基于改进随机位移替代法的宽间隔跳频序列构造方法

曾梦姣[1]
ZENG Mengjiao

摘 要 随着电力行业数字化转型的不断深入，越来越多的电力设备接入无线通信网络。受制于无线信道的广播特性和开放性，电力数据传输的安全性面临严重挑战，尤其是资源受限的设备。因出色的抗干扰和抗截获能力，跳频通信技术被广泛应用于高安全通信。然而，随着电子攻击的不断升级，现阶段跳频序列的生成方法大多基于有限域和混沌理论，安全强度较低。考虑到资源受限的电力设备，基于轻量级密码算法的原理生成基序列，结合改进随机位移替代法，设计了一种面向电力物联网的跳频序列生成方案。所提出的方案具有良好的复杂度和随机性，较好地实现了效率与安全性的平衡。与现有的算法相比，基于所提出的算法原理生成的跳频序列在大部分测试指标上表现更出色。由此可见，所提出的方案能够在较低的资源消耗下实现信息的安全传输，为电力物联网中资源受限设备的无线传输提供了一种高效且安全的解决方法。

关键词 电力物联网；无线通信；跳频序列；轻量级加密算法；随机位移替代法

doi：10.3969/j.issn.1672-9528.2024.10.043

0 引言

岸电是指船舶在港口停靠时，通过岸上的电源提供电力供应，以取代船舶自行用柴油或其他化石能源发电的方式。使用岸电系统可以减少船舶使用发电机组带来的环境污染和噪音干扰，还可以降低船舶运行成本和维护费用。因此，岸电系统被认为是一种环保节能的船舶供电方式，已经被越来越多的国家和地区如美国、北欧等采用。某岸电试验区为实现对长江沿线岸电系统进行综合运维管控，一站式对多个岸电桩进行远程集中的综合管控，现建立长江岸电运维管控系统，其总体架构如图 1 所示。在此系统中涉及大量的数据传输和处理，其中码头相关电力设备和岸基管理系统间，边缘物联代理终端和岸电运维管控系统间便通过无线信道进行信息传输，本文研究重点是码头相关电力设备和岸基管理系统间的信息传输安全问题。众所周知，无线信道具有开放性，通过广播方式进行传播，容易被窃听者截获和干扰，数据的泄露或遭到未授权访问将可能导致严重的安全问题，因此，为了保证岸电系统的安全性，必须寻找高效的加密方案来保障无线信道的通信安全。

为了解决无线信道信息安全传输的问题，之前的研究者提出了一系列轻量级密码算法，如 DESL 算法 [1] 和 LED 算法 [2] 用于加密数据，以提高无线信道中数据传输的安全性。然而，这种方法仅仅在应用层及以上网络层面对信息进行安全传输，却忽略了应用层下面的安全问题。为了更全面地保障通信安全，有必要在物理层采取相应的措施，常见手段有码分多址 [3-4]、引入物理人工噪声 [5-6] 和跳频技术（frequency hopping spread spectrum，FHSS）等。码分多址通过使用不同的扩频码来区分不同的用户，使得窃听者无法获取其他用户的信息，但码分多址技术在频谱利用率方面相对较低；在传输过程中引入人工噪声，可以干扰窃听者的信号截获和解码，但物理人工噪声的引入可能会对通信质量产生一定的影响，降低信号传输的可靠性；而跳频技术则通过在传输过程中跳跃改变频率序列来保护通信，它通过在不同时间和频率上发送数据，使得窃听者无法准确捕捉到完整的信号。这种方法不仅增加了窃听者攻击的难度，还提供了更强的安全性和更高的通信可靠性。

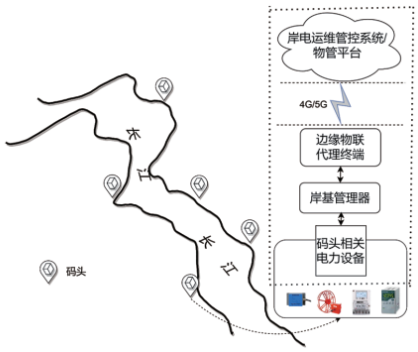

图 1 长江岸电运维管控系统总体架构图

1. 三峡大学计算机与信息学院 湖北宜昌 443000

跳频技术是一种通过频率变化来实现无线通信的技术，它能有效地提高通信系统的抗干扰能力和安全性。在跳频技术中，信号在一个较宽的频谱范围内以伪随机的顺序不断改变频率，从而使得通信信道难以被干扰或截获。在跳频通信中，跳频序列具有关键作用。通过对跳频序列进行宽间隔处理，可以显著提升跳频系统的抗干扰能力。因此，宽间隔跳频序列在跳频通信中的应用已经变得非常普遍。

1 宽间隔序列生成方案

本文采用轻量级加密算法生成跳频基序列，通过改进的随机位移替代法（Random-Shift-Replace method，RSR）对其重新映射生成宽间隔跳频序列。

1.1 FH 技术介绍及系统模型

通信系统框架及抵抗干扰的过程见图 2，FH 通信系统主要由频率合成器、FH 序列生成器以及 FH 同步器组成。

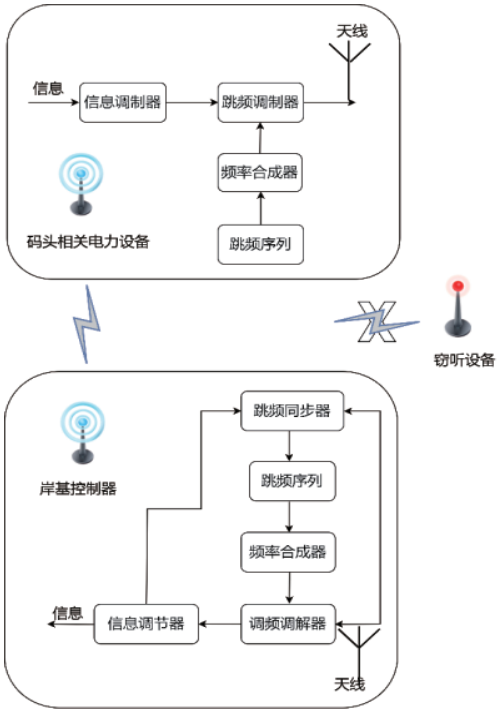

图 2 FH 系统原理图

发送和接收信号的过程如下。

（1）发射机将传输的信息调制到载波频率上，并生成调制信号。同时，FH 序列生成器生成 FH 序列，并控制本地振荡器信号以改变调制信号的频率，使传输信号的频率根据 FH 序列的跳频而变化。

（2）接收机将接收到的 FH 信号的频率进行转换。通信双方采用相同的 FH 序列并实现 FH 同步，因此很容易实现去跳频操作，并在解调后恢复输出信息。

FH 序列不仅在信息传输过程中控制频率跳变，还可以作为 FH 通信网络中区分用户的地址码。FH 序列的质量直接影响跳频系统的整体性能，因此，理想的 FH 序列应具有高度随机性、复杂度高和高安全性的特点。

由于 FH 系统和密码体制之间是等价的，可以基于分组密码算法生成兼顾安全性和效率的 FH 序列。考虑到岸电相关设备存储资源、运算资源、能耗资源有限等问题，通过轻量级加密算法生成跳频序列，能够在岸电这一特定场景中兼顾设备资源受限的同时保障设备的安全性。

1.2 跳频基序列

本文采用 Eslice-64-64[7] 轻量级加密算法生成跳频基序列，具体生成方案如图 3 所示。

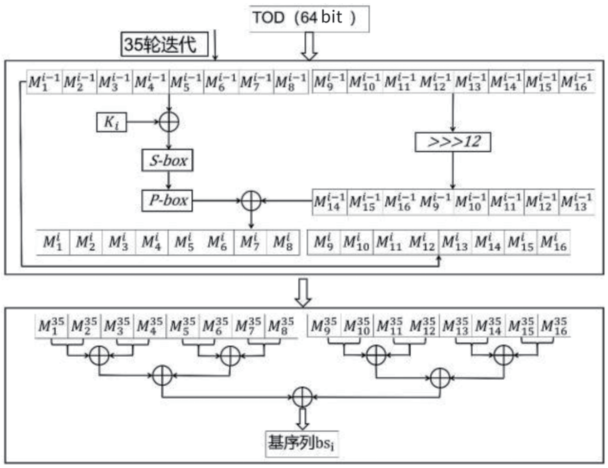

图 3 基序列生成方案

算法输入 64 bit 的 TOD，在每一轮迭代过程中将输入 4 bit 为一组，分为 $M_1, M_2, \cdots, M_{16}$，经过 35 轮迭代，线性框中是每轮迭代的非线性变换过程。具体的过程数学表达式可以表示为：

$$M_{j+8}^{i+1} = M_j^i \tag{1}$$

$$(M_9^i \| M_{10}^i \| \ldots \| M_{16}^i) >>> 12 \tag{2}$$

$$M_j^{i+1} = \mathrm{Pbox}(\mathrm{Sbox}(M_{j+8}^i \oplus K_i)) \oplus M_j^i \tag{3}$$

式中：i=1, 2, ⋯, 35 为迭代次数；j=1, 2, ⋯, 8；符号 >>> 和 ⊕ 分别表示循环右移和异或运算。迭代结束得到 ($M_1^{35} \| M_2^{35} \| \cdots \| M_{32}^{35}$)。最后经过一步异或操作得到跳频基序列 BS={bs_i}：

$$\begin{aligned} bs_i = (((M_1^{35} \| M_2^{35}) \oplus (M_3^{35} \| M_4^{35})) \oplus ((M_5^{35} \| M_6^{35}) \oplus \\ (M_7^{35} \| M_8^{35}))) \oplus (((M_9^{35} \| M_{10}^{35}) \oplus (M_{11}^{35} \| M_{12}^{35})) \oplus \\ ((M_{13}^{35} \| M_{14}^{35}) \oplus (M_{15}^{35} \| M_{16}^{35}))) \end{aligned} \tag{4}$$

1.3 宽间隔跳频序列

宽间隔跳频序列的数学表达式如下：对于任意两相邻频点 $x_i, x_{i+1} \in X$，其跳频间隔大于最小跳频间隔 d_0，则其为宽间隔跳频序列，具体数学表达式为：

$$|x_i - x_{i+1}| > d_0 \tag{5}$$

如果

$$|x_i - x_{i+1}| < d_0 \tag{6}$$

那么，X不是宽间隔跳频序列，x_{i+1}为跳频序列中的窄点。

RSR 宽间隔设计方法通过将混沌跳频序列中的窄点进行平移，使得序列满足宽间隔的要求[8]。

$$x_{i+1} = \begin{cases} x_{i+1}, & \text{if } |x_i - x_{i+1}| > d_0 \\ x_i + (d_0 + 1 + u_i), & \text{if } |x_i - x_{i+1}| < d_0 \end{cases} \tag{7}$$

式中：u_i一般取（$x_{i+1} \bmod (q - 2d_0 - 1)$）。

表 1 NIST 测试

测试方法	P 值（改进RSR）	p 值（m序列）	p 值（logistical映射）
频率检验	0.292 827	0.560 567	0.000 000
块内频率检验	0.999 975	0.510 939	0.000 000
累加和检验（Forward）	0.370 867	0.451 231	0.000 000
累加和检验（Reverse）	0.566 517	0.637 475	0.000 000
游程检验	0.000 000	0.908 969	0.000 000
最长游程检验	0.000 000	0.700 803	0.000 000
二元矩阵秩检验	0.724 310	0.000 000	0.051 532
离散傅里叶变换检验	0.117 701	0.000 000	0.194 366
非重叠模块匹配检验	0.650 027	0.028 821	0.000 003
重叠模块匹配检验	0.976 908	0.003 776	0.000 004
通用统计检验	0.349 622	0.122 817	0.000 000
近似熵检验	0.756 483	0.622 186	0.000 000
随机游动检验	0.000 000	0.000 000	0.000 000
随机游动状态频数检验	0.000 000	0.000 000	0.000 000
序列检验	0.963 831	0.939 418	0.000 000
线性复杂度检验	0.041 724	0.000 000	0.763 527

本文采用改进的 RSR 宽间隔设计方法，具体流程如下：

$$\mathrm{ws}_{i+1} = \begin{cases} \mathrm{bs}_{i+1}, & \text{if } |\mathrm{ws}_i - \mathrm{bs}_{i+1}| > d_0 \\ \mathrm{ws}_i + (d_0 + 1 + u_i), & \text{if } |\mathrm{ws}_i - \mathrm{bs}_{i+1}| < d_0,\ \mathrm{ws}_i > \mathrm{bs}_{i+1} \\ \mathrm{bs}_{i+1} + (d_0 + 1 + u_i), & \text{if } |\mathrm{ws}_i - \mathrm{bs}_{i+1}| < d_0,\ \mathrm{ws}_i < \mathrm{bs}_{i+1} \end{cases} \tag{8}$$

式中：$u_i = \mathrm{ws}_i \bmod (q - 2d_0 - 1)$，$\mathrm{ws}_0 = \mathrm{bs}_0$。

2 数值分析与结果

2.1 随机性

在岸电通信系统中，序列的良好随机性对于提高安全性和可靠性至关重要，能有效防止预测、干扰或操纵。因此，在设计跳频序列时，进行随机性验证是必不可少的步骤，以确保序列的质量和可靠性，满足岸电通信系统的要求。为了评估由密码算法生成的 FH 序列的随机性，采用了美国国家标准与技术研究院（NIST）的测试方法[9]。根据假设检验原理，选择了显著性水平 α=0.01 进行 NIST 测试。测试过程包括将生成的序列转换为二进制数据，并利用 sts-2.1.1 软件进行具体的 NIST 测试操作。

表 1 展示了 NIST 测试的结果。可以从中看到，由改进的 RSR 控制生成的跳频序列在所有 12 项 NIST 测试项目中均表现出色。这表明改进的 RSR 方法在随机性方面具有很高的可靠性。相比之下，m 序列通过了其中的 10 项测试，显示出较好的随机性，但仍有改进空间。logistical 序列的表现相对较差，仅通过了 3 项测试，说明其生成的跳频序列在随机性和安全性方面存在明显不足。这些结果清晰地表明，改进的 RSR 控制方法在生成高质量的跳频序列方面具有明显优势，有助于提高岸电通信系统的安全性和可靠性。

2.2 复杂度

Lempel-Ziv（LZ）复杂度的计算可以揭示跳频序列中跳变模式的多样性和重复性。较低的 LZ 复杂度可能表示序列中存在更多的重复跳变模式，而较高的 LZ 复杂度则表明跳变模式更为多样化。通常，随机序列的复杂度接近 1，而规则序列的复杂度接近 0。根据 Lempel 和 Ziv 的研究[10]，给定序列 $S = (s_1, s_2, \cdots, s_n)$，有：

$$\lim_{n \to \mathbf{0}} c(n) = b(n) = \frac{n}{\log_2(n)} \tag{9}$$

$b(n)$ 表示随机序列的渐进行为，则其复杂度表示为：

$$C_{\mathrm{LZN}} = \frac{c(n)}{b(n)} \tag{10}$$

图 4 给出了每种算法生成 FH 序列的 LZ 复杂度测试结果，本文提出算法生成的跳频序列的 LZ 复杂度普遍要高于其他两类。

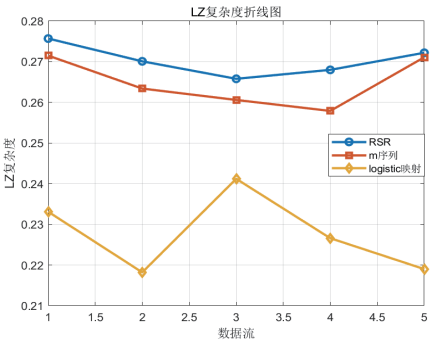

图 4 LZ 复杂度

3 结语

RSR 宽间隔技术可以与现有的无线通信系统兼容，不需要大幅度改动硬件设备，具有良好的实用性和经济性。综上所述，改进 RSR 宽间隔通过优化无线信道的频率利用，提高了岸电系统在数据传输过程中的抗干扰能力和安全性，是一种有效的物理层安全增强方法。

参考文献：

[1]JI F, ZHANG W, DING T. Improving Matsui's search algorithm for the best differential/linear trails and its applications for DES, DESL and GIFT[J].The computer journal, 2019, 64: 610-627.

[2]LIU X, QIAN Y.Research on LED lightweight cryptographic algorithm based on RFID tag of Internet of things[C]//2019 IEEE 8th Joint International Information Technology and

基于 ABE 算法的数据库隐私数据加密方法研究

贾 俊[1] 谭振华[1]
JIA Jun TAN Zhenhua

摘 要 针对现有加密方法在对数据库隐私数据加密时，未充分考虑属性基安全性，并且存在关键字、密文索引过大的问题，导致数据库开销较大、安全性不佳，研究了基于 ABE 算法的数据库隐私数据加密方法。为了实现对加密列中数据的灵活查询、降低开销，设计数据库数据外部索引方式，引入 ABE 算法，确定双线性关系，根据列名在十字链表中定位到对应的列，然后依次遍历该列的所有元素，并使用提供的密钥加密处理每个元素，使用相同的密钥解密每个元素，解密后的数据替换原有加密数据，保存在原位置，完成初步隐私数据加密。为进一步增强隐私数据的安全性，通过加密访问控制数据库属性基，优化数据库隐私数据加密方法。通过对比实验证明，新的加密方法应用下，加密后在保证数据安全的前提条件下，有效降低关键词和密文索引数据量，降低数据库计算开销和存储开销，数据量降到了 1.23 Mbit，隐私数据量降到了 18.56 Mbit，促进数据库运行性能提升。

关键词 ABE 算法；隐私；加密；数据；数据库

doi：10.3969/j.issn.1672-9528.2024.10.044

0 引言

数据库作为信息存储和管理的核心载体，其安全性与隐私保护问题日益凸显。数据库隐私数据的加密方法研究，对于保护用户隐私、维护信息安全具有重要意义。当前，数据库加密技术已取得了长足进步，然而现有加密方法仍存在诸多不足。首先，对称加密算法虽然速度快，但密钥管理困难，一旦密钥泄露，整个加密数据库将面临严重威胁。哈希算法虽然可以实现数据的单向加密，但一旦数据被篡改，其完整性将无法得到保障。针对该问题，相关学者进行了研究，如黎明[1]以支持快速查询为出发点，研究了嵌入式数据库加密技术，但是该方法存在开销大的问题。裴江艳[2]以 MD5 数据库加密为核心，研究了信息数据安全存储方法，但是该方

1. 晋中信息学院大数据学院、信息工程学院 山西晋中 030800
[基金项目] 晋中信息学院校级教改项目的课题“基于课程思政视域下网络安全课程教学方法的探索与研究”

Artificial Intelligence Conference,[Volume 1 of 3].Piscataway, N.J.: IEEE, 2019: 1717-1720.
[3]ABDULSADA H F, MOHAMMED S J.Comparison of bit error rate and performance analysis for multicode CDMA techniques in fading and AWGN channels[C]//2022 5th International Conference on Engineering Technology and its Applications. Piscataway: IEEE, 2022:212-217.
[4] 李召飞 . 综合测控终端码分多址干扰分析 [J]. 数字通信世界 ,2024(3):45-47.
[5] 曹建勋 , 王谋业 , 杨胜辉 , 等 . 全双工辅助的无人机上行通信抗窃听物理层安全技术研究 [J]. 现代电子技术 , 2024, 47(9): 21-28.
[6] 雷维嘉 , 毕文佳 , 雷宏江 , 等 . 时间反转 OFDM 系统中增强安全性能的功率分配与人工噪声设计 [J]. 电子学报 , 2024, 52(5): 1570-1581.
[7] 梁丽芳 , 杜小妮 , 李锴彬 , 等 . 基于 Feistel 结构的分组密码算法 Eslice[J]. 山东大学学报 (理学版),2023,58(3):85-92.
[8] 黄琪 , 杨宇晓 , 江陈卓 . 组合跳变随机平移宽间隔混沌跳频序列设计 [J]. 电讯技术 , 2022,62(6):755-761.
[9] 王超 , 温涛 , 段冉阳 .NIST 随机性检测方法研究 [J]. 信息技术与网络安全 , 2018, 37(11):5-8+15.
[10]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】
曾梦姣（2000—），女，湖北荆门人，硕士研究生，研究方向：电力网络安全。

（收稿日期：2024-07-12）