高安全 *G* 函数算法研究

陈芮[1]，李赞[1,2]，石嘉[1]，关磊[1]
（1. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 西安中电科西电科大雷达技术协同创新研究院有限公司，陕西 西安 710071）

摘 要：差分跳频技术克服了传统跳频抗跟踪干扰能力较弱的问题。*G* 函数算法决定了差分跳频序列的性能，也直接影响差分跳频系统的性能。然而随着无线系统的复杂化，如大容量的差分跳频系统，传统序列的应用受到严重挑战。因此，为了提升系统的安全性，提出了一种基于混合加密算法的 *G* 函数构造，证明了加密算法和 *G* 函数的等价性并分析了混合算法的安全性。仿真结果表明，新的 *G* 函数生成的序列性能优异，可以大幅度提升系统性能。

关键词：差分跳频序列；密码算法；安全性；随机性；复杂度
中图分类号：TN925
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2019.00100

Research on high security *G* function algorithm

CHEN Rui[1], LI Zan[1, 2], SHI Jia[1], GUAN Lei[1]
1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
2. Collaborative Innovation Center of Information Sensing and Understanding, Xi'an 710071, China

Abstract: The differential frequency hopping (DFH) overcomes the limitation of frequency hopping and improves the ability to resist tracking interference. The *G* function determines the DFH sequence and directly affects the performance of DFH communication systems. However, with the complication of wireless communication system such as large capacity DFH network, which poses huge challenges to the use of the number theory based and chaos theory assisted sequence. As a result, in order to improve the security of the system, the novel *G* function construction was proposed with the aid of hybrid encryption algorithm and the security of hybrid algorithm was analyzed. Moreover, the equivalence principle of *G* function algorithm and the encryption algorithm was proved. The simulation results show that the DFH sequence generated by the new *G* function has excellent performance and the performance of the DFH systems is improved greatly.

Key words: differential frequency-hopping sequence, cryptographic algorithm, security, randomness, complexity

1 引言

随着信息技术的飞速发展，无线通信给人们的生活带来了极大便利。由于无线信道的开放性，使得用户在数据传输过程中遇到很多安全问题，如窃听、手机用户信息泄露等，这对未来无线通信发展是一个巨大的挑战。因此，研究无线通信的数据和信息安全是必要的。

传统加密技术是针对数据内容的保护，其核心在于不断提高破解密码的计算量，缺点在于保密基础不牢靠，而且主要用于网络层及以上层，与物理层独立。同时，之前的研究中假设加密和解密的信道是完美无差错传输。随着 Wyner 提出窃听信道的数学模型及无线通信的广泛应用，大

收稿日期：2018−09−18；**修回日期：**2018−10−29
基金项目：国家自然科学基金资助项目（No.61631015）；陕西省重点科技创新团队计划（No.2016KCT-01）
Foundation Items: The National Natural Science Foundation of China (No.61631015), The Key Scientific and Technological Innovation Team Plan of Shaanxi Province (No.2016KCT-01)

多数的研究开始从物理层角度研究通信安全问题。利用物理信道的唯一性和互易性，实现信息加密、产生密码以及辨识合法用户等。因此，物理层安全可以作为上层安全的补充出现，极大地增强了整个系统的安全性能。

目前，已有许多物理层安全技术[1-2]，如发射信号方式安全技术和扩频通信技术[3-4]、信道编码加密技术和调制方式加密技术等。由于具有优异的抗干扰能力、较高的频谱利用率等优点[5]，扩频通信技术被广泛应用于各种无线通信系统中。扩频通信可分为直接序列扩频、跳频等基本方式，通过直接序列扩频方式扩频后，信号功率分散在很宽的频带内，从而隐藏在噪声中；通过跳频方式扩频后，信号频率在较宽的频率范围内变化，以躲避的方式对抗通信干扰。然而，传统跳频技术无法抵抗跟踪干扰，且窃听者捕获信号的能力越来越强。1995 年美国 Sanders 公司研发出一种相关跳频增强型扩展频谱（Chess）电台，受到了广泛关注[6-7]。该电台的核心技术为差分跳频，是一种新型的跳频技术，其跳频速率快，有效提高了高频通信数据的传输速率和频谱利用率，同时能够抵抗跟踪干扰并克服多径衰落[8-10]。差分跳频归因于一种 G 函数算法，与传统跳频不同，G 函数本身具有调制/解调功能。即使窃听者捕获到信号，由于无法预知频率之间的关联性，则不能正确解调传输的信息。因此，G 函数算法的研究对整个差分跳频系统至关重要。

当前，针对 G 函数的构造有许多方法，如 Chen 等[11-12]基于线性同余理论构造 G 函数，该方法简单、易实现，但是随机性较差。Zhou 等[13-14]基于模糊和混沌理论构造 G 函数，生成的差分跳频序列具有较大的线性复杂度，但是均匀性较差。Zhu 等[15]提出了一种时频扰动 G 函数，改进了加性高斯白噪声信道的抗部分频带干扰性能，但是该方法需要发送方和接收方同步。Bao 等[16-19]研究了基于密码学算法的 G 函数，该方法生成的序列具有良好的均匀性和随机性，但没有具体分析其安全性。若算法的安全强度不够，则序列及其系统性能将受到严重影响。随着信息技术的不断发展，万物互联使用户之间（物与物之间）交换信息越来越频繁。如大容量的跳频网络，多用户通信如图 1 所示，当用户数逐渐增加时，信息量也急剧增加，其中，需分配的密钥量为 $n(n-1)/2$（n 为用户数），加大了系统开销。同时，传统的对称密码算法在分布式网络中无法完全保证信息传输的安全性，密钥的管理和分配变得困难，严重影响了差分跳频系统的安全性。因此，考虑非对称密码算法和对称密码算法各自的优点，结合两种密码系统，本文提出了一种基于混合密码算法的 G 函数，进一步解决了大规模跳频网络中密钥信息的安全传输问题，新构造的序列综合性能优异。其中，良好的均匀性保证了频率使用的最大化，提高了差分跳频通信的频谱利用率，较高的复杂度和安全性、较好的随机性保证了差分跳频系统具有较强的抗破译能力。

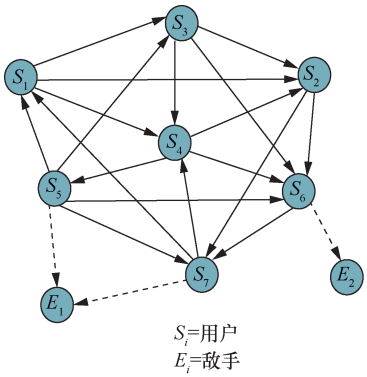


图 1　多用户通信

2　系统模型

由于电离层的抗毁性，近年来高频通信取得了一系列的突破和发展。许多国家和公司陆续研究和推出了一些性能优良的设备和系统，如美国的 Chess 电台，其中，差分跳频技术极大地解决了高频通信速率受限的问题。本节主要描述差分跳频系统及差分跳频序列原理。

2.1　差分跳频系统原理

常规跳频通信收/发双方通过不断改变载波频率，以躲避的方式对抗通信干扰。与常规跳频不同，差分跳频没有传统的数字调制过程，而是通过在相邻频率间引入相关性来调制信息，因此，差分跳频也称为相关跳频，差分跳频系统原理如图 2 所示。在发送端，数据经过 G 函数映射为频率，即差分跳频序列由 G 函数决定，而不受伪随机码控制。然后，差分跳频序列控制频率合成器和本地振荡器合成载波频率，形成差分跳频信号。在接收端，采用基于 FFT 的信号检测技术和频率

序列译码技术对检测到的差分跳频序列进行数据信息解调。

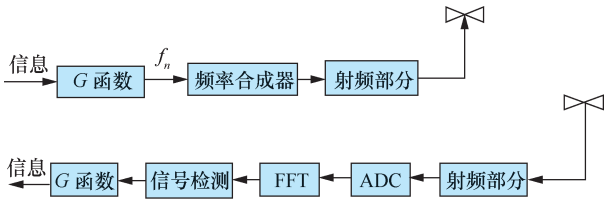


图 2 差分跳频系统原理

2.2 差分跳频序列原理

由差分跳频系统原理可知，差分跳频序列的性能直接决定了整个差分跳频系统的性能。差分跳频序列由 G 函数生成，因此，G 函数设计的好坏直接影响系统性能。首先介绍 G 函数，其数学表达式如下

$$f_n = G(f_{n-1}, X_n) \tag{1}$$

$$X_n = G^{-1}(f_{n-1}, f_n) \tag{2}$$

由式(1)、式(2)可知，当前频率 f_n 由上一跳频率 $f_{n\text{-}1}$ 和当前信息符号 X_n 共同决定。因此，差分跳频可以看作是一种以频率的变化携带信息的调制方式，即 G 函数具备数据调制/解调功能。同时，由于信息符号的随机性，理论上由 G 函数生成的跳频图案具有无限长的周期，保密性较好。

差分跳频的频率转移过程可以看作是有向图，G 函数算法的有向图如图 3 所示。每个频率可看作一个状态，每个状态可选择的分支数 $N = 2^B$，B 为每跳携带的比特数，如 Chess 电台中 $B \leqslant 4$，每个分支上标记有传输的信息符号。当 $B = 2$ 时，每个状态上有 4 个分支(00,01,10,11)，将比特流作为每 B bit 的符号发送，然后形成符号流，并根据有向图生成相应的频率序列。

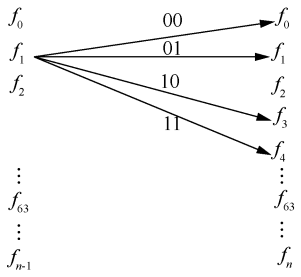


图 3 G 函数算法的有向图

差分跳频序列具有高速数据传输能力，即每跳比特数越多，则数据传输速率越高，从而提高了高频通信的质量。

3 基于混合加密算法的 G 函数

对称密码算法具有计算速度快、开销低等优点，但是密钥的管理和分配困难。非对称密码算法解决了密钥的管理问题，但是其计算速度非常慢。因此，在大容量用户的差分跳频系统中，为了提高系统安全性，结合两种密码系统的优点，设计基于混合加密算法的 G 函数。具体原理是采用非对称密码算法加密用户的秘密密钥，采用对称密码算法加密传输的信息。

3.1 等价设计原理

为了满足高性能差分跳频序列的需求，提出了差分跳频序列设计的基本理论。参考文献[20]得出了传统跳频与密码算法的等价性，而与传统跳频图案不同，差分跳频图案没有时钟 TOD 的参与，直接由 G 函数决定。

定理 设 g_1 为差分跳频的 G 函数，$F = \{f_i \mid i = 0,1,\cdots,N\}$ 为 G 函数生成的差分跳频序列集，即有 $f_{i+1} = g_1(f_i, x_i)$。同时，设 g_2 为加密算法，密文空间 $C = \{c_i \mid 0,1,\cdots,M\}$ 由 g_2 生成，即有 $c_i = g_2(p_i, k_i)$，其中，p_i 为明文，k_i 为子密钥，则 g_1 和 g_2 的设计是等价的。

证明 主要从两方面分析，即输入、输出参数的等价和运算规则的等价。

1) 输入、输出参数等价

在差分跳频系统中，假设初始频率 f_0 为随机选取，所传输的数据为 x_A 和 x_B，即有 $f_A = g_1(f_0, x_A)$ 和 $f_B = g_1(f_0, x_B)$。在生成的频率号遍历区间[0,N−1]的所有整数前，$x_A \neq x_B \Rightarrow f_A \neq f_B$。同时，$\forall f_i \in F$，存在 f_j和x_j 使得 $f_i = g_1(f_j, x_j)$，即 g_1 可看作双射。同理，在密码系统中，由于分组密码算法是确定性算法，采用相同密钥加密某些明文。设明文空间为 $P = \{p_i \mid i = 0,1,\cdots,M\}$，即 $\forall p_A,\ p_B \in P$，$c_A = g_2(p_A,\ k_0)$，$c_B = g_2(p_B, k_0)$，$c_A = c_B \Rightarrow p_A = p_B$。$\forall c_i \in C$，存在 p_i 和 k_i 使得 $c_i = g_2(p_i, k_i)$，即 g_2 也可看作双射。因此，g_1 和 g_2 的输入、输出参数等价。

2) 运算规则等价

在差分跳频系统中，G 函数要求必须可逆，即 $x_i = g_1^{-1}(f_{i-1}, f_i)$，且 G 函数的运算主要是较容易的可逆运算。在对称密码系统中，由于采用分

组密码算法加密和解密操作相似，其中，解密算法的密钥 k' 为加密算法密钥 k 的重排，即 $p=g_2^{-1}(c,k')$。故两个系统的运算规则可看作等价，因此，g_1 和 g_2 的设计等价。

3.2　G 函数构造原理

采用对称密码算法 GOST[21]和非对称密码算法 RSA[22]构造 G 函数，首先介绍两种算法的基本原理。GOST 算法是 64 位分组，密钥长度为 256 bit，迭代次数为 32 次。由于简化了 S 盒的设计，实现了效率和安全性之间的平衡。同时，GOST 算法是典型的 Feistel 结构，GOST 算法流程如图 4 所示。轮函数 f 包括 3 个部件：模 2^{32} 次加法运算、S 盒和循环左移运算。每次加密前，将明文等分成左、右两个部分，右部分与子密钥经过轮函数 f 变换后与左部分异或形成下一轮的右部分，而上一轮的右部分形成下一轮的左部分，具体描述如下

$$L_i = R_{i-1} \tag{3}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{4}$$

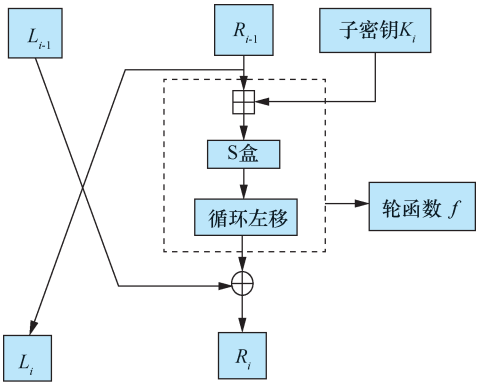


图 4　GOST 算法流程

RSA 算法是现今较流行的非对称密码算法，加密和解密采用不同的密钥，加密密钥公开，解密密钥则被合法接收者保留，且从加密密钥推导解密密钥的计算困难。RSA 算法的安全性基于一个简单的事实，即两个大素数相乘是容易的，而分解一个大整数是困难的。RSA 算法流程如图 5 所示，发送者随机选择两个大素数 p 和 q，且计算 $n=pq$，然后选择两个正整数 e 和 d，使得 $ed \equiv 1 \bmod(\varphi(n))$，$\varphi(n)$ 为 n 的欧拉函数。(n,e) 作为公开的加密密钥 PK，(p,q,d) 则作为解密密钥 SK，加密和解密计算式描述分别如式(5)和式(6)所示，其中，m 和 c 分别为明文和密文信息。

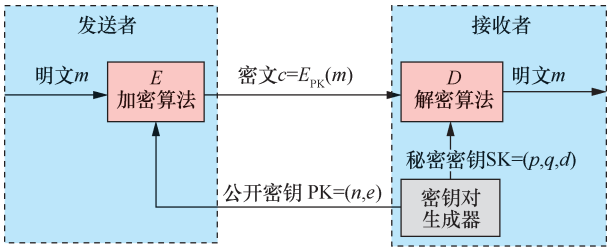


图 5　RSA 算法流程

$$c = m^e \bmod(n) \tag{5}$$

$$c^d \bmod(n) = m^{ed} \bmod(n) = m \tag{6}$$

根据上述等价设计和密码算法的原理，基于混合加密算法的 G 函数构造如图 6 所示。基本方法是利用对称密码算法 GOST 加密当前转换后的频率号信息，利用非对称密码算法 RSA 加密用户共享的密钥，然后与传输的信息异或得到下一个频率号。发送过程和接收过程分别如图 7 和图 8 所示。首先，在发送信息前，初始频率号和秘密密钥用 RSA 算法加密后发送给接收方，其他频率号作为明文用 GOST 算法加密。接收方收到信息后，用自己的秘密密钥解密得到初始频率号和共享密钥，然后用 GOST 算法解密得到所传输的信息和频率号。

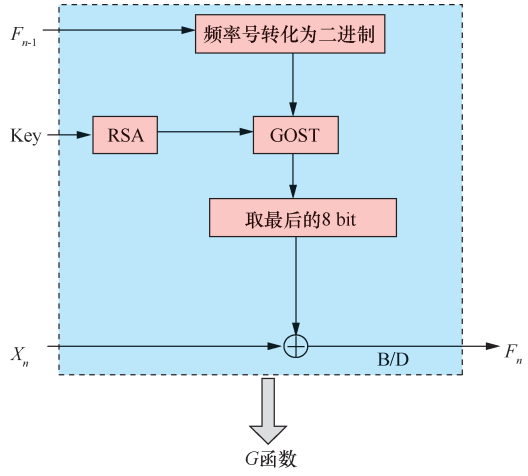


图 6　基于混合加密算法的 G 函数构造

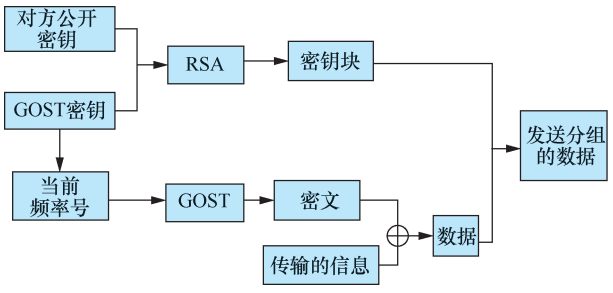


图 7　发送过程

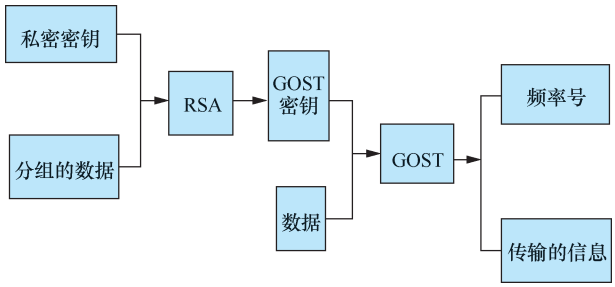


图 8　接收过程

3.3　混合加密算法的安全性分析

由 Kerckhoffs 准则可知，一个系统的安全性不在于算法的保密性，而在于密钥的保密性。混合加密算法的安全性主要依赖于非对称密码算法的密钥，因此，主要分析 RSA 算法密钥破解的可能性，考虑常用的两个攻击方法。

1) 穷举攻击

RSA 算法选取的密钥长度通常为 1 024 bit，其中，大素数 p 和 q 分别为 512 bit 左右。因此，攻击者想要穷举所有的 p 和 q，穷举的次数为

$$\frac{(2^{512}-2^{511})}{2}=2^{510} \tag{7}$$

由式(7)可知，目前的计算机无法穷举 p 和 q，从而无法破译 RSA 算法的密钥。因此，只要参数选择合适，RSA 算法的密钥是相对安全的。

2) 分解 n

由于 $n=pq$，若攻击者知道 p 和 q，则可以计算 $\varphi(n)$，进而可以通过式(8)计算秘密密钥 d，即攻破 RSA 算法。

$$ed\equiv 1\bmod(\varphi(n)) \tag{8}$$

RSA 算法的安全性依赖于大整数分解的困难性，而分解大整数目前无有效方法，尽管不能证明 RSA 算法的安全性等价于大整数分解，只要合理地选择参数，RSA 算法依然能抵抗现有的大部分攻击。

4　数值结果分析

差分跳频序列的综合性能决定差分跳频系统的性能，因此，主要对序列常用的 4 个性能进行测试，包括均匀性、随机性、复杂度和安全性。与此同时，均匀性和随机性的测试结果主要根据假设检验[23]。假设检验原理如表 1 所示，由表 1 可知，I 类错误为显著性水平，根据参考文献[23]，通常定义为 $\alpha=0.05$。序列的测试条件为：频隙数 N=256，长度 L=10 000。对仿射变换、可逆散列算法和混合加密算法生成的差分跳频序列在 B=(1, 2, 4) 3 种情形下进行性能测试，每种情形分别选取 4 组数据。

表 1　　假设检验原理

真实情况	结论	
	接受 H0	接受 H1
H0 为真	正确	I 类错误
H1 为真	Ⅱ类错误	正确

4.1　均匀性

均匀性是指每一个频率号出现的概率服从均匀分布。好的均匀性能够使各载波被等概率选取，从而提高系统的抗干扰能力。测试时，选取 $\alpha=0.05$，原假设 H0 为样本分布与(0, 1)均匀分布没有显著差异，若测试的概率 p 值大于 0.05，则接受原假设，认为样本是均匀分布的，否则不是均匀分布。B=(1, 2, 4) 3 种情形的检验统计量如图 9 至图 11 所示。

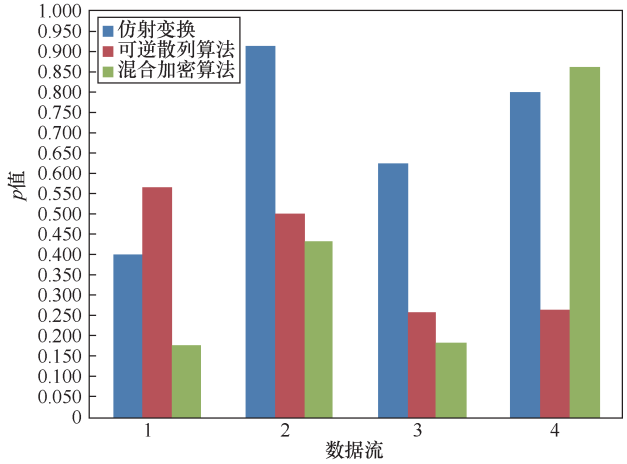


图 9　检验统计量（B=1）

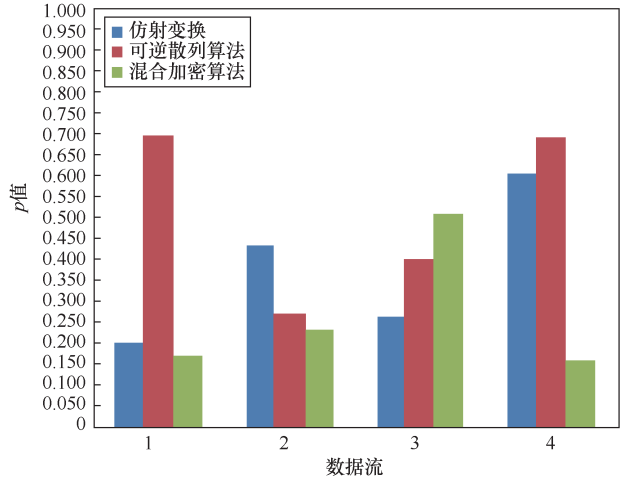


图 10　检验统计量（B=2）

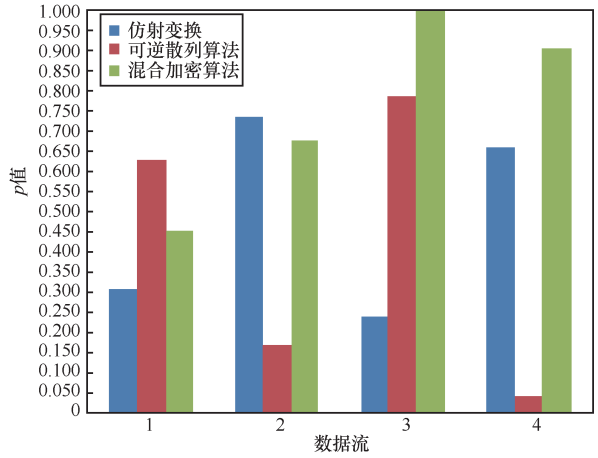


图 11　检验统计量（B=4）

从图 9 至图 11 可以看出，当 $B=1$ 和 $B=2$ 时，3 种算法生成的序列均通过测试，可认为是均匀分布；当 $B=4$ 时，基于可逆散列算法生成的序列 p 值小于 0.05。因此，基于所有样本的测试中，仿射变换和混合加密算法生成的序列是均匀分布的，而可逆散列算法的序列不是均匀分布的。

4.2　随机性

随机性检验又称为独立性检验，被用来检验两个随机变数之间的统计相关性是否显著。差分跳频为相关跳频，即频率之间有一定相关性，美国国家标准与技术研究院（NIST）所提供的统计方法无法通过此项测试。因此，采用快速的检验方法，即游程检验来检测差分跳频序列的随机性。该方法最早由 Wald[24]提出，主要用于单样本变量的随机性测试，检验变量值是否为随机变量。同样地，选取 $\alpha=0.05$，原假设 H0 为变量值认为是随机的。若测试的概率 p 值大于 0.05，则接受原假设，认为样本是随机变量，否则不是随机变量。B=(1, 2, 4) 3 种情形的检验统计量如图 12 至图 14 所示。

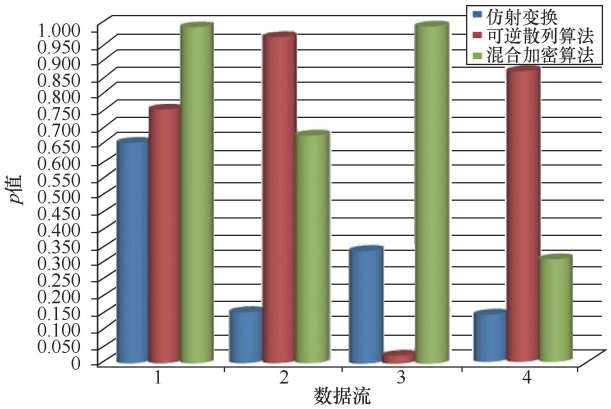


图 12　检验统计量（B=1）

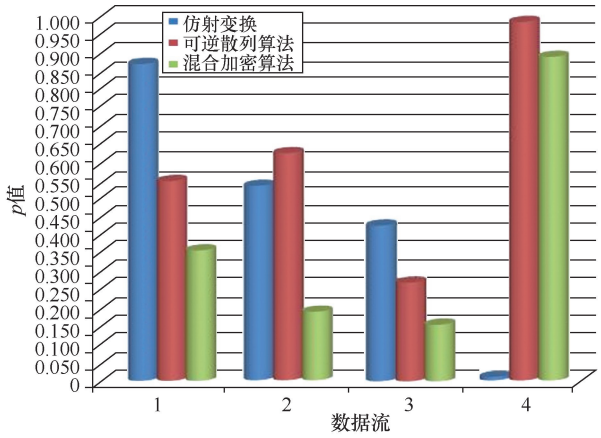


图 13　检验统计量（B=2）

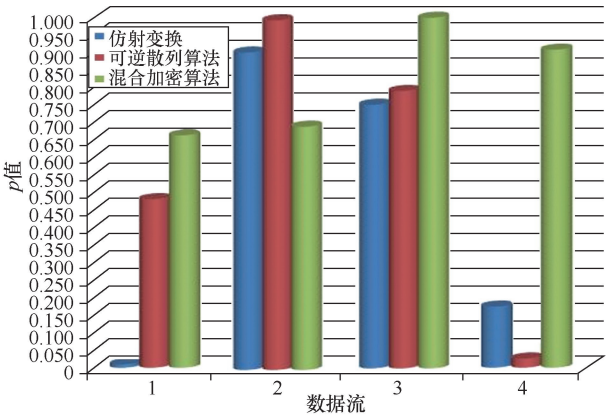


图 14　检验统计量（B=4）

根据测试结果可以看出，当 $B=1$ 时，可逆散列算法生成的跳频序列没有通过全部样本测试；当 $B=2$ 时，基于仿射变换的差分跳频序列没有全部通过测试；当 $B=4$ 时，仿射变换和可逆散列算法生成的序列同时没有通过测试。因此，基于混合加密算法生成的序列被认为是随机的，而其他两个算法生成的序列不是随机的。

4.3　复杂度

由于线性复杂度不易区分序列复杂度的高低，采用 Lempel-Ziv（LZ）复杂度衡量单个序列的复杂度。该方法由 Lempel 和 Ziv[25]首次提出，通过测量一个新模式在单个序列中出现的速率来表征序列的复杂性。相比于其他方法，LZ 复杂度是可计算的，且计算速度非常快。此方法描述如下，设 $c(n)$ 为给定符号序列 $S=(s_1s_2\cdots s_n)$ 的复杂度，根据 Lempel 和 Ziv 的研究，归一化复杂度定义如下

$$C_{\mathrm{LZN}}(n)=\frac{c(n)}{b(n)} \tag{9}$$

其中，$b(n)$ 是随机序列的渐进行为，通常用式(9)描述单个符号序列的复杂度，可以看出，随机序列的复杂度趋于 1，而规则序列的复杂度趋于 0。因此，C_{LZN} 越大，则复杂度越高。B=(1, 2, 4)3 种情形的 LZ 复杂度如图 15 至图 17 所示。

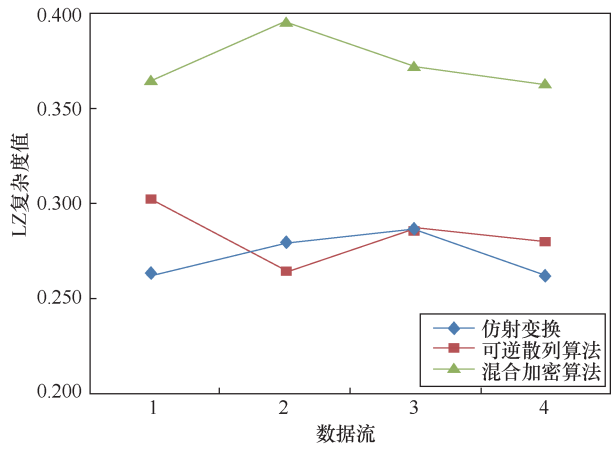


图 15　LZ 复杂度（B=1）

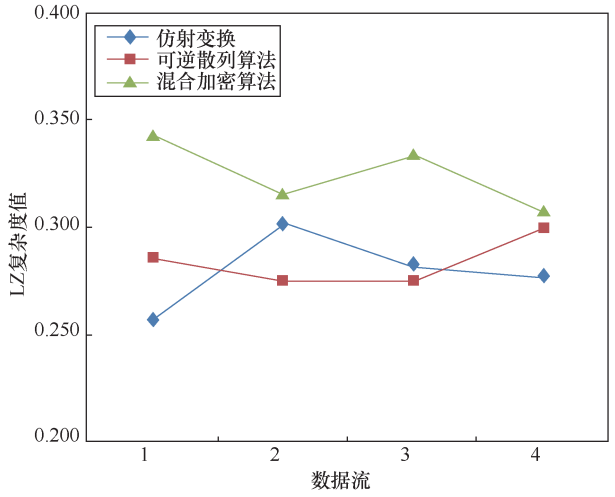


图 16　LZ 复杂度（B=2）

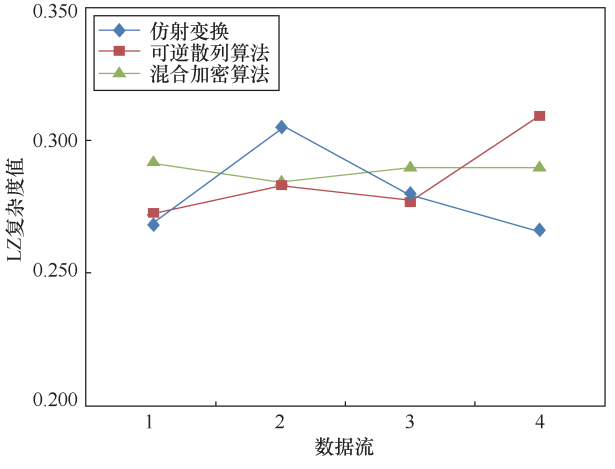


图 17　LZ 复杂度（B=4）

由上述结果可知，当 $B=1$ 和 $B=2$ 时，基于混合加密算法生成的序列复杂度最高。每跳传输 1 bit 时，表现最好，当传输的比特数逐渐增加时，复杂度的优势不再明显。因此，传输少量比特时，本文所提的混合加密算法生成的序列复杂度最高。

4.4　安全性

由 G 函数的构造及可逆性可知，密码系统中加密的逆操作即为解密，把解密同样长度的符号序列所需时间（单位：s）作为衡量安全性的指标，解密时间测试结果如表 2 所示。为了方便测试，解密暂且只考虑对称密码算法，密钥长度为 32 bit。

表 2　解密时间测试结果

	仿射变换/s	可逆散列/s	混合加密/s
$B=1$	0.974	8.949	1 333.842
$B=2$	0.963	8.332	1 330.200
$B=4$	0.981	8.526	1 332.970

由上述结果可知，解密混合加密算法序列所需时间多于其他两个算法。而当密钥长度增加后，考虑整个解密过程，解密非对称密码算法密钥所需的时间呈指数级增长。因此，混合加密算法的安全性最高，即破译十分困难。

5　结束语

针对大容量跳频网络中用户数据传输的安全问题，利用非对称密码系统的优点，结合对称密码系统，提出了一种基于混合加密算法的 G 函数，有效解决了用户数庞大情况下密钥的安全管理和分配问题，提升了差分跳频系统的安全性。与此同时，给出了这种设计的等价性证明。仿真结果表明，基于混合加密算法的 G 函数生成的差分跳频序列在随机性、复杂度和安全性等方面表现优异，具有较好的综合性能。因此，在未来万物互联的时代，采用高安全性的物理层安全技术对提升无线通信安全具有重要意义。

参考文献：

[1] LI J, CHENG Q, ZHANG X X, et al. Secure beamforming design for SWIPT in cooperative D2D communications[J]. China Communications, 2017, 14(1): 20-33.

[2] SUN G C, HAN Z, JIAO J B, et al. Physical layer security in MIMO wiretap channels with antenna correlation[J]. China Communications, 2017, 14(8): 149-156.

[3] HANNON M, FENG S, KWON H, et al. Jamming statistics dependent

frequency hopping[C]//IEEE Military Communications Conference. IEEE, 2016: 138-143.

[4] LI Z, CHANG Y L, JIN L J, et al. Analysis of FHMA performance on block cipher based frequency-hopping sequences[J]. IEEE Communication Letter, 2004, 8(7): 434-436.

[5] WANG D Y, ZHANG N, LI Z, et al. Leveraging high order cumulants for spectrum sensing and power recognition in cognitive radio networks[J]. IEEE Transactions on Wireless Communications, 2018, 17(2): 1298-1310.

[6] HERRICK D L, LEE P K. Chess a new reliable high speed HF radio[C]//IEEE Military Communications Conference. IEEE, 1996: 684-690.

[7] HERRICK D L, LEE P K, LEDLOW L L. Correlated frequency hopping—an improved approach to HF spread spectrum communications[C]//Tactical Communications Conference. IEEE, 1996: 319-324.

[8] DONG B H, TANG P, DU Y, et al. Performance of a compressed spectrum differential frequency hopping signal over Rician fading channel[J]. Journal of Electronics and Information Technology, 2015, 37(4): 836-840.

[9] ZHU W, YI B S, GAN L C, et al. Anti-jamming performance of fountain coded differential frequency hopping systems in AWGN[J]. China Communications, 2014, 11(14): 53-60.

[10] CHEN Z, SONG Y, DONG B H. Performance of a compressed spectrum differential frequency hopping system over Rayleigh fading channels[C]//IEEE Military Communications Conference. IEEE, 2013: 781-785.

[11] CHEN Y, ZHAO H S. Study of DFH *G* function algorithm used for DFH systems[J]. Journal on Communications, 2006, 27(10): 100-105.

[12] YANG Y L, HE Z W, KUANG J M. Research on the transition function of differential frequency hopping[J]. Journal on Communications, 2002, 23(4): 103-108.

[13] ZHOU Z, LI S, CHENG Y. Designing frequency transition function of differential frequency hopping system[C]//International Conference on Communications and Mobile Computing. IEEE, 2010: 296-300.

[14] GAN L C, WU S Y. A kind of shortwave frequency hopping code based on DFH transform function[J]. Journal of Electronics and Information Technology, 2005, 27(2): 218-220.

[15] ZHU W, YI B S, GAN L C. Performance research of fountain-DFH concatenated coding systems over AWGN with partial-band noise jamming[J]. Systems Engineering and Electronics, 2016, 38(3): 665-671.

[16] BAO Z Q, WANG B, GAO F. A new differential frequency hopping scheme based on encryption algorithm[J]. Study on Optical Communications, 2017, 202(4): 74-78.

[17] CHENG L, ZHOU J R. Differential frequency hopping *G* function algorithm based on advanced encryption standard[J]. Ship Electronic Engineering, 2008, 28(6): 107-109.

[18] YI D J, YANG Q L. Study of DFH frequency transition function based on the principle of affine cipher[J]. Journal of Air Force Engineering University, 2005, 6(3): 50-52.

[19] LIANG F L, LUO W X, ZHANG S L. Differential frequency hopping *G* function algorithm based on reversible integer hash function[J]. Transactions of Beijing Institute of Technology, 2004, 24(3): 254-257.

[20] GUAN L, LI Z, SI J B, et al. Generation and characteristics analysis of cognitive-based high performance wide-gap FH sequences[J]. IEEE Transactions on Vehicular Technology, 2015, 64(11): 5056-5069.

[21] SCHNEIER B. Applied cryptography: protocols, algorithms and source code in C[M]. USA: Wiley, 1996.

[22] RIVEST A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

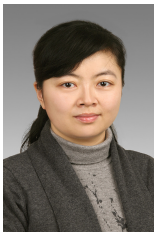
[23] LEHMANN L E, ROMANO J P. Testing statistical hypotheses[M]. Germany: Springer-Verlag, 2005.

[24] WALD A, WOLFOWITZ J. On a test whether two samples are from the same population[J]. The Annals of Mathematical Statistics, 1940, 11(2): 147-162.

[25] LEMPEL A, ZIV J. On the complexity of finite sequences[J]. IEEE Transactions on Information Theory, 1976, 22(1): 75-81.

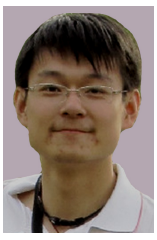
[作者简介]

陈芮（1988− ），男，湖北宜昌人，西安电子科技大学博士生，主要研究方向为跳频序列设计、物理层安全。



李赞（1975− ），女，陕西西安人，西安电子科技大学教授、博士生导师，教育部“长江学者特聘教授”，主要研究方向为突发通信、数字信号处理、无线通信系统等。

石嘉（1987− ），男，陕西西安人，西安电子科技大学副教授，主要研究方向为无线系统资源分配、多载波通信、毫米波通信、隐蔽通信、物理层安全、认知无线电等。



关磊（1986− ），男，陕西渭南人，西安电子科技大学讲师，主要研究方向为跳频序列设计、跳频通信、频谱感知网络等。