=i+e_0$，$0\leqslant i\leqslant k-1$时，序列$Y_s$一定会出现$p-1$个长为$n-k+1$的游程。　　证毕

定理5和6是很有意义的。它指出了最佳跳频序列族的最长游程的极大值，表明A.Lempel和H.Greenberger提出的模型存在最严重的Hop-and-Stay问题，并为避免出现最差情况指明了方向：使用k个非相邻级去控制频合（这里假定第1级和第n级亦为相邻级）。

比较序列(11)和序列(12)中的最长游程，(11)中为4，(12)中仅为2。笔者对$n\leqslant 10$，$k=3$的情况进行了计算机模拟，表明使用k个非相邻级时最长停留时间减少一半左右，大大改善了抗截获性能。

4　结　束　语

当$k=n$时，$q=p^n-1$，$H(Y)=0$且$M(Y_r,Y_s)=1$。具有p^n个序列的跳频序列族是GF(p^n)上一阶R—S码的子集，它已广泛应用于跳频系统，尤其是具有自同步技术的跳频系统。

当$k<n$时，$q=p^n-1$，$H(Y)=p^{n-k}-1$，$M(Y_r,Y_s)=p^{n-k}$，具有p^k个跳频序列。使用k个非相邻级控制频合，可部分地解决使用k个相邻级时存在的Hop-and-Stay问题，并具有更大的密钥量。

感谢周兆祺教授、李情与副教授、饶世林副教授的指导和帮助。

参　考　文　献

[1] A.Lempel and H.Greenberger. Families of Sequences with Optimal Hamming Correlation Properties. IEEE Trans. on IT—20,1974:(1):90～94

[2] D.V.Sarwate and M.B.Pursley. Hopping Patterns for Frequency—Hopped Multiple—Access Communication. ICC'78:7(4):1～3

[3] M.K.Simon et al. Spread Spectrum Communications Computer Science Press, Inc., 1985:1

[4] S.W.Golomb. Shift Register Sequences. San Francisco: Holden—Day, 1967

Families of Frequency-Hopping Sequences with Optimal Hamming Correlation Properties

Mei Wenhua Chen Xianfu

Abstract

Families of p^k-ary sequences with small Hamming crosscorrelation are required for hopping patterns in asynchronous frequency-hopping spread-spectrum multiple-access communication systems. Lower bounds on the out-of-phase auto correlation and on the crosscorrelation of sequences of given length and alphabet size are derived in [1], and a method of constructing families of sequences that uniformly realize these bounds is presented as well. In this paper, a commonest method of constructing families of frequencyhopping sequences with optimal Hamming correlation properties is presented, taking the method in [1] as its special case. By driving the frequency synthesizer from k inconsecutive stages Tather than from k consecutive stages, we can partially solve the Hop-and-Stay problem existing in [1].

Key words: Communication, Frequency-hopping, Sequences

Research on Periodicity of Input and Output of S-boxes in DES

Xiao Rong

Abstract

There are not any general conclusions about periodicity of DES when it is used in stream cipher system. The author discusses this problem and gives a low bound for period of S-boxes.

Key words: Cipher communication, DES method, periodi city