基于仿射密码原理的差分跳频频率转移函数研究

易大进1,　杨千里2

(1. 空军工程大学电讯工程学院，陕西西安 710077；2. 总参通信部，北京 100840)

摘要：差分跳频是一种新型的跳频通信技术。基于仿射密码的加密原理，构造了一种差分跳频的频转移函数。该函数具有构造简单，便于密钥管理和控制，而且具有密钥量大的特点。最后通过实例说明了由该函数产生的跳频图案具有良好的均匀性，从而系统具有较强的隐蔽性和抗破译性。

关键词：差分跳频；仿射密码；跳频图案

中图分类号：TN914.41　　文献标识码：A　　文章编号：1009-3516(2005)03-0050-03

差分跳频是一种新型的跳频通信技术，具有与传统跳频技术完全不同的技术体制。它利用前后频率的相关性来携带信息，以高跳速来提高数据率，跳速可高达5000跳/s，数据率可达19.2 kb/s[1,2]。

差分跳频的频率跳变规律类似于编码理论中的差分编码，基本原理是：当前跳的频率值f_n由上一跳的频率值f_{n-1}和当前时刻的数据符号X_n共同决定，每跳的传输信号都是取自跳频频率集中的一个单频信号。可由式$f_n = G(f_{n-1}, X_n)$描述，式中G是频率转移函数，它集跳频图案、信息调制与解调等功能于一体，由它决定频率跳变的规律，可以看作一个有向图。有向图中的每个节点代表频率集中的一个频点，全部节点即为频点集。每个节点分出$f=2^P$个分叉，P代表每跳携带的数据比特数，f为扇出系数，每个分叉与当前的数据符号一一对应。在发送端，待发送的数据比特流被分为每P个比特一组，根据G函数从有向图的某一个节点开始，沿着按照这些比特组和前次频点确定的有向图路径，依次访问有向图的节点，从而产生待发射的频率系列。在收端，通过数字化宽带接收，经特定的频率检测算法，确定f_{n-1}和f_n，由G函数的逆变换即可恢复出发送端的数据信息X_n。

1　仿射密码原理

设A表示明文字母表，内有N个“字母”或“字符”。因此可以将A抽象地表示为一个整数集$\mathbf{Z}_N = \{0,1,\cdots,N-1\}$。在加密时常将明文消息划分成长为$L$的明文组，以$m=(m_0,m_1,\cdots m_{L-1})$表示，$m$是定义在$\mathbf{Z}_N^L$上的随机变量，$\mathbf{Z}_N^L$是$z_n$上的$L$维矢量空间。明文空间$M=\{m, m\in\mathbf{Z}_N^L\}$。

令A'表示密文字母集，内含有N'个字母，可用整数集$\mathbf{Z}_{N'}=\{0,1,\cdots,N'-1\}$表示。密文组为$c=(c_0, c_1,\cdots,c_{L'-1})$，$c$是定义在$L'$维矢量空间$\mathbf{Z}_{N'}^{L'}$上的随机变量。密文空间$C=\{c, c\in\mathbf{Z}_{N'}^{L'}\}$。

加密变换是由明文空间到密文空间的映射：

$$f: m\rightarrow c \qquad m\in M, c\in C \tag{1}$$

假定函数f是一一映射，其逆映射为f^{-1}。因此，给定密文组c，有且仅有一个对应的明文组m。

$$f^{-1}(c)=f^{-1}(f(m))=m \qquad m\in M、c\in C \tag{2}$$

加密变换通常是在密钥控制下变化的，即

$$c=f(m,k)=E_k(m) \tag{3}$$

收稿日期：2004-11-12
作者简介：易大进(1976-)，男，湖南平江人，博士生，主要从事军事通信理论与基础研究；
杨千里(1933-)，男，江苏无锡人，教授，博士生导师，主要从事军事通信、卫星通信研究.

式中,$k \in \kappa$,κ 为密钥空间。一个密码系统就是在f作用下由 $\mathbf{Z}_N^L$ 的映射。当 $L=1$ 时,称为流密码,当 $L>1$ 时,称为分组密码。

1.1 加法密码

加法密码是将明文字母表中字母位置下标与密钥 k 进行模 N 加法运算的结果作为字母位置下标,相应的字母即为密文字母,在这里 $A=A'$,即明文和密文由同一字母表构成。其加密变换为

$$E_k(i)=(i+k) \mod N=j \qquad 0 \leqslant i,j<N \tag{4}$$

$$\kappa=\{k \mid 0 \leqslant k<N \mid\} \tag{5}$$

加法密码的密钥数为 N。

1.2 乘数密码

乘数密码又称采样密码,其密文字母表是将明文字母表按下标每隔 k 位取出一个字母排列而成(字母表首尾相接)。其加密变换为

$$E_k(i)=ik \mod N=j \qquad 0 \leqslant i,j<N \tag{6}$$

当且仅当 GCD(k,N) =1(GCD 表示 k 与 N 的最大公约数),即 k 与 N 互素时才是一一对应的。此时乘数密码的密钥数为 $\varphi(N)-1$,$\varphi(\cdot)$ 为欧拉 Totient 函数,$\varphi(N)$表示小于 N 且与 N 互素的整数个数。

1.3 仿射密码

仿射密码是在加法密码与乘数密码的基础上进行组合而生成的一种流密码。其加密变换为

$$E_k(i)=(ik_1+k_0) \mod N=j \qquad 0 \leqslant i,j<N \tag{7}$$

其中 $k_1,k_0 \in \kappa$,且 k_1满足 GCD(k_1,N) =1。[k_1,k_0]表示密钥,仿射密码的密钥数为 $N\varphi(N)-1$ 。

2 频率转移算法

差分跳频图案与传统跳频图案具有明显的不同,前者是基于频率转移函数所确定的有向图,而后者是基于非线性伪随机码。文献[5]提出了差分跳频频率转移函数的一种构造方法,通过分析其构造原理,实质上是基于加法密码的原理。因此在频率集比较小的情况下,其密钥量非常有限,在一定时间内密码分析员通过穷举法即可破译。本文在文献[5]的基础上,并利用仿射密码的原理构造一种频率转移函数,由于密钥量增加,因此在相同条件下,增加了密码分析员破译的难度,从而增强了系统的抗破译性。设差分跳频通信系统的频率集为 $F=\{f_n,n=0,1,\cdots,N-1\}$,每跳携带的比特数为 P,$f=2^P$为有向图中的扇出系数。信源符号集合为 $X=\{X_n,n=0,1,\cdots,f-1\}$ 。令前一跳的频率为 f_i,当前跳的频率为 f_j,则按照仿射密码原理,j 可由下式确定

$$j=[ik+\phi(k_0)] \mod N \tag{8}$$

其中,$k_0 \in X$,$\phi(k_0)$为 $1 \times f$ 维数组,$\phi(k_0)$中的元素取从到 1 到 $N-1$ 的整数,且两两互不相等,其中至少有一个与 N 互质,同时 $\phi(k_0)$中有两个元素的差与 N 互质。k 满足 GCD(k,N) =1。因此,由该算法确定的频率转移函数具有一一对应性。由式(8)并与文献[5]比较,可知本文所介绍的算法具有较多的密钥量。

类似于文献[5],可以证明:①当信源为离散无记忆信源时,由(8)式确定的频率转移过程是一个马尔可夫过程,并且是马尔可夫链;②在充分多步转移后,系统以相同的概率 $1/N$ 使用各个频点。

3 算法检验

假设 $N=8$,$P=1$,信源为二进制无记忆信源,且符合 0、1 出现的概率分别为 0.4、0.6,$k=3$, $\phi=[2,3]$,则根据式(8)可得相应的频率转移概率矩阵为

$$P=\begin{bmatrix}0 & 0 & 0.4 & 0.6 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0.4 & 0.6 & 0\\ 0.4 & 0.6 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0.4 & 0.6 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0.6\\ 0 & 0.4 & 0.6 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0.4 & 0.6 & 0 & 0\\ 0.6 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4\end{bmatrix};\quad P^{27}=\begin{bmatrix}0.1250 & \cdots & 0.1250\\ \vdots & & \vdots\\ 0.1250 & \cdots & 0.1250\end{bmatrix}$$

可见,27 步转移矩阵中的各项已经与理论值非常一致。改变频率集的大小、每跳携带的数据比特数、k 以及 $\phi(k_0)$,可得类似的结果,从而说明由(8)式所构造的频率转移函数的正确性。

4 结束语

差分跳频是一种全新的跳频通信体制,其频率转移函数的性能好坏,决定了差分跳频通信系统性能的优劣。本文基于仿射密码的加密原理,构造了差分跳频的一种频率转移函数。该函数具有构造简单,便于密钥管理和控制,同时具有密钥量大的特点。最后通过实例说明了经常充分多步转移后,系统以相同的概率使用各个频点,从而具有较强的隐蔽性和抗破译性。

参考文献:

[1] Herrick D L, Lee P K. Correlated Frequency Hopping: An Improved Approach to HF Spread Spectrum Communications[A]. IEEE Proceedings of The Tactical Communications Conference 1996[C]. 1996:319 - 324.

[2] Herrick D L, Lee P K. A New Reliable High Speed HF Radio[A]. IEEE Military Communications Conference MILCOM96[C]. 1996,3:684 - 690.

[3] Ma Yusong, Liu Kaihua. A Design of Differential Frequency Hopping Pattern[A]. IEEE MILCOM[C]. 2001:820 - 823.

[4] 王育民,刘建伟. 通信网的安全 - 理论与技术[M]. 西安:西安电子科技大学出版社,1999.

[5] 杨裕亮,何遵文,匡镜明. 差分跳频系统的转移函数研究[J]. 通信学报,2002,23(4):103 - 108.

(编辑:门向生)

Study of DFH Frequency Transition Function Based on the Principle of Affine Cipher

YI Da - jint, YANG Qian - li2

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China; 2. Dept. of Communication, Headquarters of the General Staff, Beijing 100840, China)

Abstract: Differential frequency hopping (DFH) is a kind of new frequency hopping (FH) technique. Based on the encryption principle of affirie cipher, a frequency transition function of DFH is designed. This function is convenient for realization, easy in controlling the secret keys and also has more secret keys. The final results of experiment prove that the frequency hopping pattern based on this function is good in uniformity, so the system has high complexity and strong anti -attack features.

Key words: differential frequency hopping; affine cipher; frequency hopping pattern