引用本文：杨梦媛，梁晓东，李亮，等. 基于量子随机数分发的光物理层信息防护方法研究[J]. 光通信技术，2026，50(5)：87-92.

基于量子随机数分发的光物理层信息防护方法

杨梦媛[1]，梁晓东[1,2]，李 亮[1,2]，赵瑞安[1,2]，李沼云[1,2]，伍浩成[1,2]，罗璋嗣[1]

（1.中国电子科技集团公司 第三十四研究所，广西 桂林 541004；2.广西光网络与光信息安全重点实验室，广西 桂林 541004）

摘要：针对光纤通信物理层抗截获能力不足的问题，提出一种基于量子随机数分发的光物理层信息防护方法。利用量子随机数模块生成随机源，通过云端管理平台完成随机数的存储、分发与日志管理，并设计基于同步索引的流加密方案，收发双方利用相同的离线量子随机数库和索引序列实现数据加解密。以512×512像素的Lena图像为实验数据，构建了光物理层信息防护演示实验。实验结果表明：量子随机数模块生成的随机数通过NIST SP800-22随机性测试；接收端能够无失真、无噪点地恢复图像数据；加密后的数据像素直方图分布均匀，水平、竖直和对角方向上的相邻像素相关系数显著降低并趋近于0，信息熵提升幅度为7.4%，逼近理论最大值，可有效抵御光纤通信物理层的信息截获、窃听与篡改行为。

关键词：物理层安全；量子随机数；图像加密；相关系数

中图分类号：TN256　　**文献标志码：**A　　**文章编号：**1002-5561(2026)05-0087-06

DOI：10.13921/j.cnki.issn1002-5561.2026.05.014

Optical physical-layer information protection method based on quantum random number distribution

YANG Mengyuan[1]，LIANG Xiaodong[1,2]，LI Liang[1,2]，

ZHAO Ruian[1,2]，LI Zhaoyun[1,2]，WU Haocheng[1,2]，LUO Zhangsi[1]

（1. The 34th Research Institute of CETC，Guilin Guangxi，541004，China；

2. Guangxi Key Laboratory of Optical Network and Optical Information Security，Guilin Guangxi，541004，China）

Abstract：Aiming at the insufficient anti-interception capability of the physical layer in optical fiber communications，an optical physical layer information protection method based on quantum random number distribution is proposed. A quantum random number module is used to generate random sources，and a cloud management platform is adopted for random number storage，distribution，and log management. A stream encryption scheme based on synchronous indexing is designed，in which the transmitter and receiver use identical offline quantum random number libraries and index sequences to perform data encryption and decryption. A demonstration experiment for optical physical layer information protection is constructed using a 512×512-pixel Lena image as the experimental data. The experimental results show that the random numbers generated by the quantum random number module pass the NIST SP800-22 randomness test；the receiver can recover the image data without distortion or noise；the pixel histogram of the encrypted data is uniformly distributed，and the correlation coefficients of adjacent pixels in the horizontal，vertical，and diagonal directions are significantly reduced and approach 0. The information entropy increases by 7.4%，approaching the theoretical maximum，and the method can effectively resist information interception，eavesdropping，and tampering at the physical layer of optical fiber communications.

Key words：physical layer security，quantum random numbers，image encryption，correlation coefficient

收稿日期：2025-07-21。

基金项目：国家自然科学基金项目(U25B2001)资助；国防基础科研计划项目(JCKY2024210B016)资助。

作者简介：杨梦媛(1991—)，女，本科，工程师，2014年毕业于韩国建国大学。现就职于中国电子科技集团公司第三十四研究所，从事光通信技术及光网络安全技术等研究。



0 引言

随着全球信息化进程的持续深化，光纤通信网络作为现代信息基础设施的核心骨架，承载着海量敏感数据，其安全性直接关系到国家安全与社会稳定。然而，光纤链路并非绝对安全，攻击者可通过光纤弯曲耦合、分光器窃听等手段，在不中断通信的条件下截获传输数据[1]。传统基于计算复杂度的数学加密方案

在理论上无法抵御量子计算、量子算法攻击等新兴攻击手段的威胁。物理层安全（PLS）的理论基础源于Wyner A D[2]提出的窃听信道模型，后经推广至广播信道场景。该技术利用信道本身的物理特性实现信息论安全的保密通信，为突破传统加密的局限提供了新思路[3-4]。在量子通信领域，量子密钥分发（QKD）已被证明具有信息论安全性[5-6]，且逐步走向广域工程化部署[7-8]。因此，在物理层直接构建高安全性、兼容现有光网络的信息防护机制，已成为光通信物理层安全领域亟待解决的关键科学问题。

在光纤通信物理层安全增强技术方面，国内外学者开展了大量探索并取得了显著进展。Hirota O等人[9-10]提出了Y-00量子噪声随机化流密码协议，利用激光相干态的量子噪声掩蔽多进制调制信号，将数学算法与物理噪声相结合，实现了100 Gbit/s及以上的波分复用安全传输。国内学者在特定应用场景下也取得了大量创新性成果。例如，提出“三区耦合”微元噪声模型以提升量子噪声流加密效率[11]；将量子噪声流加密与正交频分复用技术相结合，实现高速光纤安全传输[12]；对不同调制格式的随机加密系统进行严格的安全性定量分析[13]；提出基于差分相移键控（DPSK）调制的量子噪声流加密光隐藏通信系统[14]；在光通信物理层密钥分发与加密控制方面开展系统性研究[15]；在光学混沌同步保密通信技术上取得长足进步[16]。此外，国内学者针对可见光通信（VLC）链路的数据传输安全性不高的问题也取得了重要突破[17]，并探索了低密度奇偶校验（LDPC）信道编码在相干光通信量子噪声流密码（QNSC）系统中的应用[18]。尽管已有丰硕成果，但现有安全技术在规模化部署中仍面临挑战。一方面，加密与密钥管理多处于分离的状态，缺乏量子随机数生成器（QRNG）与光通信物理层的深度融合架构。另一方面，针对海量量子随机数的离线存储与云端分发缺乏系统性安全设计，传统流加密在动态信道下的同步机制易失效，抗截获与高级窃听的能力仍需进一步验证[19]。针对上述挑战，本文提出一种基于量子随机数分发的光物理层信息防护方法。

1 系统原理

1.1 系统模型

本文提出的基于量子随机数分发的光物理层信息防护系统模型示意图如图1所示。该系统由量子随机数生成模块、云端量子随机数管理平台、发送端、接收端以及传输信道组成。其中，量子随机数生成模块用于产生系统所需的高安全性的随机源。云端量子随机数管理平台负责对量子随机数进行集中存储、分发和日志管理。发送端和接收端分别配置本地离线量子随机数库、索引生成模块以及加密/解密模块。传输信道用于承载经过加密处理后的业务数据。云端量子随机数管理平台将量子随机数预先分发至通信双方，使收发两端在不通过业务信道实时传递密钥的情况下，能够依据一致的索引序列从本地离线量子随机数库中提取相同随机数，构建相同的密钥流。与传统仅依赖算法复杂度的保护方式不同，该方法采用量子随机数预分发和同步索引的架构具有传输介质无关性。密钥流与业务数据进行按字节异或运算，从而实现数据混淆和信息防护，不依赖任何特定传输介质的物理特性。因此，该模型可直接部署于光纤通信、VLC、WIFI等任意通信网络中。针对当前光通信网络

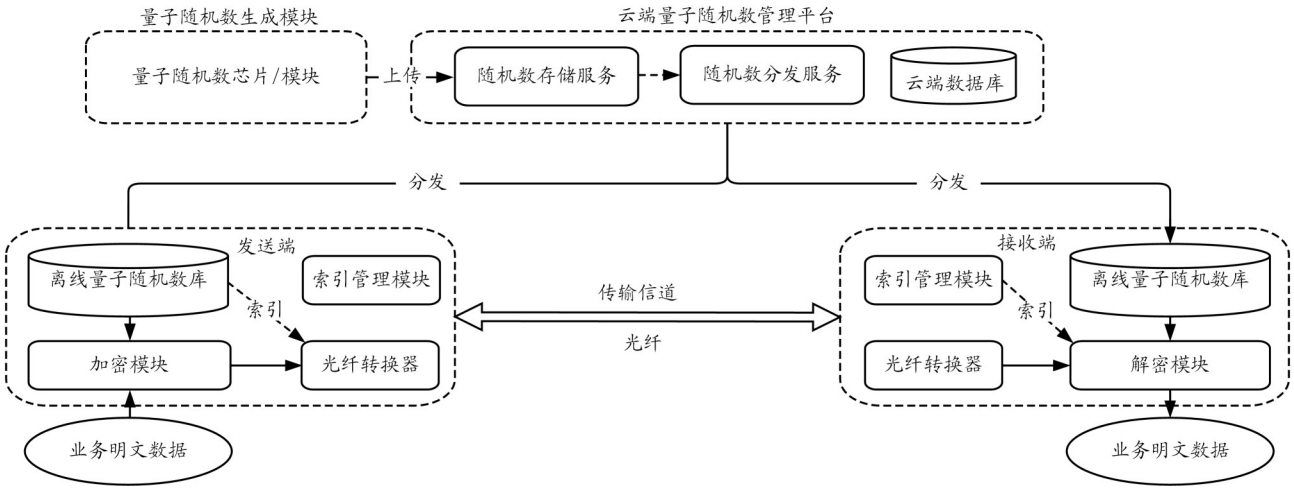


图1 基于量子随机数分发的光物理层信息防护系统模型示意图

普遍存在的物理层窃听威胁，如分光器窃听、光纤弯曲耦合窃听等，攻击者即使在光物理层截获到完整的光信号，也只能得到经过量子随机数完全混淆后的密文数据，无法从中提取任何有效明文信息。

量子随机数生成模块基于放大自发辐射（ASE）原理产生随机数，其随机性来源于量子态的内禀不确定性，无算法依赖、无周期、无偏、不可预测。通过后处理得到的高质量的随机数，为系统提供高安全等级的随机源[20]，该模块输出的序列Q如式（1）所示。

$$Q = \{q_1, q_2, \cdots, q_N\} \tag{1}$$

式中：N表示随机数序列的总字节长度；q_i表示第i个随机数，$q_i \in \{0, 1, 2, \cdots, 255\}$。

云端量子随机数管理平台将生成的随机数序列进行集中存储，并同步下发至发送端和接收端，使通信双方分别建立内容一致的本地离线量子随机数库。通信双方除了存储本地离线量子随机数库外还需预先配置相同的初始种子s_0，并采用相同的伪随机数算法生成索引序列I，其生成过程如式（2）所示。

$$I = G(s_0, m) \tag{2}$$

式中：$G(\cdot)$表示双方约定的伪随机数生成算法，m为加密明文数据所需的索引数量。在初始种子、伪随机数算法、索引长度均一致的条件下，发送端和接收端能够独立生成相同的索引序列，收发双方使用相同的离线量子随机数库和索引序列实现安全业务数据传输。

1.2 加解密原理

加解密原理如图2所示，收发两端具有相同的索引序列和离线量子随机数库，在加密阶段，通过同步索引序列生成一致的密钥流，对业务数据流进行逐字节异或加解密。整个过程不依赖数据的内容、格式和上层应用协议，可实现对图像、文本、语音、视频等各类业务数据的防护。将业务数据转换为一维明文字节序列P，如式（3）所示。

$$P = p_1, p_2, \cdots, p_k \tag{3}$$

式中：，p_k为原始业务数据展开为一维字节序列后的第k个明文字节，$k = 1, 2, \cdots, K$。发送端根据索引序列I，依次遍历本地离线量子随机数库Q。针对明文序列中的每一个字节p_i，发送端依据索引值I_i从库中提取出对应的量子随机数q_{I_i}，按照遍历的顺序将其依次拼接，生成与明文数据长度严格匹配的密钥如式（4）所示。

$$R = r_1, r_2, \cdots, r_k \tag{4}$$

式中：r_i表示第i字节密钥流，$r_i = q_{I_i}$。随后，在物理层逻辑处理单元中，将明文字节序列P与量子密钥流R进行逐字节的异或掩码运算，实现对原始数据的混淆和置乱。加密后的密文字节序列C如式（5）所示。

$$C = c_1, c_2, \cdots, c_k \tag{5}$$

式中：c_k表示加密后密文的第k个字节数据。

解密阶段则是加密流程的逆运算，由于接收端拥有与发送端完全相同的随机数索引序列I和离线量子随机数库Q，因此接收端能够按照相同的映射规则，从本地库中提取出量子随机数重构量子密钥流R'，且保证$R' = R$。在恢复原始业务数据时，系统利用布尔代

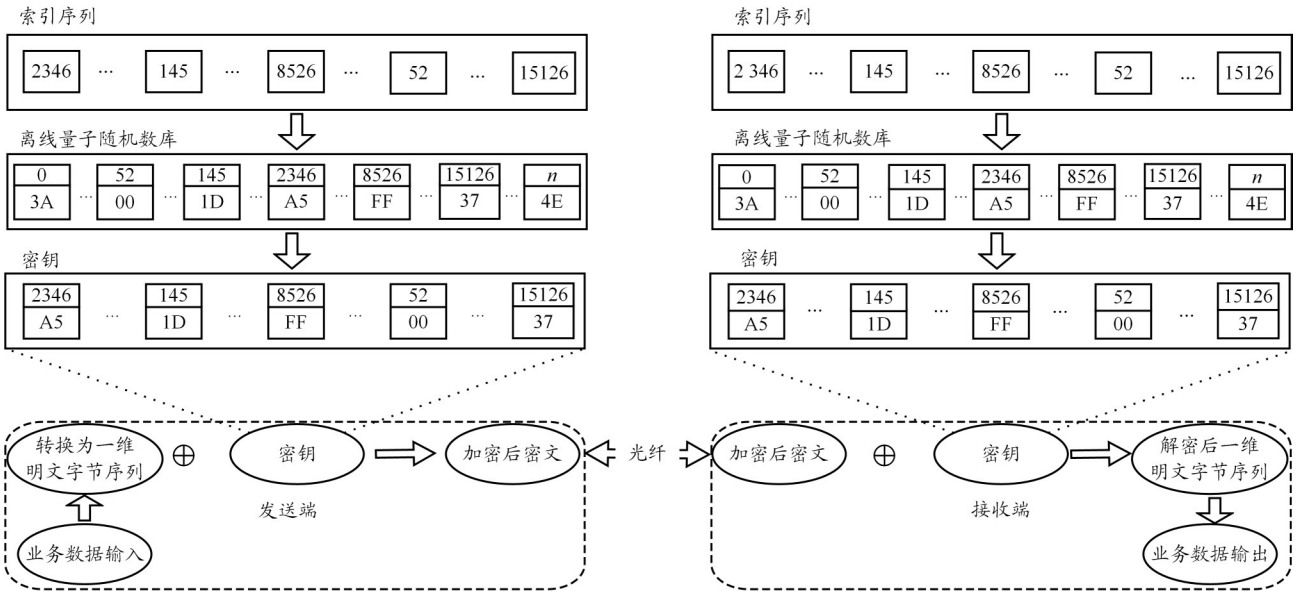


图2 加解密原理图

数中异或运算固有的对合特性，即对于任意布尔变量A和B，满足式(6)。

$$(A\oplus B)\oplus B = A \tag{6}$$

接收端将密文序列C与重构密钥流R'进行逐字节异或运算，从而实现对原始业务数据的无损还原。整个物理层流加解密过程如式(7)、式(8)所示。

$$c_k = p_k\oplus q_{I_k} \tag{7}$$

$$p'_k = c_k\oplus q_{I_k} = (p_k\oplus q_{I_k})\oplus q_{I_k} = p_k \tag{8}$$

式中：$\oplus$表示逐字节异或运算，q_{I_k}为根据索引序列I_k从离线量子随机数库Q中定向抽取出的量子随机数，p'_k为解密端恢复出的原始业务数据的一维明文字节。只要密钥流同步机制不失效，业务数据便能实现安全的端到端传输。

1.3 密钥量需求与安全性评估

本文密钥体系包含离线量子随机数库、索引序列与初始种子三部分，本地量子随机数库容量、加密过程的密钥取用量以及索引序列长度与待传输业务数据长度完全对等，三者始终与明文数据长度保持一致。通信双方预共享1字节初始种子，仅用于同步生成索引序列。以初始种子为同步参数，生成与业务数据等长的密钥流，整个增殖过程仅做地址映射，不会改变量子随机数本身的统计特性与不可预测性。密钥核心熵值完全来源于量子随机数库，种子和索引只承担同步寻址作用，无法反向推导出有效密钥。加之量子库采用离线分发、动态补全、用完即销毁的机制，大幅降低泄露风险。整套密钥增殖链路无算法漏洞与熵损失，结合光通信物理层部署模式，能够稳定保障系统整体安全。

2 实验结果与分析

2.1 量子随机数随机性测试

本文所提防护方法不依赖任意传输介质固有物理特性，适配光纤、无线射频等多类光通信传输链路。本次原理验证基于Wi-Fi 5(802.11ac)链路搭建物理层环境，硬件采用Intel(R) Wi-Fi 6 AX201 160MHz网卡，链路收发速率为173 Mb/s。首先，采用NIST SP800-22国际通用密码学随机数测试标准，完成对量子随机数的随机性验证。再以尺寸为512×512像素的标准Lena图像为测试对象，从加解密正确性、像素分布均匀性、相邻像素相关性与信息熵4个维度，评估所提方法的可行性和有效性。

本文采用标准的NIST SP800-22全套测试套件，对从量子随机数模块采集到的1 Gbit量子随机数进行测试，设置显著性水平$\alpha = 0.01$。P值为各测试项在真随机假设下的显著性概率，当P值大于α时判定该测试项通过。测试结果如表1所示。可以看出，量子随机数所有测试项P值均高于0.01，序列通过率满足标准置信区间要求，全部15项测试均通过检验，这表明本文方法所生成的随机数具有良好的统计特性。

表1 NIST SP800-22测试结果表

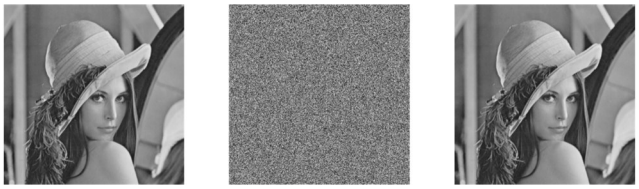
统计测试项	P值	通过率
频率测试	0.610 07	0.993
块内频率测试	0.128 132	0.995
累加和测试	0.578 057	0.991 5
游程测试	0.798 139	0.992
最长游程测试	0.908 76	0.992
矩阵秩测试	0.034 031	0.989
离散傅里叶变换测试	0.773 405	0.991
非重叠模板匹配测试	0.535 909	0.989 608
重叠模板匹配测试	0.151 19	0.992
通用统计测试	0.127 393	0.987
近似熵测试	0.482 707	0.989
随机游走测试	0.525 352	0.989 752
随机游走变量测试	0.328 949	0.989 252
序列测试	0.430 472	0.99
线性复杂度测试	0.984 881	0.994

2.2 加解密正确性验证

本文以标准尺寸为512×512像素的Lena图像作为实验传输数据来演示图像加密传输与解密。将发送端原始图像、加密后图像及接收端解密恢复得到的图像进行对比，如图3所示。可以看出，经本文方法的量子随机数加密后的图像像素灰度值被完全随机化，原始图像的轮廓、纹理、灰度分布等所有可辨识的视觉信息与结构特征被完全遮蔽，无法从加密图像中提取任何与明文相关的有效信息，有效阻断了图像原始信息的泄露风险。在接收端，通过相同的量子随机数以及索引序列完成解密操作后，恢复得到的图像与发送端原始明文图像完全一致，无任何失真、噪点与数据丢失。

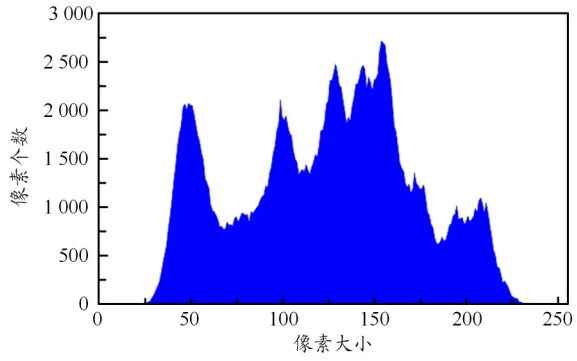
2.3 抗统计分析能力分析

图4为原始图像与加密后图像的像素灰度分布直

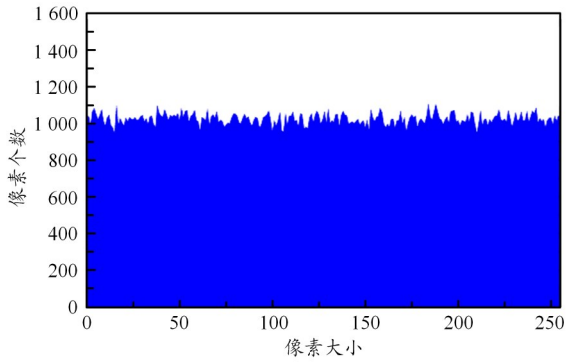


（a）原始图像　（b）加密后图像　（c）恢复后图像

图3 原始图像、加密后图像、恢复后图像对比



（a）原始图像



（b）加密后图像

图4 Lena图像加密前后的像素直方图对比

方图，可以看出，原始图像的像素分布呈现明显的多峰特征，灰度值集中在特定区间，能够直观反映图像的轮廓与纹理信息。经本文方法量子随机数加密后的图像，像素分布已趋于均匀，各灰度级的像素个数无显著差异，原始图像的灰度分布特征被完全破坏。均匀的像素分布意味着加密后的图像已不具备任何可被识别的统计规律，攻击者无法通过直方图分析获取明文信息，有效提升了数据的抗统计分析攻击能力，验证了本文方法在信息隐匿上的有效性。

为量化分析本文方法加密后数据的去相关性效果，本次实验分别从水平、竖直、对角3个相邻像素的空间关联方向，对加密前后图像数据的相邻像素相关性进行计算，采用密码学领域通用的皮尔逊线性相关系数作为量化指标[21]，计算结果如表2所示，可以看出，原始图像在3个方向的相邻像素相关系数均趋近于1。经本文方法量子随机数加密后图像在3个方向的相邻像素相关系数均降至1×10^{-3}以下，几乎完全趋近于0，其中竖直方向相关系数降低至1.38×10^{-4}，为3个方向中的最低值，降幅达到99.9%，去相关效果最为显著。

表2 图像相邻像素的相关系数

图像	水平相关系数	竖直相关系数	对角相关系数
原始	0.97	0.98	0.95
加密后	1.57×10^{-4}	1.38×10^{-4}	8.38×10^{-4}

这是由于原始图像的高相关系数，直接反映了自然图像固有的强空间线性关联，这种关联特性为攻击者提供了可利用的统计漏洞，而本文方法加密后相关系数的大幅下降，证明本文方法能够彻底打破明文像素间的空间线性关联，完全消除密文数据的局部结构特征与统计冗余。

信息熵是香农信息论中用于量化数据随机程度与不确定性的核心指标，也是目前评估加密方案抗统计攻击能力、密文随机特性的通用核心参数[21-22]。本次实验采用标准香农信息熵计算公式，对图像加密前后的信息熵进行量化计算得出原始Lena图像的信息熵为7.446，低于理论最大值。经量子随机数加密后，测试图像的信息熵提升至7.999，逼近理论最大值8，提升幅度7.4%。加密后信息熵接近理论极限的结果，从信息论层面证明本文方法加密后的密文数据具备近乎理想的均匀分布特性与随机性，无显著统计规律与信息冗余，攻击者无法通过统计分析手段从密文中提取有效明文信息。

2.4 传输性能分析

本文所提方法对业务数据逐字节进行异或运算，本质上是8个独立的逐比特异或运算并行执行。由于量子随机数密钥流满足均匀分布，加密后的比特序列同样服从均匀分布，与原始比特分布无关。这一特性意味着，加密本质上是对业务数据内容的无损重新编码，不会改变信号的任何物理传输属性。对于任意给定的调制方式，加密前后的调制信号具有完全相同的平均功率、幅度分布和概率密度函数。

在加性噪声信道下，信道噪声仅作用于信号的物理波形，与信号承载的二进制信息内容无关，因此加密信号与未加密信号在接收端的单比特误判概率相同，系统整体误码率也必然一致。该结论与调制方

式、编码方式和传输介质无关，表明本文方法不会对物理层传输性能产生负面影响。

3 结束语

针对光纤通信物理层抗截获能力不足和传统伪随机加密方案密钥安全性受限的问题，本文提出并实现了一种基于量子随机数分发的光物理层信息防护方法。该方法利用量子随机数模块产生高安全性随机源，依托云端管理平台实现随机数的集中存储、同步分发与日志管理，并设计了基于同步索引的流加密方案，收发双方利用相同的离线量子随机数库和索引序列即可完成数据加解密，避免了密钥在业务信道中的在线传输。

实验结果表明：量子随机数模块生成的随机数通过NIST SP800-22全部15项随机性测试，密钥源具有良好的统计特性；以512×512像素的Lena图像为业务数据，接收端能够无失真、无噪点地恢复原始图像；加密后数据像素直方图分布均匀，水平、竖直和对角方向上的相邻像素相关系数均降至10^{-3}量级以下，信息熵由7.446提升至7.999，提升7.4%，逼近理论最大值。上述结果说明，该方法能够有效消除明文的统计冗余，抵御光纤通信物理层的信息截获、窃听与篡改行为。

本文在理论上将量子真随机性与物理层信息防护相结合，在实践上提升了数据的随机化程度与去相关性，为高安全光通信系统提供了一种可行的防护方案。后续工作将聚焦量子随机数生成速率提升及多节点同步协议优化，以推动该方法在高速大容量光传输网络中的规模化应用。

参考文献：

[1] 张睿沛. 光纤通信网络窃听方法及防御措施[J]. 电信科学，2012，28(11)：112-115.

[2] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal，1975，54(8)：1355-1387.

[3] Csiszár I，Körner J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory，1978，24(3)：339-348.

[4] Fok M P，Wang Zhexing，Deng Yanhua，et al. Optical layer security in fiber-optic networks[J]. IEEE Transactions on Information Forensics and Security，2011，6(3)：725-736.

[5] Bennett C H，Brassard G. Quantum cryptography：public key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers，Systems and Signal Processing. 1984：175-179.

[6] Shor P W，Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters，2000，85(2)：441.

[7] Liao Shengkai，Cai Wenqi，Liu Weiyue，et al. Satellite-to-ground quantum key distribution[J]. Nature，2017，549：43-47.

[8] 朱宏峰，陈柳伊，王学颖，等. 量子密钥分发网络架构、进展及应用[J]. 沈阳师范大学学报(自然科学版)，2023，41(6)：515-525.

[9] Hirota O，Sohma M，Fuse M，et al. Quantum stream cipher by the Yuen 2000 protocol：design and experiment by an intensity-modulation scheme[J]. Physical Review A，2005，72(2)：022335.

[10] Futami F，Hirota O. 100 Gbit/s(10×10 Gbit/s) Y-00 quantum stream cipher transmission for secure optical communication[C]//Proceedings of 2014 OptoElectronics and Communication Conference and Australian Conference on Optical Fibre Technology. Australia: IEEE，2014：4-6.

[11] 马乐，张杰，王博，等. 光通信物理层安全中量子噪声流加密[J]. 激光与光电子学进展，2020，57(23)：122-134.

[12] 张旭，张杰，李亚杰，等. 基于量子噪声流加密的光纤物理层安全传输技术[J]. 光通信技术，2020，44(4)：18-22.

[13] 陈毓锴，蒲涛，郑吉林，等. 相移键控量子噪声随机加密系统性能研究[J]. 量子电子学报，2021，38(6)：846.

[14] 刘占琪，朱华涛，唐正毅，等. 基于DPSK的量子噪声流加密光隐藏通信系统[J]. 光学学报，2024，44(21)：73-81.

[15] 刘宇明，刘问宇，崔晨，等. 基于光通信物理层的密钥分发与加密控制系统研究[J]. 电力信息与通信技术，2020，18(12)：1-8.

[16] 王安帮，毛晓鑫，张蓉，等. 光学混沌保密光纤通信技术研究进展(特邀)[J]. 光学学报，2025，45(13)：364-389.

[17] 杨立锐，郭心悦. 基于物理层加密的OFDM可见光通信系统安全传输方案[J]. 光通信技术，2023，47(1)：17-24.

[18] 刘川，黄在朝，刘世栋，等. 基于LDPC码的相干光通信QNSC系统方案[J]. 光通信技术，2021，45(2)：24-27.

[19] Skorin-Kapov N，Furdek M，Zsigmond S，et al. Physical-layer security in evolving optical networks[J]. IEEE Communications Magazine，2016，54(8)：110-117.

[20] 童启夏，胡莹莹，何德勇，等. 自发辐射放大的量子随机数快速后处理方法[J]. 激光与光电子学进展，2024，61(5)：491-495.

[21] 郭永宁，孙树亮. 基于随机数和伪随机数相结合的图像加密算法[J]. 陕西师范大学学报(自然科学版)，2020，48(2)：52-57.

[22] Hayashi M，Vázquez-Castro A. Application of α-order information metrics for secure communication in quantum physical layer design[J]. AVS Quantum Science，2025，7(2)：0260710-1-0260710-11.